TRAFFIC TICKET REASONABLE, CELL PHONE SEARCH NOT: APPLYING THE SEARCH-INCIDENT-TO-ARREST EXCEPTION TO THE CELL PHONE AS "HYBRID"

*Eunice Park**

TABLE OF CONTENTS

* Assistant Professor of Lawyering Skills, Western State University College of Law. A special thank you to Professor Neil Gotanda, Professor Edith Warkentine, and John Lee, Esq., for their detailed and insightful comments, and to my former student, Jeff Guarrera, for his outstanding research assistance. The views expressed in this Article are the Author's own. I am grateful always to my parents and to my husband and children for their patience and support. I dedicate this Article to my mom, Kyung S. Park, and to the memory of my dad, Jong M. Park.

I. INTRODUCTION

The tension between the citizen's right to privacy and law enforcement's need to conduct a reasonable search faces a modern challenge: the cell phone. Incident to a lawful custodial arrest, a law enforcement officer may conduct a warrantless search of items "of the person," such as a purse, wallet, or pack of cigarettes.[1] On the other hand, items that are not of the person, but rather, are "possessions," such as a suitcase or computer, are considered to have a higher expectation of privacy and require a search warrant.[2]

What about the cell phone? This sleekly mobile, multifunctioning, and omnipresent device does not fit neatly into the dichotomy. As the law currently stands, it would not be unreasonable for an officer to search an arrestee's cell phone even for a minor traffic violation. Indeed, cell phones have replaced many of the tangible items individuals used to carry that officers could search without question, such as address books and photographs. However, cell phones house a vast amount of this kind of data and also store newer-generation information, such as text messages and e-mails. Most individuals would attest strongly that they have an expectation of privacy in their cell phones' contents and would object to such a search. Yet, officers need to be able to conduct a search of the person incident to custodial arrest. Should the electronic form shield the traditionally tangible data from view? What about the newer kinds of data? Moreover, how has the cell phone's very existence and sophisticated capabilities altered the way people communicate and the kinds of data that are relevant in an arrest?

This Article identifies five main rationales courts have offered in support of warrantless cell phone searches, surveys the caselaw according to this five-point spectrum, and proposes a rule for searching this "hybrid" device that balances each of the five points. The proposed rule factors in the strains suffered by the traditional framework, caused by both the newness of cell phone technology and the manner of cell phone use.

Part II of this Article describes the history and precedent behind the

1. *See* United States v. Robinson, 414 U.S. 218, 235 (1973).
2. *See* United States v. Chadwick, 433 U.S. 1, 11 (1977).

search incident to arrest rules, which has led to the present confusing status of the law on warrantless searches incident to arrest as applied to cell phones.[3]

Part III presents the disconnect between the law, technology, and cell phone use.[4] Subsection A both identifies a five-point spectrum of reasons that have evolved in the common law, both for and against warrantless cell phone searches, and surveys the rationales courts have adopted for finding a search reasonable within each point of the spectrum.[5] Subsection B explains why the existing framework is unable to accommodate searches of cell phones.[6] Part C provides a brief review of the current literature that can be broadly described as offering four major categories of arguments regarding cell phone searches which, while insightful, still leave many gaps.[7]

Part IV proposes a rule for warrantless searches of cell phones incident to custodial arrest that balances the five-point spectrum with modern technology's Fourth Amendment challenges based on the cell phone's "hybrid" nature.[8] Balancing the five distinct categories of reasons identified as evolving from the common law and taking into account the inconsistencies and areas upon which focus is needed, the proposed rule is that cell phones should be permitted to be searched incident to a valid custodial arrest when likely to yield evidence related to the reason for arrest by a relevant limited intrusion into data in which there is a diminished expectation of privacy. To this end, the presumption should be that only text messages, e-mail logs, and call logs may be searched. If there is a safety-related exigency, the officer's discretion is required to decide whether the exigency is reasonably related to the need to search additional data. The other exigency, of data destruction because of limited capacity, is no longer valid with the modern cell phone. Additionally, the unique risk of remote wipe or automatic deletion is a constant, and therefore non-exigent, threat that cannot justify the cell phone's warrantless search.

3. *See infra* Part II.
4. *See infra* Part III.
5. *See infra* Part III.A.
6. *See infra* Part III.B.
7. *See infra* Part III.C.
8. *See infra* Part IV.

II. THE HISTORY OF THE EXPECTATION OF PRIVACY IN ITEMS THAT CAN BE PERMITTED AND EXCLUDED FROM A WARRANTLESS SEARCH INCIDENT TO A VALID CUSTODIAL ARREST

A. *The Fourth Amendment and Search-Incident-to-Arrest Exception*

The Fourth Amendment protects individuals against unreasonable searches and seizures.[9] Although no general constitutional right to privacy exists, and no such right is expressly written into the Amendment's language,[10] Fourth Amendment jurisprudence encompasses an expectation of privacy.[11] The Fourth Amendment originally "was understood to embody a particular concern for government trespass,"[12] but, since *Katz v. United States*, it also implicates a reasonable expectation of privacy.[13] To invoke Fourth Amendment protection against unreasonable or warrantless searches based on a "*Katz* invasion of privacy,"[14] the area searched must be one where there is "a constitutionally protected reasonable expectation of privacy."[15] This "constitutionally protected reasonable expectation of privacy" consists of both a subjective and an objective requirement: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[16]

---

9. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

10. *See* Katz v. United States, 389 U.S. 347, 350 (1967) ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"); Newhard v. Borders, 649 F. Supp. 2d 440, 449–50 (W.D. Va. 2009) ("[A]ny plausible claim would arise . . . not under privacy rights protected by the Constitution.").

11. *See Katz*, 389 U.S. at 351 ("[T]he Fourth Amendment protects people, not places.").

12. United States v. Jones, No. 10-1259, slip op. at 5 (U.S. Jan. 23, 2012) (footnote omitted).

13. *See id.* at 5–7 (explaining the need to preserve these past rights by embodying them in the definition of a reasonable expectation of privacy, which is grounded in the Fourth Amendment). *But see id.* at 5 (Alito, J., concurring) (interpreting *Katz* as "finally [doing] away with the old approach, holding that a trespass was not required for a Fourth Amendment violation").

14. *Id.* at 7 n.5 (majority opinion).

15. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

16. *Id.* at 361. The Court held that

> a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to

Once this expectation is established, the burden is on the government to justify a warrantless search.[17] "[T]he Constitution requires 'that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police . . . .'"[18] A warrantless search is per se unreasonable, "subject only to a few specifically established and well-delineated exceptions."[19] One such exception is when the search is conducted incident to lawful arrest:

> "The right without a search warrant contemporaneously to search persons lawfully arrested while committing crime and to search the place where the arrest is made in order to find and seize things connected with the crime as its fruits or as the means by which it was committed, as well as weapons and other things to effect an escape from custody, is not to be doubted."[20]

The following will discuss the search-incident-to-arrest exception as it relates to cell phones.

B. *General Precedent Before Cell Phones*

The tradition of the Fourth Amendment expectation of privacy for searches conducted incident to lawful arrest recognized in *Katz*[21] was reinforced, though also narrowed, in *Chimel v. California*.[22] There, the Supreme Court reiterated it is reasonable for the arresting officer to search the person arrested to remove any weapons that could be used to resist arrest, effect escape, or endanger the officer's safety.[23] In addition, the Court broadened the justification for a warrantless search by specifically including the "concealment or destruction [of evidence]" as a basis for

---

> assume that the words he utters into the mouthpiece will not be broadcast to the world.

Id. at 352 (majority opinion).

17. *See id.* at 354 (noting whether the search and seizure was justified depended on the constitutional standards and reviewing the government's argument as to why it was justified).

18. *Id.* at 357 (second and third alterations in original) (quoting Wong Sun v. United States, 371 U.S. 471, 481–82 (1963)).

19. *Id.* (footnote omitted).

20. *Id.* at 357 n.20 (quoting Agnello v. United States, 269 U.S. 20, 30 (1925)).

21. *See id.* at 357 & n.20 (reaffirming the search incident to arrest is a search that meets one of the "few specifically established and well-delineated exceptions" to obtaining a warrant).

22. Chimel v. California, 395 U.S. 752 (1969).

23. *Id.* at 763.

searching "the arrestee's person and the area 'within his immediate control'—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence."[24] Applying this broadened justification to the facts in *Chimel*, the Court found that the search incident to defendant's proper arrest in the house on a burglary charge was unreasonable because it extended beyond his "person and the area from within which he might have obtained either a weapon or something that could have been used as evidence against him."[25] Thus, the warrantless search of defendant's entire house, including rooms other than where the arrest occurred, or even the desk drawers and other closed or concealed areas of the room where the arrest occurred, was not reasonable.[26]

Four years later, in *United States v. Robinson*, the Supreme Court rejected an expanded argument that the authority to search should depend on "what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect."[27] The defendant had been arrested for driving without a license when, in the course of the search incident to arrest, the officer found a crumpled-up package of cigarettes that did not feel like cigarettes.[28] When the officer opened the package, he found what was later determined to be heroin.[29] Though the defendant was arrested for driving without a license, the court held that "[h]aving in the course of a lawful search come upon the crumpled package of cigarettes, [the officer] was entitled to inspect it; and when his inspection revealed the heroin capsules, he was entitled to seize them as 'fruits, instrumentalities, or contraband' probative of criminal conduct."[30]

Moreover, because the custodial arrest itself gave "rise to the

24. *Id.*

25. *Id.* at 768.

> "After arresting a man in his house, to rummage at will among his papers in search of whatever will convict him, appears to us to be indistinguishable from what might be done under a general warrant; indeed, the warrant would give more protection, for presumably it must be issued by a magistrate."

Id. at 767 (quoting United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926)).

26. *Id.* at 763.

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

28. *Id.* at 220–23.

29. *Id.* at 223.

30. *Id.* at 236 (citations omitted).

authority to search, it is of no moment that [the officer] did not indicate any subjective fear of the respondent or that he did not himself suspect that respondent was armed."[31] The United States had already conceded on appeal that "'in searching respondent, [the officer] was not motivated by a feeling of imminent danger and was not specifically looking for weapons.'"[32] The Court called the "judgment" that persons arrested for the offense of driving with a revoked license are less likely to possess dangerous weapons than those arrested for other crimes "rather speculative,"[33] thus seeming to suggest the possibility of possessing dangerous weapons may be considered to exist with an arrest even if the officer does not actually suspect it.

A few years later, the Court swung back toward protecting the expectation of privacy unless the officers perceive an actual exigency. In *United States v. Chadwick*, law enforcement agents opened and searched defendants' locked footlocker seized from the trunk of a car outside a train terminal without a warrant and discovered marijuana.[34] The Supreme Court held the defendants had an expectation of privacy that was violated by the warrantless search where no exigency existed.[35]

> By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination. No less than one who locks the doors of his home against intruders, one who safeguards his personal possessions in this manner is due the protection of the Fourth Amendment Warrant Clause. There being no exigency, it was unreasonable for the Government to conduct this search without the safeguards a judicial warrant provides.[36]

In contrast to *Robinson*, in which the Court found "it [was] of no moment that [the officer] did not indicate any subjective fear of the respondent or that he did not himself suspect that respondent was armed,"[37] the Court in *Chadwick* took pains to point out there was no

31. *Id.* (footnotes omitted).

32. *Id.* at 236 n.7 (alteration in original) (citation omitted) ("Officer Jenks testified, 'I just searched him [Robinson]. I didn't think about what I was looking for. I just searched him.'").

33. *Id.* at 234.

34. United States v. Chadwick, 433 U.S. 1, 3–5 (1977).

35. *Id.* at 11.

36. *Id.*

37. *Robinson*, 414 U.S. at 236 (footnote omitted).

exigency calling for an immediate search.[38]

> The agents had no reason to believe that the footlocker contained explosives or other inherently dangerous items, or that it contained evidence which would lose its value unless the footlocker were opened at once. Facilities were readily available in which the footlocker could have been stored securely; it is not contended that there was any exigency calling for an immediate search.[39]

Thus, although in both *Robinson* and *Chadwick* the law enforcement officers did not believe exigency existed or posed a threat to the officer or general public, it appears that in *Robinson* this was inconsequential,[40] whereas in *Chadwick* the absence of any such perceived exigency was a fact in the defendants' favor.[41]

The grab zone notably included the passenger compartment of the vehicle where the arrestee was riding at the time of his arrest in *New York v. Belton*.[42] The Court held any container, "whether it is open or closed," in the car's passenger compartment may be searched, because a "lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have."[43] The police officer, after stopping a speeding vehicle, noticed the smell of "burnt marihuana and had seen on the floor of the car an envelope marked 'Supergold' that he associated with marihuana."[44] After directing the four passengers to get out of the car and placing them under arrest for unlawful possession of marijuana, the officer searched the passenger compartment of the car where he found a jacket in the back seat belonging to passenger Belton, unzipped a pocket, and discovered cocaine.[45]

The Court reconciled the facts of *Chimel*, where the police could not

38. *Chadwick*, 433 U.S. at 4.

39. *Id.*

40. *Robinson*, 414 U.S. at 236 ("Since it is the fact of custodial arrest which gives rise to the authority to search, it is of no moment that Jenks did not indicate any subjective fear of the respondent . . . ." (footnotes omitted)).

41. *Chadwick*, 433 U.S. at 11 ("There being no exigency, it was unreasonable for the Government to conduct this search without the safeguards a judicial warrant provides.").

42. *See* New York v. Belton, 453 U.S. 454, 460 (1981) (footnote omitted) (applying the *Chimel* grab area analysis in the context of a car and finding the passenger compartment searchable incident to a lawful arrest).

43. *Id.* at 461.

44. *Id.* at 455–56.

45. *Id.* at 456.

search all the drawers in an arrestee's house simply because the police had arrested him at home, with the observation that the *Chimel* Court "noted that drawers *within an arrestee's reach* could be searched because of the danger their contents might pose to the police."[46] Similarly,

> the police may . . . examine the contents of any containers found within the passenger compartment [of the vehicle], for if the passenger compartment is within reach of the arrestee, so also will containers in it be within his reach. . . . [T]he justification for the search is not that the arrestee has no privacy interest in the container, but that the lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have.[47]

Because the *Belton* Court did not clarify whether the item needed to be within the arrestee's grab zone at the time of the search or at the time of arrest, the Supreme Court in *Arizona v. Gant* decisively limited the vehicular search by declaring that under *Chimel*, *Belton* should be read to authorize police to search a vehicle incident to a recent occupant's arrest only when the arrestee is unsecured and can access the passenger compartment at the time of the search.[48] Moreover, the *Gant* court observed, in this case,

> [a]n evidentiary basis for the search was also lacking . . . . Whereas Belton . . . [was] arrested for drug offenses, Gant was arrested for driving with a suspended license—an offense for which police could not expect to find evidence in the passenger compartment of Gant's car. Because police could not reasonably have believed either that Gant could have accessed his car at the time of the search or that evidence of the offense for which he was arrested might have been found therein, the search in this case was unreasonable.[49]

The Court expressed concern about law enforcement rummaging without evidentiary basis.

> A rule that gives police the power to conduct such a search whenever

46. *Id.* at 461 (emphasis added) (citing Chimel v. California, 395 U.S. 752, 763 (1969)).

47. *Id.* at 460–61 (footnote omitted) (citations omitted).

48. *See* Arizona v. Gant, 129 S. Ct. 1710, 1714 (2009). The court contrasted *Belton*, "a single officer confronted with four unsecured arrestees" to this case, "the five officers . . . outnumbered the three arrestees, all of whom had been handcuffed and secured in separate patrol cars before the officers searched Gant's car." *Id.* at 1719.

49. *Id.* (citation omitted).

> an individual is caught committing a traffic offense, when there is no basis for believing evidence of the offense might be found in the vehicle, 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.[50]

Justice Scalia would place this concern about relatedness of the search to the reason for arrest at the forefront of the analysis. In his concurrence in *Thornton v. United States*, Justice Scalia stated he would "limit *Belton* searches to cases where it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle."[51] He continued to maintain in his concurrence in *Gant* five years later that he "would hold that a vehicle search incident to arrest is *ipso facto* 'reasonable' only when the object of the search is evidence of the crime for which the arrest was made, or of another crime that the officer has probable cause to believe occurred."[52] Scalia would hold the search unlawful "[b]ecause [Gant] was arrested for driving without a license (a crime for which no evidence could be expected to be found in the vehicle)."[53] His position is that a search for evidence should be limited to the reason for arrest, unless an officer safety or evidence preservation exigency exists.

> When officer safety or imminent evidence concealment or destruction is at issue, officers should not have to make fine judgments in the heat of the moment. But in the context of a general evidence-gathering search, the state interests that might justify any overbreadth are far less compelling. A motorist may be arrested for a wide variety of offenses; in many cases, there is no reasonable basis to believe relevant evidence might be found in the car.[54]

The role the relatedness of the evidence to the reason for arrest plays in the absence of an imminent risk that evidence will be destroyed—as introduced by *Chimel*[55] and pointed out in *Chadwick*[56]—is less certain

50. *Id.* at 1720 (footnote omitted).

51. Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring).

52. *Gant*, 129 S. Ct. at 1725 (Scalia, J., concurring).

53. *Id.*

54. *Thornton*, 541 U.S. at 632 (citations omitted).

55. *See* Chimel v. California, 395 U.S. 752, 763 (1968) ("[I]t is entirely reasonable for the arresting officer to search for and seize any evidence on the

under *Gant*.[57] The circuit courts are also "divided over whether *Gant* applies solely in the vehicular-search context or whether it generally limits the scope of the search-incident-to-arrest exception."[58]

In summary, the pre-cell phone era established the following framework for the validity of warrantless searches, under the Fourth Amendment, incident to a lawful custodial arrest: officers may search the arrested person and also the area within the arrestee's immediate control or grab zone, including the vehicle passenger compartment if the arrestee is unsecured or the evidence sought is related to the reason for arrest. An item of the person is a "container" in which the individual, by virtue of being arrested, forfeits the expectation of privacy, which must have been both subjectively and objectively reasonable. The two general exigencies justifying the warrantless search incident to arrest of the person are (1) to ensure officer safety and (2) to prevent the concealment or destruction of evidence. The officer's perception regarding the existence of an exigency should be considered. On the other hand, officers may not search "possessions," or personal property not immediately associated with the person, which may be distanced by being locked or because the item is unrelated to the reason for the arrest, without a warrant.

III. THE DISCONNECT BETWEEN THE LAW, TECHNOLOGY, AND USE

The five-point spectrum of rationales the courts have generated to apply the search-incident-to-arrest exception to cell phones is contradictory and inconsistent because of the cell phone's unique technological capabilities, the corresponding changes to everyday communication, and the cell phone data's value to law enforcement. The current literature offers valuable contributions to the gaps in the ongoing dialogue, but it tends to evaluate the warrantless searchability of the cell phone vis-à-vis limited prisms. Additionally, some of the criteria suggested and

arrestee's person in order to prevent its concealment or destruction. And the area into which an arrestee might reach . . . must, of course, be governed by a like rule.").

56. *See* United States v. Chadwick, 433 U.S. 1, 14 (1977) ("The reasons justifying search in a custodial arrest are quite different. When a custodial arrest is made, there is always some danger that the person arrested may seek to use a weapon, or that evidence may be concealed or destroyed.").

57. *See* Hawkins v. State, 704 S.E.2d 886, 889 (Ga. Ct. App. 2010) ("[T]here is some uncertainty about the precise scope of a search for evidence under *Gant* in the absence of an imminent risk that evidence will be destroyed . . . .").

58. *See* United States v. Curtis, 635 F.3d 704, 713 & n.22 (5th Cir. 2011), *cert. denied*, 132 S. Ct. 191 (2011).

technological assumptions made need further guidance and inquiry.

A. *The Confusing Five-Point Spectrum Regarding Warrantless Cell Phone Searches Incident to a Valid Custodial Arrest*

The courts have struggled to keep up with the rapidly changing cell phone technology and corresponding changes in communication and have faithfully, but confusingly, attempted to apply common law precedent to this evolving and unanticipated landscape.

At first glance, there appear to be two camps: those jurisdictions that allow cell phone searches as an item of the "person" and those that label the phone as a "possession." However, among those courts that both support and oppose warrantless cell phone searches incident to custodial arrests, the specific reasons offered are varied and conflicting.

This Article distills those reasons into five main points that courts have offered in support of warrantless cell phone searches: (1) the cell phone is a traditional container in which the expectation of privacy is forfeited upon a lawful arrest;[59] (2) the search is related to the reason for arrest;[60] (3) although the arrestee may have an expectation of privacy in the contents of the cell phone, the officer's search is justified because of the exigency that evidence can be inadvertently deleted or even deliberately destroyed;[61] (4) the officer's search is justified to prevent harm to the officer;[62] and (5) the arrestee cannot claim a reasonable expectation of privacy in the information on a cell phone stored on third-party servers.[63]

This Article then organizes the common law by discussing select cases on both sides of each point, and, while many cases incorporate multiple rationales, the Author has chosen a case to represent a specific point or points when its reasoning for that category is particularly notable.

The majority of jurisdictions allow the cell phone search for some combination of these reasons; the courts "trend heavily in favor of finding that the search incident to arrest or exigent circumstances exceptions apply to searches of the contents of cell phones."[64]

59. *See infra* Part III.A.1.
60. *See infra* Part III.A.2.
61. *See infra* Part III.A.3.
62. *See infra* Part III.A.4.
63. *See infra* Part III.A.5.
64. United States v. Wurie, 612 F. Supp. 2d 104, 109 (D. Mass. 2009) (citations omitted).

1. *Cell Phone as Container*

The first point in the five-point spectrum is that the cell phone is a container in which the expectation of privacy is forfeited upon arrest. This is the point that emerges most frequently in the discussion of the reasonableness of a warrantless cell phone search.

a. *Cell phone is a container.* The main argument behind the rationale that a warrantless cell phone search is reasonable is that the cell phone is no different than any traditional container subject to search incident to arrest.[65]

The Fifth Circuit Court of Appeals is the highest-ranking federal court at the time of this writing to declare the call records and text messages retrieved from a warrantless cell phone search are admissible because the defendant's cell phone is a container.[66] While oft-cited for this position,[67] the *Finley* case actually offers very little reasoning for its finding that the cell phone was a container.[68] The defendant had already conceded the cell phone was a container, contending that because it was "closed," the police had no authority to examine its contents.[69] The court readily found that because the phone was on the defendant's person and a lawful arrest extends to containers found on the arrestee's person—whether open or closed—"no warrant was required since the search was conducted pursuant to a valid custodial arrest."[70]

The California Supreme Court likewise deemed the cell phone no different from the cigarette package taken from the defendant's coat pocket in *Robinson* and unlike the footlocker in *Chadwick*.[71] The *Diaz* court disapproved of a "'subjective and highly fact specific [approach that] would require precisely the sort of ad hoc determinations on the part of officers in the field and reviewing courts' that the high court has

65. *See* United States v. Robinson, 414 U.S. 218, 236 (1973).

66. United States v. Finley, 477 F.3d 250, 260 & n.7 (5th Cir. 2007).

67. *See, e.g.*, United States v. Curtis, 635 F.3d 704, 712–13 (5th Cir. 2011) (citing *Finley* to show a warrant is not needed to search a cell phone pursuant a lawful arrest); United States v. Zavala, 541 F.3d 562, 576–77 (5th Cir. 2008) (citing *Finley* for the proposition that "'[t]he permissible scope of a search incident to a lawful arrest extends to containers found on the arrestee's person'").

68. *See Finley*, 477 F.3d at 260 & n.7.

69. *See id.* at 260 (citing Walter v. United States, 447 U.S. 649 (1980)).

70. *Id.* (citing *Robinson*, 414 U.S. at 235).

71. People v. Diaz, 244 P.3d 501, 505 (Cal. 2011).

condemned"[72] and rejected a "quantitative approach" in which the validity of a search required considering the amount of personal information a particular item might contain.[73] Instead, the court held in accordance with *Belton*, in which the Court stated any container may "'be searched whether it is open or closed, since the justification for the search is not that the arrestee has no privacy interest in the container, but that the lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have.'"[74]

Courts since have stated outright that the information in a cell phone in digital form is no different than the same information in physical form:

> [T]he information found within [a digital file] is likely no different than information found within a printed physical copy of a digital file. Indeed, before the innovations made available in current cell phone technology, the information contained within digital files would have been contained in tangible copies and carried in closed containers. . . . [T]he cell phone merely acts as a case (i.e. closed container) containing these personal effects. . . . Accordingly, a distinction based upon the manner in which that information is stored is unwarranted.[75]

The *Fawdry* court held the images of child pornography found on the defendant's cell phone, which was searched after his arrest on an unrelated warrant, were admissible.[76] District courts have agreed "[a] cell phone, like a beeper, is an electronic 'container,' in that it stores information . . . . While such electronic storage devices are of more recent vintage than papers, diaries, or traditional photographs, the basic principle still applies . . . ."[77] Hence, defendant's cell phone, found on his person, "should not be

72. *Id.* at 508–09 (citations omitted).

73. *Id.* at 508.

74. *Id.* at 507 (quoting New York v. Belton, 453 U.S. 454, 460–61 (1981)); *see also* People v. Nottoli, 130 Cal. Rptr. 3d 884, 907 (Ct. App. 2011) ("Respondents assert that 'the issue of whether a cell phone should be distinguished from traditional containers due to its capacity for storage of digital information is not yet settled' and that a cell phone is not a container within the meaning of U.S. Supreme Court's decisions. In *Diaz*, the California Supreme Court rejected the arguments that the nature or character of a cell phone, its capacity for storing personal data, or the arrestee's expectation of privacy in its contents required courts to treat the arrestee's cell phone found on him differently from other types of personal effects or containers that may be validly searched incident to arrest." (citing *Diaz*, 244 P.3d 501)).

75. *See, e.g.*, Fawdry v. State, 70 So. 3d 626, 630 (Fla. Dist. Ct. App. 2011).

76. *Id.* at 627.

77. United States v. McCray, No. CR408-231, 2009 WL 29607, at *4 (S.D. Ga. Jan. 5, 2009); *see also* United States v. Wurie, 612 F. Supp. 2d 104, 110 (D. Mass. 2009)

treated any differently than, for example, a wallet taken from a defendant's person."[78]

b. *Cell phone is not a container.* Courts that have disagreed with the container analogy have noted the vastness of data a cell phone can carry, the inability to assess a cell phone's contents from its exterior, the cell phone's inability to hold tangible items, and its absence from the original container analysis framework.

For example, the district court in *United States v. Park* found that "for purposes of Fourth Amendment analysis cellular phones should be considered 'possessions within an arrestee's immediate control' and not part of 'the person.'"[79] The court focused on the vast quantity of information a cell phone can store, "[u]nlike pagers or address books."[80] "[M]odern cellular phones have the capacity for storing immense amounts of private information. . . . Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages."[81]

In addition to this vastness of data, courts have noted an officer's inability to outwardly assess a cell phone's contents. The court of appeals in Kansas held that the expectation of privacy in a cell phone does not differ from a personal computer, applying the ruling of its state supreme court that required a warrant to search a computer hard drive.[82] The state

(finding "no principled basis for distinguishing a warrantless search of a cell phone from the search of other types of personal containers found on a defendant's person" in reviewing a number of cases involving storage devices on the person); United States v. Dennis, No. 07-008-DLB, 2007 WL 3400500, at *7 (E.D. Ky. Nov. 13, 2007) (noting "[t]here is nothing to indicate that the Sixth Circuit would treat the retrieval of information from a cell phone differently than it treats other evidence gathered in a search incident to arrest" (citation omitted)).

78. United States v. Hill, No. CR 10-00261 JSW, 2011 WL 90130, at *7 (N.D. Cal. Jan. 10, 2011) (citations omitted); *see also* Watters v. City of Cotati, No. C 10-2574 SBA, 2011 WL 4853590, at *5 (N.D. Cal. Oct. 13, 2011) (finding no violation of plaintiff's constitutional rights as a matter of law when police officer searched plaintiff's cellular telephone incident to personal search).

79. United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007) (quoting United States v. Chadwick, 433 U.S. 1, 16 n.10 (1977)).

80. *Id.* (footnote omitted).

81. *Id.*

82. State v. Isaac, No. 101,230, 2009 WL 1858754, at *4 (Kan. Ct. App. June 26, 2009) (citing State v. Rupnick, 125 P.3d 541 (Kan. 2005)).

supreme court stated:

> [A] computer is not truly analogous to a simple closed container or conventional file cabinet, even a locked one. Rather, it is the digital equivalent of its owner's home, capable of holding a universe of private information. Further, a computer's outward appearance, unlike the containers dealt with in at least some of the cases . . . tells the observer nothing about the content or character of the information or potential evidence contained on its hard drive.[83]

On the other hand, the Ohio Supreme Court objected to the container analogy because of the cell phone's inability to hold a tangible object.[84] In *State v. Smith*, the court disagreed with the *Finley* court, which held that the cell phone could be a closed container and thus subject to search upon a lawful arrest,[85] because "[o]bjects falling under the banner of 'closed container' have traditionally been physical objects capable of holding other physical objects. Indeed, the United States Supreme Court has stated that in this situation, 'container' means 'any object capable of holding another object.'"[86] The court discounted the cases analogizing cell phones to pagers and early computer memo books that "bear little resemblance to the cell phones of today," stating the wealth of information even a basic cell phone can hold is "wholly unlike any physical object found within a closed container."[87]

Other courts have similarly rejected the container analysis but have disagreed with the Ohio Supreme Court's reasoning. A Florida district court rejected the argument that a cell phone must be a container at all when it held a warrantless cell phone search was valid under the Fourth Amendment.[88]

> While *Chimel*, *Robinson* and *Belton* permitted the search and inspection of items within the arrestee's reach, including containers, none of these cases required an item to be a 'container,' as opposed to some other type of item, in order to be searched upon arrest. Thus, whether or not a cell phone is properly characterized as a traditional

83. *Rupnick*, 125 P.3d at 552.

84. *See* State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009).

85. *See id.* at 953–54 (distinguishing this case from the analysis used by the Fifth Circuit in deciding *Finley*).

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

87. *Id.*

88. Smallwood v. State, 61 So. 3d 448, 460 (Fla. Dist. Ct. App. 2011).

> 'container' is irrelevant to whether or not it is searchable upon arrest.[89]

The California Supreme Court similarly noted "[t]he word 'container' does not appear in *Robinson* and *Edwards*. It appears once in *Chadwick*, in a footnote where the high court explained that the defendant's principal privacy interest in the footlocker was 'not in the container itself . . . but in its contents.'"[90]

While dismissing the vastness of storage capacity as a basis for heightened protection for cell phones,[91] the Florida appellate court in *Smallwood* empathized with the Ohio court's position in *Smith*,[92] observing "the *Robinson* court could not have contemplated the nearly infinite wealth of personal information cell phones and other similar electronic devices can hold. Modern cell phones can contain as much memory as a personal computer . . . ."[93] The court further noted,

> Cell phones are also capable of accessing the internet and are, therefore, capable of accessing information beyond what is stored on the phone's physical memory. . . . Essentially, cell 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.[94]

Although bound by precedent, the court found compelling the position that a cell phone does not seem to be a traditional container.[95]

2. *Relatedness to the Reason for Arrest*

The second point in the five-point spectrum is the warrantless search of the cell phone's relatedness to the reason for the arrest.

a. *Relatedness required.* Worried about law enforcement

89. *Id.*

90. People v. Diaz, 244 P.2d 501, 510 n.14 (Cal. 2011) (second alteration in original) (quoting United States v. Chadwick, 433 U.S. 1, 13–14 n.8 (1997)).

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

92. *See Smith*, 920 N.E.2d at 955 (reasoning the "ability [of a cell phone] to store large amounts of data gives their users a reasonable and justifiable expectation of a higher level of privacy in the information they contain").

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

94. *Id.*

95. *See id.* at 448 (noting it is "not unmindful . . . of the unique qualities of a cell phone").

"rummaging" in the course of a cell phone search to discover incriminating evidence, some courts required that the search be related to the reason for arrest. A subset of those courts has further specified that law enforcement officer needs no reasonable probability of finding evidence related to the reason for the arrest, while another subset asserts the search must be reasonably likely to yield evidence related to the reason for arrest.

In *Gant*, the Supreme Court observed that "to allow vehicle searches incident to any arrest would serve no purpose except to provide a police entitlement" and declared that permitting a warrantless search on that basis "is anathema to the Fourth Amendment."[96] In one concurring opinion in a state court, the judge asserted "[u]nder *Gant*, the warrantless search for evidence in the passenger compartment of the vehicle *must* be justified by a reasonable belief that evidence supporting the crime for which [the arrestee] was arrested, i.e. drugs, may be found there."[97]

Concern over rummaging similarly led the Georgia Court of Appeals in *Hawkins v. State* to declare "[t]he most restrictive plausible interpretation of *Gant* is that such a search is limited in scope to a search of places and things in a vehicle in which one reasonably might find the specific kinds of evidence of the crime of arrest that the officer has reason to believe may be found in the vehicle."[98] Specifically, "[j]ust because an officer has the authority to make a search of the data on a cell phone . . . does not mean that he has the authority to sift through *all* of the data stored on the phone,"[99] especially because cell phones may contain private, or even privileged, communications.[100] Instead, the officer's "search must be limited as much as is reasonably practicable by the object of the search."[101]

The court acknowledged the subjectiveness of this approach but determined such decision making was within the proper scope of the

96. Arizona v. Gant, 129 S. Ct. 1710, 1721 (2009).

97. Commonwealth v. Gerald, No. 2010-CA-000015-MR, 2011 WL 2582526, at *4 (Ky. Ct. App. July 1, 2011) (Caperton, J., concurring) (emphasis added); *see also* United States v. Bradley, No. 2:11cr00013, 2012 WL 160065, at *4 (W.D. Va. Jan. 18, 2012) (denying the defendants' motion to suppress evidence found in a vehicle search based on the fact the officer "had a reasonable belief that evidence relevant to the crime of making false statements might be found in the vehicle" (citations omitted)).

98. Hawkins v. State, 704 S.E.2d 886, 889–90 (Ga. Ct. App. 2010) (footnote omitted).

99. *Id.* at 891.

100. *Id.*

101. *Id.* at 892 (citing United States v. Ross, 456 U.S. 798, 824 (1982)).

officer's duties.

> Although this approach admittedly requires a fact-specific assessment in each case of the reasonable scope of the search at issue, that is something with which both police officers and judges are accustomed to dealing [and is] preferable to the approach . . . which would require police officers and judges to distinguish between 'ordinary' cell phones and those with a 'capacity comparable to that of a computer.' . . . We too would worry if officers were permitted without good cause or reason to rummage through all the data stored on a cell phone without limitation.[102]

Likewise, in *United States v. McGhee*, the court, facing a drug-related arrest, limited the scope of a *Gant* search by requiring a reasonable probability of finding evidence.[103] The defendant was arrested pursuant to a "warrant based on a conspiracy to distribute drugs and for distribution of drugs."[104] The court held the cell phone contact list searched and copied by the officer was not justified because the officers could not reasonably have believed a search of the defendant's cell phone in January 2009 would produce evidence related to the crime for which he was arrested, dating back to March 2008.[105]

Other courts have focused on the original justifications for a warrantless search, as spelled out in *Chimel*,[106] as the basis for the relatedness requirement. The cell phone search in *United States v. Quintana*—in which the defendant was pulled over for speeding and the officer noticed the smell of marijuana emanating from the vehicle[107]—not only went beyond the twin justifications of *Chimel*, but had "nothing to do with officer safety or the preservation of evidence related to the crime of arrest" of driving with a suspended license.[108] The officer "was rummaging for information related to the odor of marijuana emanating from the vehicle," and such a search "pushe[d] the search-incident-to-arrest doctrine

102. *Id.* at 892 n.6.

103. United States v. McGhee, No. 8:09CR31, 2009 WL 2424104, at *3 (D. Neb. July 21, 2009).

104. *Id.*

105. *Id.* at *1, *3; *see also* United States v. Jenkins, No. 5:11-cr-6, 2011 WL 3812621, at *5 (N.D. W. Va. June 28, 2011) (finding "it was not reasonable for the patrolmen to believe a search of the memory card seized from Defendant's pocket [incident to arrest] would produce evidence related to the theft of the 'four-wheeler'").

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

107. United States v. Quintana, 594 F. Supp. 2d 1291, 1294 (M.D. Fla. 2009).

108. *Id.* at 1300 (citations omitted).

beyond its limits."[109]

The *Quintana* court added a notable exception that stands in contrast to the *McGhee* decision.[110] When defendants are arrested for drug-related activity, there may be a "reasonable probability that information stored on the device [is] 'evidence of *the arrestee's crime*'" because electronic devices may have been used to communicate with others participating in drug trafficking.[111] Thus, police may be justified in searching the cell phone for evidence related to a drug-related arrest "even if the presence of such evidence is *improbable*."[112]

While still maintaining that relatedness is a requirement, the court of appeals in California even more boldly asserted that a broad interpretation of *Gant*—which requires no "reasonable" probability of finding relevant evidence[113]—applies to arrests generally, not merely drug-related arrests.[114] The court rejected the respondents' assertion that "in order to retain the integrity of the *Gant* rationale, the police may search only any container that is reasonably likely to contain relevant evidence of the offense."[115] Instead, the court declared, "We must immediately dispel any misconception that *Gant* limits the scope of a vehicular search incident to arrest in the situation where 'it is reasonable to believe that evidence of the offense of arrest *might* be found in the vehicle.'"[116] Rather, *Gant* "does not require *any degree of probability* that evidence bearing on [the reason for arrest] will be found in a particular container that is searched."[117] Where

109. *Id.* (citations omitted). "During oral argument [in *Gant*] . . . Justice Scalia seemed skeptical that law enforcement could arrest someone and then 'rummage around for evidence of a different crime.'" *Id.* (citations omitted); *see* United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) (frowning upon "'general rummaging . . . to discover incriminating evidence,'" and distinguishing a cell phone search from a routine driver's license check in an investigative vehicle stop (footnote omitted) (citation omitted)).

110. *See McGhee*, 2009 WL 2424104, at *3 (finding cell phone search unreasonable because the officer could not have had a reasonable belief the search would produce evidence related to the crime he was arrested for).

111. *Quintana*, 594 F. Supp. 2d at 1299 (emphasis added) (quoting United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007)).

112. *Id.* at 1300 (emphasis added).

113. People v. Nottoli, 130 Cal. Rptr. 3d 884, 902 (Ct. App. 2011) (citing Arizona v. Gant, 129 S. Ct. 1710, 1719 (2009)).

114. *See id.* at 902–03.

115. *Id.* at 904.

116. *Id.* (quoting *Gant*, 129 S. Ct. at 1714).

117. *Id.* at 905 (emphasis added).

"(1) the arrestee is unsecured and within reaching distance of the vehicle or (2) there is a reasonable basis for believing the vehicle might contain evidence relevant to the offense of arrest," the officer "has the generalized authority to search the entire passenger compartment of a vehicle and any containers therein incident to arrest."[118]

b. *Relatedness not required.* For those courts that do not require the search to be related to the reason for arrest at all, the rationale centers on adhering to the basic principle that a custodial arrest justifies a warrantless search.

The *Smallwood* court found no basis in the precedent to even consider a rationale that the search was likely to lead to evidence of the crime of arrest.[119] Observing that in *Robinson* the Court granted the authority to search the person incident to a lawful custodial arrest without depending on the probability that weapons or evidence would be found, the court interpreted *Robinson* and other precedent to establish "a bright-line rule permitting a search incident to arrest . . . . Thus, [in Florida,] whether or not the officer had reason to believe appellant's cell phone contained evidence of the crime is irrelevant."[120]

Similarly, the court in *Fawdry* rejected the defendant's argument that the *Gant* Court held "searches of containers under *Belton* are limited to searches for evidence of the crime of arrest."[121] Instead, the court asserted the *Gant* Court's intent was to correct "what it deemed to be an overly broad reading of that opinion by other courts," and reasoned *Gant* held only that "*Belton* does not justify the search of a vehicle where a suspect is secured and not able to reach the area of the car being searched."[122]

The district court in *Park* also shunned inclusion of relatedness to the reason for arrest as a basis for holding the cell phone search reasonable, even though the arrests were specifically drug-related and the officers found drug-related evidence.[123] The officers' search of the phones in order to find evidence of marijuana trafficking or cultivation was "purely investigatory," and "[o]nce the officers lawfully seized defendants' cellular

118. *Id.* at 904 (citing *Gant*, 129 S. Ct. at 1714, 1719, 1721).
119. Smallwood v. State, 61 So. 3d 448, 460 (Fla. Dist. Ct. App. 2011).
120. *Id.*
121. Fawdry v. State, 70 So. 3d 626, 630 (Fla. Dist. Ct. App. 2011).
122. *Id.* (citing *Gant*, 129 S. Ct. at 1718–19).
123. United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *3 (N.D. Cal. May 23, 2007).

phones, officers could have sought a warrant."[124] Such a search went "far beyond the original rationales for searches incident to arrest, which were to remove weapons to ensure the safety of officers and bystanders, and the need to prevent concealment or destruction of evidence."[125] The evidence, according to the court, should then be suppressed.[126] The California court was "unwilling to further extend [the *Chimel*] doctrine to authorize the warrantless search of the contents of a cellular phone—and to effectively permit the warrantless search of a wide range of electronic storage devices—as a 'search incident to arrest.'"[127]

Even where another district court described the officer's conduct in sharing the arrestee's private photographs, which were unrelated to the reason for arrest,[128] as "certainly 'deplorable, reprehensible, and insensitive'" and "irresponsible [and] unprofessional,"[129] the court could find no basis for concluding the conduct violated any Fourth Amendment right.[130] The officers found sexually explicit photographs of the defendant and his girlfriend in the defendant's cell phone and shared them with other law enforcement officers and members of the public with the alert "that the private pictures were available for their viewing and enjoyment."[131] "[G]iven the Fourth Circuit's approval of the retrieval of text messages and other information from a cell phone seized incident to an arrest in *Murphy* and the lack of a clear rule from the Supreme Court,"[132] the court held a reasonable officer could have believed the "search of the cell phone after [defendant's] arrest 'comported with the Fourth Amendment'" as a valid search incident to arrest.[133]

Another defendant's attempt to directly characterize the search of his cell phone as a "'ruse for a general rummaging in order to discover incriminating evidence'"[134] did not deter the court from holding the search

124. *Id.* at *8 (footnote omitted).
125. *Id.* (citing Chimel v. California, 395 U.S. 752 (1969)).
126. *See id.* at *8–9.
127. *Id.* at *9 (citing United States v. Thornton, 541 U.S. 615, 632 (2004)).
128. *See* Newhard v. Borders, 649 F. Supp. 2d 440, 444 (W.D. Va. 2009).
129. *Id.* at 450.
130. *See id.* at 448–50.
131. *Id.* at 444 (citations omitted).
132. *Id.* at 448 (citing United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009)).
133. *Id.* at 448–49 (quoting Anderson v. Creighton, 483 U.S. 635, 637–41 (1987)).
134. United States v. Curtis, 635 F.3d 704, 712 (5th Cir. 2011) (footnote

was authorized.[135] Although the defendant was arrested on an outstanding warrant on charges of making a false statement to obtain credit, the officer discovered text messages later introduced at trial as evidence of the existence of a conspiracy in an unrelated mortgage fraud scheme.[136] The Fifth Circuit nonetheless held the search to be constitutional under *Finley* because the cell phone was within the area of the defendant's immediate control.[137]

3. *Need to Preserve Evidence*[138]

The third point in the five-point spectrum is the law enforcement officer's need to preserve evidence on the cell phone.

a. *Evidence destruction risk.* Courts concerned about the destruction of evidence emphasized the officer could not know if the information on the cell phone would be deleted. A frequently arising preoccupation of courts is that call histories and text messages can be lost by incoming phone calls or remote delete or deactivation[139] and there is no

omitted) (quoting Florida v. Wells, 495 U.S. 1, 4 (1990)).

135. *See id.* at 712–13 (footnote omitted) (rejecting the ruse argument as it only applies to inventory searches).

136. *Id.* at 711.

137. *Id.* at 712–13 (footnote omitted).

138. This section will not discuss the reasoning in the cases involving pagers, which can receive only a limited number of digits and have such limited technology that incoming phone calls can "destroy currently stored telephone numbers in a pager's memory" if not immediately pulled off the pager. United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996); *see also* United States v. Romero-Garcia, 991 F. Supp. 1223, 1225 (D. Or. 1997) (involving a case in which the defendant consented to a search of his pager, yet the court explained the search would have been reasonable even without proper consent due to the exigency to preserve evidence associated with pagers).

139. *See, e.g.*, United States v. Young, 278 F. App'x 242, 245–46 (4th Cir. 2008) ("[The] officers had no way of knowing whether the text messages would automatically delete themselves or be preserved. Accordingly, based upon . . . the manifest need of the officers to preserve evidence, we conclude that the officers permissibly accessed and copied the text messages on the phone during the search incident to arrest."); United States v. Santillan, 571 F. Supp. 2d 1093, 1102–03 (D. Ariz. 2008) (holding the search was justified by the exigency of needing to preserve evidence where the agents had a valid concern that "incoming calls . . . could destroy evidence that was then located on the cell phone's recent contacts lists"); United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3–4 (E.D. Wis. Feb. 8, 2008) (holding a search of the defendant's cell phone was lawful when the investigating officer concerned about remote erase or deactivation "knew that call histories on cell phones could be deleted or lost, giving rise to a legitimate concern about destruction of evidence"); United

"way of knowing whether the text messages and other information stored on a cell phone will be preserved or be automatically deleted simply by looking at the cell phone."[140]

The district court in *United States v. Zamora* also noted the value of the evidence in the cell phone, particularly for drug trafficking arrests and the dynamic nature of that evidence.[141] "[C]ell phones provide vital links in drug conspiracies and corroborating evidence of the surveillance conducted during the transaction."[142] The court stated, "[T]he contents of the cell phones can be altered by each incoming call or by other events beyond the agent's control creating an exigency to conduct the search before the cell phone memory is altered,"[143] and the investigating agents reasonably believed the cell phones were "subject to change without warning by a call simply being made to the instrument."[144] Thus,

> [w]ith each call is the risk that a number stored would be deleted, including the loss of calls made to or from the instrument in connection with the transportation and ultimate secured storage of the pseudoephedrine at issue here. These numbers would have significant evidentiary value.[145]

The court held "the function and limitation of the cell-phone technology . . . motivated the investigating agents to conduct an immediate search of the phones, rather than seek a warrant."[146]

The argument that police had no authority to examine the phone's contents because cell phones require manipulation to access text messages

States v. Parada, 289 F. Supp. 2d 1291, 1304 (D. Kan. 2003) ("[T]he agent had the authority to immediately search or retrieve, as a matter of exigency, the cell phone's memory of stored numbers of incoming phone calls, in order to prevent the destruction of this evidence." (footnote omitted)).

140. United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009) (citing *Young*, 278 F. App'x at 245).

141. United States v. Zamora, No. 1:05 CR 250 WSD, 2006 WL 418390, at *4 (N.D. Ga. Feb. 21, 2006).

142. Order & Report & Recommendation, United States v. Zamora, No. 1:05-CR-250-WSD, 2005 U.S. Dist. LEXIS 40775, at *31–32 (N.D. Ga. Dec. 7, 2005); *see also* Order, United States v. Zamora, No. 1:05-CR-250-WSD, 2006 WL 418390, at *1 & n.2 (N.D. Ga. Feb. 21, 2006) (adopting the factual findings in the Order and Report and Recommendation).

143. *Zamora*, 2005 U.S. Dist. LEXIS 40775, at *32.

144. *Zamora*, 2006 WL 418390, at *4.

145. *Id.*

146. *Id.* (citations omitted).

has been dismissed.[147] Likewise, the argument that a cell phone "with a small storage capacity may be searched without a warrant due to the volatile nature of the information stored, but that a search of a cell phone with a larger storage capacity would implicate a heightened expectation of privacy and thus would require a warrant" has also been dismissed.[148] In both *Young* and *Murphy*, the Fourth Circuit emphasized evidence preservation over privacy and noted the practical difficulties for an officer to ascertain whether text messages could automatically delete,[149] during which time the information therein could be permanently lost.[150] Trying to quantify what "large" storage capacity means "in any meaningful way" is "problematic," and "[i]t is unlikely that police officers would have any way of knowing whether the text messages and other information stored on a cell phone will be preserved or be automatically deleted simply by looking at the cell phone."[151] Instead, the need for preservation of evidence justified the officer's warrantless retrieval of the contents from the cell phones.[152]

b. *No evidence destruction risk.* In contrast, courts that have found no exigency asserted that the risk of destruction of evidence expired once the phone was in law enforcement's custody.[153] The Ohio Supreme Court declared, "Once the cell phone is in police custody, the state has satisfied its immediate interest in collecting and preserving evidence and can take

147. *See, e.g.*, United States v. Young, 278 F. App'x 242, 245 (4th Cir. 2008) ("Privacy rights in the phone are tempered by an arresting officer's need to preserve evidence. This need is an important law enforcement component of the rationale for permitting a search of a suspect incident to a valid arrest." (citation omitted)).

148. United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009).

149. *Young*, 278 F. App'x at 245.

150. *Murphy*, 552 F.3d at 411.

151. *Id.*; *see also* People v. Diaz, 244 P.3d 501, 508–09 (Cal. 2011) (rejecting a "difficult" and "subjective" quantitative line-drawing approach for officers to follow in deciding the capacity of each particular cell phone in the field).

152. *Murphy*, 552 F.3d at 411; *Young*, 278 F. App'x at 245–46.

153. *See, e.g.*, United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *4 (S.D. Fla. Dec. 22, 2008), *aff'd*, 343 F. App'x 564 (11th Cir. 2009) (holding "the threat that messages would be destroyed was extinguished once law enforcement gained sole custody over the phones," thereby finding the warrantless search of cell phone unlawful because of the lack of any exigency that the text messages would have been destroyed absent the agent's intervention); State v. Todd, No. 23921, 2011 WL 1346864, at *9 (Ohio Ct. App. Apr. 8, 2011) (dismissing the imminent destruction of evidence within the cell phone argument, holding the warrantless search of data within the phone seized incident to arrest was thus prohibited by the Fourth Amendment).

preventive steps to ensure that the data found on the phone are neither lost nor erased."[154] Thus, although the court refused to consider the related state argument that the search of the cell phone was proper because cell phones have a finite memory and deleted records cannot be recovered, because the state had not raised the argument in the lower court,[155] it appears the court did not view this as an exigency.[156]

The Oregon Supreme Court likewise reiterated the trial court's skepticism of the state's argument "that the battery might run down and in order to power up the phone they may have to get a code from the phone's service provider" or "that the defendant, from jail, could provide certain information to the provider that may result in the provider . . . erasing information from the phone."[157] The court stated the following:

> The state offers no evidence that, even if the defendant had the information necessary and even if the service provider would accept a collect call from jail, that the service provider would not delay erasing information if a police agency called them and asked that they not do so while a search warrant was being obtained. In short, the state may have proven that it might be inconvenient for them to get a warrant and safeguard the contents of a cell phone but inconvenience falls short of exigent circumstances.[158]

Another court seemed to acknowledge a risk of evidence loss may exist, but the court did not view that risk as a justification to search. The *Nottoli* court, while not disputing the government's contention that information in cell phones may be lost, declared, "[T]he transitory nature of the contents of a cell phone found in a vehicle does not provide any additional authority to search a cell phone found in a vehicle."[159] The court emphasized that

> [t]he recognized governmental interest in preserving destructible evidence at the time of arrest relates only to the protection of evidence from an arrestee who might otherwise conceal or destroy such

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

155. *Id.*

156. *See id.* at 955–56 (noting even if the argument was to be considered at this level, the government did not provide evidence that other means to protect the data would be overcome by the asserted exigency).

157. State v. Nix, 237 P.3d 842, 848 (Or. Ct. App. 2010) (alteration in original).

158. *Id.*

159. People v. Nottoli, 130 Cal. Rptr. 3d 884, 907 (Ct. App. 2011).

> evidence. *Gant* expressly concluded that this interest is inapplicable when an arrestee cannot possibly access the vehicle.[160]

Thus, any government claim over the information dissipates once the arrestee is in custody.[161]

4. *Officer Safety*

Evidence destruction and officer safety, the fourth point in the five-point spectrum, are often paired as exigencies. Despite the prominence of officer safety as an exigency justifying the warrantless search incident to arrest generally,[162] courts have not raised officer safety as a basis for a cell phone search. The vast majority of cases simply state that neither the cell phone itself nor its contents pose a safety exigency to the officer.[163] Isolated cases have mentioned a possibility that a firearm may be disguised as a cell phone.[164]

Some courts, however, have taken a broader stance on safety exigency to include others besides the officer.[165] "[T]he original rationales for searches incident to arrest . . . were to remove weapons to ensure the safety of officers *and bystanders* . . . ."[166]

160. *Id.* (citing Arizona v. Gant, 129 S. Ct. 1710, 1718–19 (2009)).

161. *See id.*

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

163. *See, e.g.*, United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *3 (S.D. Fla. Dec. 22, 2008) ("The content of a text message on a cell phone presents no danger of physical harm to the arresting officers or others."); State v. Smith, 920 N.E.2d 949, 953 (Ohio 2009) ("[T]he search of the cell phone's contents was not conducted out of concern for the officer's safety.").

164. *See, e.g.*, United States v. Garcia-Aleman, No. 1:10-CR-29, 2010 WL 2635071, at *3 (E.D. Tex. June 9, 2010) (noting an officer placed a cell phone discovered during a pat down in the arrestee's vehicle as a precaution "because [the officer] had previously received safety information made available to officers regarding the discovery of firearms that resembled cellular telephones"); Fawdry v. State, 70 So. 3d 626, 627 (Fla. Dist. Ct. App. 2011) ("Based on prior instruction from his supervisors regarding the existence of firearms disguised as cell phones, [the officer] flipped open the cell phone to confirm that it was not a weapon.").

165. *See, e.g.*, United States v. Forker, 928 F.2d 365, 370 (11th Cir. 1991) (citing United States v. Satterfield, 743 F.2d 827, 843–44 (11th Cir. 1984)).

166. United States v. Park, No. CR 05-357SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007) (emphasis added) (citing *Chimel*, 395 U.S. 752). A close look at *Chimel*, however, finds an emphasis on the officer's safety.

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to

A vivid example is found in *Santillan*, which defined exigent circumstances as those likely to cause harm "to the officers *or other persons*, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."[167] The court held the search of the defendant's cell phone was justified by exigent circumstances[168] to preserve safety where the trucks were fleeing "at speeds approaching 100 miles per hour" in an apparent "attempt to escape back into Mexico"[169] and caused an individual on a bridge "to hang off the structure to avoid the fleeing trucks."[170] Civilians were in the area, school was in session nearby, and the vehicles "posed a danger to unsuspecting pedestrians and students."[171] "[T]his search was conducted expeditiously after a high speed chase, when suspects and danger still lurked; this was no mere wide-ranging investigatory search conducted at leisure by the officers."[172] "[T]he danger posed to the community was real and immediate. The agents had good reason to believe that the seizure of the phone might alleviate the danger to *the community and themselves*. The seizure of the cell phone was therefore justified."[173]

Similarly, where several officers reasonably believed that drug trafficking-related counter surveillance was being conducted in the immediate vicinity, the search of the recently recorded phone numbers in the cell phone retrieved from the arrestee's pants pocket was held to be justified by exigent circumstances.[174]

> use in order to resist arrest or effect his escape. Otherwise, *the officer's safety* might well be endangered . . . . In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person . . . [a]nd the area into which an arrestee might reach in order to grab a weapon . . . . A gun on a table or in a drawer in front of one who is arrested can be as *dangerous to the arresting officer* as one concealed in the clothing of the person arrested.

Chimel, 395 U.S. at 762–63 (emphasis added). The court did not seem to contemplate the safety of the general public at the moment of arrest. *See id.*

167. United States v. Santillan, 571 F. Supp. 2d 1093, 1103 (D. Ariz. 2008) (emphasis added) (quoting United States v. Brooks, 367 F.3d 1128, 1135 (9th Cir. 2004)).

168. *Id.* at 1101.

169. *Id.* at 1097–98.

170. *Id.* at 1101 n.3.

171. *Id.* at 1097–98.

172. *Id.* at 1103 n.6.

173. *Id.* at 1101 (emphasis added) (footnote omitted).

174. *See* United States v. Lottie, No. 3:07cr51RM, 2008 WL 150046, at *3

> Concern for officer safety and for the public in the midst of a large drug transaction entitled the officers to immediately search the cellular phone for recently recorded phone numbers in order to determine if the cell phone's limited memory revealed the participation of not only [the arrestee], but other unknown individuals involved in the drug transaction. The officers had reason to believe that [the arrestee] and others, unknown but potentially present and armed, were participants in the cocaine deal. In response to that exigency, the officers searched the call history of the cellular phone lawfully retrieved from [the arrestee].[175]

The possible presence of unknown, dangerous co-conspirators in their midst justified the cell phone search for the officer's and public's safety.[176]

5. *Expectation of Privacy*

The final point in the five-point spectrum of reasons for and against a warrantless search is the reasonable expectation of privacy in a cell phone.

a. *Expectation of privacy.* Courts that have found a reasonable expectation of privacy in cell phones point to the vastness of personal data a cell phone contains.[177] "[C]ell phones contain a wealth of private information, including emails, text messages, call histories, address books, and subscriber numbers."[178] As such, "[a] cell phone is similar to a personal computer that is carried on one's person . . . ."[179] Another state court of appeals agreed "the modern cell phone contains personal data in the same fashion as a computer; therefore, a cell phone owner's expectation of privacy does not differ from the expectation of privacy in the data stored in a computer."[180] The court followed its earlier state supreme court decision[181] holding a warrant must be obtained before

(N.D. Ind. Jan. 14, 2008).

175. *Id.* (citations omitted).

176. *Id.*

177. *See, e.g.*, State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) ("[Cell phones'] ability to store large amounts of private data gives their users a reasonable and justifiable expectation of a higher level of privacy in the information they contain.").

178. United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008).

179. *Id.*

180. State v. Isaac, No. 101,230, 2009 WL 1858754, at *4 (Kan. Ct. App. June 26, 2009).

181. *See id.* (citing State v. Rupnick, 125 P.3d 541 (Kan. 2005)).

conducting a search of a computer hard drive.[182]

The United States Supreme Court similarly presumed that an officer had a reasonable expectation of privacy in his employer-issued pager[183] when the audit revealed numerous sexually explicit text messages unrelated to police business,[184] notwithstanding the fact that this information necessarily was transmitted and stored by a third-party service provider.[185] "Cell 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. That might strengthen the case for an expectation of privacy."[186]

182. *Rupnick*, 125 P.3d at 550.

183. City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010), *rev'g* Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008).

184. *Id.* at 2625–26.

185. *See id.* at 2626. However, the Court held the city's review of the officer's text messages was reasonable and thus did not violate the Fourth Amendment because the search was motivated by a legitimate work-related purpose of determining whether the character limit on the city's contract with the wireless communications provider was sufficient to meet the city's needs. *Id.* at 2631.

186. *Id.* at 2630.

b. *No expectation of privacy*. Most courts that have held a warrantless cell phone search was reasonable did not extensively discuss the expectation of privacy. However, courts that addressed expectation of privacy—and held a warrantless cell phone search was reasonable—frequently pointed out the data at issue is transmitted via third-party servers and the user has no reasonable expectation of privacy in the information on a cell phone stored on third-party servers. The courts emphasize the voluntariness with which the information is given to the third-party server in order to transmit the message.[187]

Cell phone call logs have most easily fallen under the following rationale:[188]

> Traditionally, there has been no reasonable expectation of privacy in the numbers dialed on one's phone, since by voluntarily conveying numerical information to the telephone company and exposing that information to its equipment in the ordinary course of business, one loses any reasonable expectation of privacy in the existence and identity of such calls.[189]

When the defendant used his cell phone to place a call, he "'"exposed" that information to [the telephone company] in the ordinary course of business,' and therefore lost any reasonable expectation of privacy in the existence and identity of such calls."[190] There was no

187. Cases in which courts have found an expectation of privacy did not exist, and as such held that the arrestee's phone should not have been searched without a warrant, involve factually distinct situations and do not explicitly address the voluntary and knowing transmission of the data to a third party. State v. Isaac, No. 101,230, 2009 WL 1858754, at *1 (Kan. Ct. App. June 26, 2009) (finding that officers intercepting the detainee's phone call without his consent or court order was inadmissible); *see also* United States v. D'Andrea, 648 F.3d 1, 8 (1st Cir. 2011) (finding an evidentiary hearing should be held to decide if pictures obtained from a password-protected account would be admissible if the defendant through carelessness assumed the risk of disclosure); United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) (distinguishing a cell phone search from a routine driver's license check).

188. *See, e.g.*, Matthews v. Commonwealth, No. 2010-CA-001157-MR, 2011 WL 4862427, at *4 (Ky. Ct. App. Oct. 14, 2011) (citing Smith v. Maryland, 442 U.S. 735, 742–46 (1979)).

189. United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1276 (D. Kan. 2007) (citing *Smith*, 442 U.S. at 744 (holding there is no expectation of privacy in a pen register)).

190. Beckwith v. Erie Cnty. Water Auth., 413 F. Supp. 2d 214, 224 (W.D.N.Y. 2006) (quoting *Smith*, 442 U.S. at 744); *see also* United States v. Fierros-Alavarez, 547 F. Supp. 2d 1206, 1210–11 (D. Kan. 2008) (finding the defendant did not prove he had a

constitutional violation of the Fourth Amendment by the demand for the defendant's cell phone records because there was "no judicially recognized expectation of privacy in the telephone records."[191]

This logic also has encompassed e-mail to and from addresses and IP addresses of websites visited.[192] The Ninth Circuit analogized such information to information on the outside of physical mail or a telephone pen register—the surveillance of which does not constitute a search for Fourth Amendment purposes[193]—stating the technology for surveillance of e-mail may be more sophisticated but "is conceptually indistinguishable from government surveillance of physical mail."[194]

> [E]-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication. . . . Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. . . . [E]-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.[195]

The court in the recent *Nottoli* case rejected the expectation of privacy as a consideration in determining the scope of a search incident to

---

reasonable expectation of privacy in the call directory retrieved by the trooper from his cell phone following his arrest, because the information consisted only of addressing information).

191. *Beckwith*, 413 F. Supp. 2d at 223. One state supreme court recently found the defendant had an expectation of privacy in his cell phone, particularly his subscriber number, because the officers obtained the information from the defendant himself rather than the carrier. State v. Boyd, 992 A.2d 1071, 1082–83 (Conn. 2010). However, the facts of *Boyd* involved a warrant. *See id.* at 1076–77. The defendant's house was being searched pursuant to a warrant that included specifics, such as "computers, computer programs, [and] computer data," but it did not explicitly include a cell phone. *Id.* at 1077. As the defendant's apartment was being searched, another set of officers stopped the defendant in his car nearby as he was returning to his apartment. *Id.* The officers with the warrant went to the location where the defendant had been stopped, noticed the cell phone on the passenger seat of the car, and seized it. *Id.*

192. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).

193. *See id.* at 510–11.

194. *Id.* at 511.

195. *Id.* at 510 (citing *Smith*, 442 U.S. at 742, 744).

arrest.[196]

> [N]othing in Gant suggests that an arrestee's privacy expectations in particular objects affect the scope of vehicular searches incident to the arrest. As stated in *Belton*, "the justification for the search [incident to arrest] is not that the arrestee has no privacy interest in the container, but that the lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have."[197]

The court further noted, "The California Supreme Court recently observed in *People v. Diaz* that *Gant* 'reaffirmed *Belton*'s holding that whether a particular container may be searched does not depend on . . . the extent of the arrestee's expectation of privacy in it.'"[198] The *Diaz* court also rejected the argument that "the arrestee's expectation of privacy in its contents required courts to treat the arrestee's cell phone . . . differently from other types of personal effects or containers that may be validly searched incident to arrest."[199]

B. *Why the Traditional Models Fail*

Since *Chimel*, the judicial justifications for a search incident to arrest have been (1) to remove any weapons that could be used to resist arrest, effect escape, or that could endanger the officer's safety and (2) "to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction."[200] Only the need to ensure the officer's safety and preserve evidence comprises the classic *Chimel* duo of reasons justifying warrantless searches in the five-point spectrum.[201] Yet the five-point spectrum has developed by courts trying to accommodate cell phone technology and evolving uses.[202] The counterpoints are worthy and deserve consideration, but they fail to provide a coherent rule.

This Article does not challenge the notion that the cell phone is an item in which there is both a subjective and objective reasonable expectation of privacy. Instead, this Article discusses the ideal standards for a reasonable warrantless cell phone search incident to a valid custodial

196. People v. Nottoli, 130 Cal. Rptr. 3d 884, 906–07 (Ct. App. 2011) (quoting People v. Diaz, 244 P.3d 501 (2011)).

197. *Id.* at 906 (quoting New York v. Belton, 453 U.S. 454, 461 (1981)).

198. *Id.* (quoting *Diaz*, 244 P.3d 501).

199. *Id.* at 907 (citing *Diaz*, 244 P.3d 501).

200. Chimel v. California, 395 U.S. 752, 763 (1969).

201. *See id.*; *see also supra* Part II.B.

202. *See supra* Part III.A.

arrest. The following sections describe how cell phone technology has changed everyday communication and its value to law enforcement; and the inconsistencies and technological gaps in the five-point spectrum.

1. *Cell Phone Technology: How It Has Changed Everyday Communication and Its Value to Law Enforcement*

a. *Increasing reliance on cell phones and changes in the ways people communicate*. The cell phone arguably has become an omnipresent and potent force in American communication. "[Eighty-five percent] of Americans age 18 and older own a cell phone;"[203] of cell phone users, thirty-eight percent in America now carry a smart phone.[204] The early cell phone models are increasingly being replaced by smart phones with mobile operating systems, multimedia features such as a built-in camera for recording and transmitting photographs and short videos, and multiple connectivity possibilities, including the ability to transfer data to and from computers and other devices.[205] "A smart phone may be though of as a handheld computer integrated within a mobile telephone."[206] The operating system allows software applications, or "apps," to be installed into the smart phone's internal memory or microSD (SIM) card.[207]

The mobility and versatility of cell phones have caused people to become increasingly reliant on them. Most people do not feel compelled to take their laptops with them when they leave the house, yet most people would feel stranded and vulnerable if they were to leave the house without

203. *A Closer Look at Generations and Cell Phone Ownership*, PEW INTERNET, PEW RESEARCH CENTER (Feb. 3, 2011), http://www.pewinternet.org/Infographics/2011/Generations-and-cell-phones.aspx.

204. *In US, Smartphones Now Majority of New Cellphone Purchases*, NIELSENWIRE, (June 30, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/in-us-smartphones-now-majority-of-new-cellphone-purchases.

205. *See* William L. Hosch, *Smartphone*, BRITANNICA ONLINE ENCYCLOPEDIA, http://www.britannica.com/EBchecked/topic/1498102/smartphone (last visited Mar. 14, 2012).

206. *Id.*; *see also* Jenna Wortham, *Cellphones Now Used More for Data than for* Calls, N.Y. TIMES, May 13, 2010, at B1, *available at* http://www.nytimes.com/2010/05/14/technology/personaltech/14talk.html (detailing that an avid smartphone user rarely uses it to place phone calls compared to its other computer-like uses).

207. *See iPhone*, BRITANNICA ONLINE ENCYCLOPEDIA, http://www.britanica.com/EBchecked/topic/1326453/Iphone (last visited Mar. 14, 2012); *see also infra* note 367.

their cell phones. "For many Americans, cellphones have become irreplaceable tools to manage their lives and stay connected to the outside world, their families and networks of friends online."[208]

Increasingly, the cell phone is used not for its talking application, but for sending e-mail, text messages, browsing the Web, listening to music, and playing games.[209] The growth in voice minutes used by consumers has stagnated, while "[t]he number of text messages sent per user increased by nearly fifty percent nationwide [in 2009]."[210] The amount of data in text, e-mail messages, and other services on mobile devices has surpassed the amount of voice data in cell phone calls.[211]

b. *Value of information on cell phones to law enforcement.* The types of data a law enforcement officer may now expect or seek in an arrest has been transformed by the cell phone. The data on a cell phone holds great value to law enforcement,[212] particularly as the chosen communication medium trends more and more exclusively toward e-mail and text messaging and away from talking and written notes.[213] Whereas a phone call made on a traditional landline or a note scribbled on a piece of paper is transient or easily lost, cell phone use creates a record etched into the cell phone database until deleted, and this database is becoming increasingly vast. The "growing utility" of cell phones is like that of computers; it "may well cause individuals to structure more of their private lives" around such technology and it "creat[es] more physical evidence of

208. Wortham, *supra* note 206.

209. *Id.*

210. *Id.*; *see also CTIA-The Wireless Association® Announces Semi-Annual Wireless Industry Survey Results*, CTIA: THE WIRELESS ASSOCIATION® (Mar. 23, 2010), http://www.ctia.org/media/press/body.cfm/prid/1936.

211. *See* Wortham, *supra* note 206 ("'Originally, talking was the only cellphone application,' . . . '[b]ut now it's less than half of the traffic on mobile networks.'").

212. Bob Sullivan, *Gadget Gives Cops Quick Access to Cell Phone Data*, THE REDTAPE CHRONICLES ON MSNBC.COM (Apr. 20, 2011, 4:09 PM), http://redtape.msnbc.msn.com/_news/2011/04/20/6503253-gadget-gives-cops-quick-access-to-cell-phone-data ("Cell phone data is an indispensable tool in both investigations and prosecutions.").

213. *See* People v. Reese, No. C065511, 2011 WL 4347024, at *2 (Cal. Ct. App. Sept. 19, 2011) ("Officer Wilson also testified he was trained to understand 'computers, cell phones, that kind of stuff, are now where people keep items that . . . they would have kept in their briefcase, for example.'" (alteration in original)).

what they do from hour to hour."[214]

At the same time, criminals are attracted to the anonymity and difficulty of tracing disposable phones,[215] while smart phones, such as Apple iPhones, are also sought by drug dealers.[216] The cell phone's accessibility and prevalence have increasingly caused it to become the instrument of choice for criminals rather than the traditional computer. For example, one court noted that "[t]he records reveal an incriminating tapestry of cell phone calls which demonstrate how this method of communication has changed not only the way fraud can be perpetrated, but how it can be detected."[217] Cell phones, not computers or laptops, have been recognized as tools of the narcotics trade, used by traffickers to communicate and coordinate with their associates.[218] Traffickers, in fact, may have multiple cell phones.[219] Such cell phones "provide vital links in drug conspiracies and corroborating evidence of the surveillance conducted

214. Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 165–66 (2011).

215. *See* Beth Kampschror, *Cell Phones Ideal for Crime*, ORGANIZED CRIME AND CORRUPTION REPORTING PROJECT (Aug. 11, 2009), http://reportingproject.net/occrp/index.php/ccwatch/cc-watch-indepth/402-cell-phones-ideal-for-crime ("Disposable phones . . . are ideal for criminals. They can buy the phones anonymously, use them for a week or so and throw them away before police figure out the number, much less get authorization to tap the phones.").

216. *See Confessions of an Apple Store Employee*, POPULAR MECHANICS (Feb. 16, 2011, 6:30 AM), http://www.popularmechanics.com/technology/gadgets/news/confessions-of-an-apple-store-employee?click=main_sr (providing an employee's perspective on dealing with drug dealers as customers at an Apple store).

217. Cooper v. United States, 28 A.3d 1132, 1134 (D.C. 2011).

218. United States v. Slater, 971 F.2d 626, 637 (10th Cir. 1992) ("The search of his vehicle produced a large amount of cash, a semiautomatic pistol, and a cellular phone, each of which is a recognized tool of the trade in drug dealing." (citing United States v. Martinez, 938 F.2d 1078 (10th Cir. 1991))); United States v. Stringer, No. 10-05038-01-CR-SW-GAF2011, 2011 WL 3847026, at *9 (W.D. Mo. July 20, 2011) ("It should be noted . . . cell phones have been held by several circuits to constitute recognized tools of the drug trade." (citations omitted)); United States v. Davis, 787 F. Supp. 2d 1165, 1170–71 (D. Or. 2011) ("[C]ell phones provide the means for drug smugglers to coordinate efforts that could endanger officers and the public." (citation omitted)); People v. Nottoli, 130 Cal. Rptr. 3d 884, 906 (Ct. App. 2011) (receiving testimony that "drug users and sellers use cell phones as their 'main communication device'" and "cell phones can contain text messages related to acquiring and offering drugs").

219. *See, e.g.*, People v. Serrano, No. G043584, 2011 WL 3810214, at *1 (Cal. Ct. App. Aug. 29, 2011) (identifying an officer's suspicion that defendant was engaged in drug trafficking because he had multiple cell phones in his possession).

during the transaction."[220] Specifically, "the telephones often contain telephone numbers, contacts, and other information that would assist law enforcement in prosecuting those crimes."[221] Accordingly, there exists a "reasonable probability that information stored on the [cell phone] was 'evidence of *the arrestee's crime*.'"[222]

2. *The Five-Point Spectrum: Inconsistencies and Technological Gaps*

The first part of the discussion below summarizes the inconsistencies within each point as outlined in Part III.A. The latter part provides a comment on the point's relevance, if any, and perspective with which a rule should be approached given the technological realities.

a. *Container*. The courts that have held a cell phone is like any traditional container subject to a search incident to arrest reasoned any open or closed container found on the arrestee's person can be searched without a warrant pursuant to a valid custodial arrest.[223] These courts have hesitated to create a subjective, ad hoc approach in which the amount of personal information a particular item may contain determines whether it can be searched.[224] Instead, the reasoning is that the search of a cell phone, as with any other container, is reasonable because the lawful custodial arrest justifies the infringement of the privacy interest the arrestee may have had.[225] The courts have provided very little guidance as to whether a cell phone or only specific files or apps can be reasonably searched.

The courts that have held a cell phone is not a container have offered four main reasons. First, they noted the immense amount of private data a cell phone can carry, including the ability to link to the Internet.[226] Second, they are concerned the cell phone's outward appearance does not allow the observer to assess the wealth of the potential evidence its contents contain, which is akin to a personal computer.[227] Third, they point out the cell

220. United States v. Zamora, No. 1:05-CR-250-WSD, 2005 U.S. Dist. LEXIS 40775, at *31–32 (N.D. Ga. Dec. 7, 2005).

221. State v. Nix, 237 P.3d 842, 847 (Or. Ct. App. 2010).

222. United States v. Quintana, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2009) (quoting United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007)).

223. *See, e.g.*, *Finley*, 477 F.3d at 260 & n.7.

224. *See, e.g.*, People v. Diaz, 244 P.3d 501, 508–09 (Cal. 2011).

225. *Id.* at 507.

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

227. *See, e.g.*, State v. Isaac, No. 101,230, 2009 WL 1858754, at *4 (Kan. Ct.

phone is not a physical object capable of holding another physical object; thus, the phone cannot be analogized to other physical objects.[228] The final reason is that the container analogy cannot be found in the original framework and is irrelevant.[229]

There is no dispute that a traditional container such as a wallet or purse might hold an address book, mail, photos, or other searchable data; whereas a police officer might have come across some limited contacts, a note, letter, or a photo or two before the cell phone era, the capacity of today's cell phone allows an individual to carry around virtual file cabinets and megabyte photo albums. The vastness of the cell phone's memory does matter. The fact that data is in electronic rather than physical form and saved on a hard drive or memory card instead of a little black book means that rather than a cursory search—which is how the search-incident-to-arrest exception was originally intended[230]—the entirety of an individual's personal history could be laid bare. This immense scale of the virtual address book, mail, or photo album contained in cell phone data form—contact lists, e-mails, text messages, or photo log, for example—renders a search of this information more invasive than its physical corollary. In addition to the traditionally tangible items, cell phones can contain call logs, personal account information, privileged communications, and even "cloud" data—data accessible by links stored on third-party servers. The intrinsic nature of cell phone technology and society's increasing dependence on it create a vast and constant log of one's private life in a manner that did not formerly exist.

Moreover, the cell phone is an all-inclusive form of all data at all times. Unlike traditional tangible items, one does not select the relevant data on a cell phone to carry on a given day for a particular activity. Because of the cell phone's mobility and functions, the entire scope of the personal information on a cell phone is literally on the person[231] or within the grab zone[232] at all times. The information on a cell phone can even exceed that of a computer because of functions like text messaging which,

App. June 26, 2009) (citing State v. Rupnik, 125 P.3d 541, 552 (Kan. 2005)).

228. *See, e.g.*, State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009).

229. *See, e.g.*, *Diaz*, 244 P.2d at 510 n.14.

230. *See* United States v. Robinson, 414 U.S. 218, 234 (1973) (allowing the limited search of the person incident to arrest for safety purposes); Chimel v. California, 395 U.S. 752, 762–63 (1969) (providing the spatial limits on what an officer can search without a warrant to be reasonable in protecting his safety).

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

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

for a frequent user, can essentially track one's activities throughout the day. Moreover, a person's cell phone is unlikely to be stored in the trunk of a vehicle or a double-locked footlocker.[233] The criterion of finding an item physically of the person at the time of arrest does not meaningfully distinguish any set of data within the cell phone from another and provides no demarcation in the vastness of the cell phone's contents.

Even if "containerhood" is accepted as a valid criterion,[234] simply labeling the cell phone as a container cannot address the complexity of cell phone technology and reality of its use. This criterion arose from a tradition that did not anticipate and cannot accommodate the cell phone of today or the future.[235] The question of whether a cell phone is a container is akin to the question of when life begins because ultimately, neither the question nor the answer can resolve the issue of whether the cell phone can be searched incident to a custodial arrest and, if so, what the scope of that search should be. While the container doctrine works well for searches of tangible and finite items, forcibly applying the doctrine to cell phones in order to adhere to an analytic framework—created at a time when the modern cell phone did not exist—does not advance the dialogue. This Article proposes a rule for searching the cell phone, under defined circumstances, without requiring embroilment in the traditional container debate.

b. *Relatedness to reason for arrest.* Those courts that require the search to be related to the reason for arrest are concerned about law enforcement rummaging to discover incriminating evidence in the cell phone and bypassing the protections a warrant should afford.[236] Those courts that opposed such a requirement have pointed out that this rationale was not in the original *Chimel–Robinson* framework and adding it would create an extraneous criterion.[237]

The rule for relatedness to the reason for arrest has been stated in inconsistent variations. Sometimes, it is suggested the search should be related to the reason for arrest, regardless of the likelihood of actually finding relevant evidence;[238] other times, it is suggested the search should

233. *See* United States v. Chadwick, 433 U.S. 1, 4 (1977).
234. *See supra* Part III.A.1.
235. *See supra* Part III.A.
236. *See, e.g.*, Hawkins v. State, 704 S.E.2d 886, 892 & n.6 (Ga. Ct. App. 2010).
237. *See, e.g.*, Smallwood v. State, 61 So. 3d 448, 460 (Fla. Dist. Ct. App. 2011).
238. *See, e.g.*, People v. Nottoli, 130 Cal. Rptr. 3d 884, 902 (Ct. App. 2011).

be reasonably likely to yield evidence related to the reason for the arrest.[239]

In whatever variation the rule is offered and whatever the factual scenario, determining relatedness to the reason for the arrest will ultimately be a subjective, situation-specific assessment, despite the fact this criterion is intended to serve as a curb to law enforcement officer rummaging.[240] A search may unearth evidence that is indeed relevant to the reason for arrest, but the part of the phone searched may be obscure and the purported expectation of finding related evidence would thus be doubtful. On the other hand, an officer may search parts of the phone in which he or she reasonably expects to find relevant evidence and find nothing related to the reason for arrest and, instead, find evidence of a new crime. Can an officer now claim this evidence is in "plain view"?

This Article provides a rule that explains why and how the relatedness of the object of the search to the reason for arrest should matter for cell phone searches, taking these potential pitfalls and rummaging concerns into account.

c. *Need to preserve evidence*. The courts that have found cell phones present an evidence destruction exigency emphasize there is no way for the officer to know if the information on the phone can be deleted by incoming phone calls or remote wipe or deactivation and that evidence valuable to law enforcement may be permanently lost.[241] The courts that have found no exigency exists assert that the risk of destruction of evidence expires once the phone is in law enforcement's custody.[242]

In fact, the exigency of destruction of evidence because of limited storage capacity is a remnant of a bygone era. Cell phones today have the capacity to hold vast records of phone calls and other data, akin to a computer, simply by scrolling up or down the screen. The destruction of evidence rationale, with origins in the pager cases,[243] does not apply to the technology of the modern cell phone.

On the other hand, although courts have asserted the evidence

239. *See, e.g.*, United States v. McGhee, No. 8:09CR31, 2009 WL 2424104, at *3 (D. Neb. July 21, 2009).

240. *See Hawkins*, 704 S.E.2d at 892.

241. *See, e.g.*, United States v. Young, 278 F. App'x 242, 245–46 (4th Cir. 2008).

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

243. *See, e.g.*, United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996).

destruction risk expires once the cell phone is in police custody and reduced to their exclusive control, no court seems to have actually explained what preventive steps can be taken to ensure the data found on the phone is neither lost nor erased. Unlike the contents of the *Chadwick* footlocker, which would remain static and safely in place at the federal building,[244] cell phones are dynamic and can perform functions without human manipulation.

The relatively new threat of remote wipe or automatic deletion apps[245] that smart phones offer poses a particular challenge. The courts have proffered only conclusory findings about these threats, likely because the parties themselves did not understand the matter or offer evidence or an expert to testify.[246] Courts have been relegated to relying on the testimony of the parties, typically the law enforcement officer himself,[247] notwithstanding that such an individual might have had an agenda. It is this risk of remote wipe or automatic deletion that this Article will further investigate and address in the proposed rule, rather than assuming that simply seizing the phone and placing it in law enforcement's exclusive custody resolves evidence preservation concerns.

d. *Safety*. The physical cell phone cannot pose a threat of harm to the officer because the device cannot realistically be used as a weapon to assault an officer.[248] Nor has a situation arisen where the court has found that the contents pose an imminent threat to the officer's safety. Simply put, the harm to officer safety rationale is not meaningful in the context of the cell phone. However, where a threat existed to others besides the officer, because of an imminent or ongoing crime, a safety exigency may be found to justify a warrantless cell phone search.[249] It is in this context of the

244. *See* United States v. Chadwick, 433 U.S. 1, 4 (1977).

245. *See iPhone*, APPLE INC., http://www.apple.com/iphone/built-in-apps/find-my-iphone.html (last visited Feb. 29, 2012) (explaining that an iPhone owner can use "a remote wipe to restore it to its factory setting").

246. *See, e.g.*, United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *4 (S.D. Fla. Dec. 22, 2008) ("[T]here was limited testimony as to how cell phones store text messages, because neither the Government nor the Defendant called an expert in such matters to testify.").

247. *See, e.g.*, United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008) (stating the agent knew "call histories on cell phones could be deleted or lost, giving rise to a legitimate concern about destruction of evidence").

248. *See, e.g.*, *Wall*, No. 08-60016-CR, 2008 WL 5381412, at *3.

249. *See, e.g.*, United States v. Santillan, 571 F. Supp. 2d 1093, 1101 (D. Ariz. 2008).

safety exigency that this Article presents a rule.

e. *Expectation of privacy*. Those courts that have found a reasonable expectation of privacy in cell phones focus on the cell phone's computer-like storage capacity.[250] Those courts that have found no reasonable expectation of privacy in the cell phone emphasize the voluntariness with which users give the information to third-party servers in order to transmit the message.[251]

However, this purported "voluntariness" appears to be a convenient assumption made by some courts based on the reasoning applied to traditional technologies such as the land-based telephone[252] and mail.[253] Nor have the courts clearly addressed the expectation of privacy in information that is not on the third-party server, such as contact lists and photo logs. In the *Newhard* case, for example, the court equated the photo log, which is saved on the cell phone's memory, with "text messages and other information from a cell phone," which may require third-party transmission and may be stored on remote servers, as equally reasonable to search.[254]

This Article provides a rule that considers what role the method of transmitting or storing data may have on the expectation of privacy of data generally within the cell phone. The rule offers law enforcement specific guidelines in situations where a cell phone can be searched and limitations on the data that can be accessed.

C. *A Brief Review of the Current Literature*

The current literature has attempted to address some of these inconsistencies. Although distinctions certainly exist, the arguments can be described as falling into one or more of the following broad categories:

250. *See, e.g.*, United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008).

251. *See, e.g.*, Matthews v. Commonwealth, No. 2010-CA-001157-MR, 2011 WL 4862427, at *4 (Ky. Ct. App. Oct. 14, 2011) (citing Smith v. Maryland, 442 U.S. 735, 742–46 (1979)).

252. *See, e.g.*, United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1276 (D. Kan. 2007) (citation omitted).

253. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2007).

254. Newhard v. Borders, 649 F. Supp. 2d 440, 448 (W.D. Va. 2009) (relying on the Fourth Circuit's "approval of the retrieval of text messages and other information seized incident to an arrest").

Warrantless cell phone searches are unreasonable.[255]

Warrantless cell phone searches are constitutional if officers believe evidence of the crime of arrest will be found in the phone.[256]

The constitutionality of a warrantless cell phone search requires a consideration of the differing expectations of privacy regarding the multitude of data a cell phone presents.[257]

A number of unsatisfactory limitations have been imposed on warrantless cell phone searches generally, and now some limits need to be imposed.[258]

While various commentators have each offered a unique and valuable perspective to the dialogue on warrantless cell phone searches, the approaches tend to focus on one of the five points this Article has outlined. Instead of following these approaches, this Article first offers the recognition that such a five-point spectrum exists and subsequently proposes a "hybrid" approach, which weighs each of the five points and correlates with the cell phone's "hybrid" technology, its most common uses, and the value of that corresponding data to law enforcement.[259]

A review of the highlights from some of the relevant literature will be followed by a synopsis of the gaps and then the proposal.

1. *Warrantless Cell Phone Searches Are Unreasonable*

A large group of commentators assert that a warrantless cell phone search is unreasonable.[260] Some maintain the cell phone is a possession within the arrestee's immediate control, like the *Chadwick* footlocker or a computer or a laptop, in which there is a heightened expectation of privacy.[261] The cell phone's ability to hold large amounts of private data

255. *See infra* Part III.C.1.

256. *See infra* Part III.C.2.

257. *See infra* Part III.C.3.

258. *See infra* Part III.C.4.

259. *See infra* Part IV (outlining a proposal for the "hybrid" approach).

260. Ashley B. Snyder, Comment, *The Fourth Amendment and Warrantless Cell Phone Searches: When is Your Cell Phone Protected?*, 46 WAKE FOREST L. REV. 155, 180 (2011) (following the rationale of *State v. Smith* in arguing that warrants should be required to search the contents of a cell phone once seized by officers); *see, e.g.*, Bryan Andrew Stillwagon, Note, *Bringing an End to Warrantless Cell Phone Searches*, 42 GA. L. REV. 1165, 1206 (2008) (stating, absent certain exigent circumstances, a warrant should be procured prior to searching a cell phone).

261. *See, e.g.*, Byron Kish, Comment, *Cellphone Searches: Works Like a*

gives its users a higher expectation of privacy in the information it contains,[262] and a search should be prohibited once the cell phone is within the police's exclusive control.[263]

Another group argues that the container analogy does not work for cell phones.[264] One position maintains that the traditional twin rationales[265] cannot justify cell phone searches because the mere content of data on a cell phone presents no danger, the cell phone is incapable of carrying weapons, and once the officer has seized the phone, the arrestee can no longer reach the phone in order to destroy evidence.[266] Thus, once within the officer's exclusive control, the cell phone should require a warrant to be searched.[267]

Obtaining a warrant for searches of "mass storage devices, from laptops to portable hard drives to cell phones," would not be an overly burdensome requirement for law enforcement.[268] Unless an intrusion can

Computer, Protected Like a Pager?, 60 CATH. U. L. REV. 445, 471–72 (2011) (arguing a cell phone should be treated as a possession within the arrestee's control and should require a warrant to be searched); Justin M. Wolcott, Comment, *Are Smartphones Like Footlockers or Crumpled up Cigarette Packages? Applying the Search Incident to Arrest Doctrine to Smartphones in South Carolina Courts*, 61 S.C. L. REV. 843, 865–66 (2010) (suggesting courts take the approach from *Smith*, which focused on a justifiable expectation of privacy).

262. Wolcott, *supra* note 261, at 866 ("[T]he ability of modern cell phones and smartphones 'to store large amounts of private data gives their users a reasonable and justifiable expectation of a higher level of privacy in the information they contain.'" (quoting State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009))).

263. Kish, *supra* note 261, at 471 (citing Arizona v. Gant, 129 S. Ct. 1710, 1723–24 (2009)).

264. *See, e.g.*, 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, 1200 (2010) ("Lower courts have erroneously categorized cell phones as containers . . . ." (footnote omitted)); J. Patrick Warfield, Note, *Putting a Square Peg in a Round Hole: The Search-Incident-to-Arrest Exception and Cellular Phones*, 34 AM. J. TRIAL ADVOC. 165, 192 (2010) ("A cell phone is not a container; it holds too much information and has the ability to contain data that is both private and personal." (footnote omitted)).

265. *See* Chimel v. California, 395 U.S. 752, 762–63 (1969) (providing the rationales of officer safety and preventing destruction of evidence for search incident to arrest).

266. *See* Oxton, *supra* note 264, at 1208–10 (analyzing the rationales set forth in *Chimel* and reaffirmed in *Gant* to conclude neither safety nor evidence destruction are true threats in cell phone searches).

267. *Id.*

268. Andrew Wrona, Comment, *How Far Can the Automobile Exception Go?*

"reasonably be justified by purposes such as officer protection, evidence preservation, or arrestee containment, a simple seizure of the device must suffice until a warrant can be procured."[269] One such exception may arise "[i]n the unlikely situation that there is a truly exigent circumstance, like a life-threatening emergency that could possibly be remedied with information on the device."[270] Accordingly, courts should follow the lead of the Ohio Supreme Court and focus on the sufficiency of any exigent circumstances.[271] As a result, courts will likely be forced, in the near future, to confront the issue of remote-access wipe programs.[272]

2. *Warrantless Cell Phone Searches Are Constitutional if Officers Believe Evidence of the Crime of Arrest Will Be Found in the Phone*

Another group of commentators agrees with the premise that a cell phone should not be searched without a warrant for purposes of the Fourth Amendment.[273] Neither the justification of officer safety nor destruction of evidence should apply to cell phones.[274] "The only danger to officers posed by a cell phone is the ability of an arrestee to call for assistance from confederates," which is "highly improbable."[275] Cell phone memory capabilities vastly exceed that of pagers, and once the phone is seized, the suspect cannot delete crucial evidence anyway.[276] Officers can then secure

How Searches of Computers and Similar Devices Push It to the Limit, 43 J. MARSHALL L. REV. 1119, 1138–39 (2010).

269. Stillwagon, *supra* note 260, at 1206.

270. Wrona, *supra* note 268, at 1137.

271. Snyder, *supra* note 260, at 179–80.

272. *Id.*

273. *See, e.g.*, Jana L. Knott, Note, *Is There an App for That? Reexamining the Doctrine of Search Incident to Lawful Arrest in the Context of Cell Phones*, 35 OKLA. CITY U. L. REV. 445, 461–62 (2010) (noting one approach is to "allow officers to search a cell phone seized incident to lawful arrest only if the officers have reason to believe that evidence of the crime of arrest could be found in the cell phone"); Ben E. Stewart, Note, *Cell Phone Searches Incident to Arrest: A New Standard Based on* Arizona v. Gant, 99 KY. L.J. 579, 580–81 (2011) ("Cell phones, unsurprisingly carried on a person, should not be allowed to be searched incident to arrest without a warrant apart from circumstances unique to the particular arrest. These unique circumstances would be those in which there is reason to believe that evidence of the crime of arrest may be found in the cell phone.").

274. Knott, *supra* note 273, at 462–65; Stewart, *supra* note 273, at 593–94, 598–99.

275. Stewart, *supra* note 273, at 598 (footnote omitted).

276. *See* Knott, *supra* note 273, at 465 (arguing cell phone companies can help in preserving evidence, even though the phone is already in the possession of the police

a warrant before any information contained in the phone or the phone company's records are deleted.[277] The phone can even be turned off to prevent information deletion.[278] Instead, the search-incident-to-arrest exception should be guided by *Gant* and its focus on the officer's belief that evidence related to the reason for arrest will be found on the cell phone.[279] One commentator observes that this rule avoids creating a new rule while allowing adaptability to "ever-changing technology" because it leaves open the meaning of "reason to believe."[280] The commentator notes, however, that this standard has also been criticized since "it authorizes a search on less than probable cause."[281]

3. *The Constitutionality of a Warrantless Cell Phone Search Requires Considering the Differing Expectations of Privacy in the Multitude of Data a Cell Phone Presents*

Yet another group of commentators urges attention to the differences in the kinds of data on a cell phone, at least as a starting point.[282] "Coding information describes information that merely identifies the parties to a communication."[283] Content-based information is the substance of a communication itself.[284] "Not all information stored on a cellular phone is of the same ilk, because some stored items are far more private than others."[285] Further distinctions based on method of storage and what is visible to the user are important to understanding reasonable expectations of privacy in different kinds of data.[286] Content-based information is

officer); Stewart, *supra* note 273, at 594 (positing that a phone can be turned off once seized and the large amount of data stored will be preserved).

277. Knott, *supra* note 273, at 465.

278. Stewart, *supra* note 273, at 594.

279. *See* Knott, *supra* note 273, at 461–62; Stewart *supra* note 273, at 580–81.

280. Knott, *supra* note 273, at 477.

281. *Id.* at 472–73 (citing Edward J. Butterfoss, *Bright Line Breaking Point: Embracing Justice Scalia's Call for the Supreme Court to Abandon an Unreasonable Approach to Fourth Amendment Search and Seizure Law*, 82 TUL. L. REV. 77, 77 (2007)).

282. *See, e.g.*, Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 SANTA CLARA L. REV. 183, 187 (2010) ("[W]hen considering the legality of a search of a cellular phone's contents, it makes sense to consider . . . whether some information is the subject of a reasonable expectation of privacy while other information is not.").

283. *Id.* at 187.

284. *Id.* at 188.

285. *Id.* at 187.

286. *See* Daniel Zamani, Note, *There's an Amendment for That: A*

generally considered to receive more protection than coding information, with the dialed phone numbers captured by a pen register being a classic example of unprotected coding information.[287] Thus, the distinction between coding or content-based information can "help place a limit on what information the government can access."[288]

One common option for limiting information is to categorize the content within a cell phone and permit searches of only coding-based information,[289] or as another author calls it, data that is "on" or "in" the phone versus "data that is simply accessible via the" phone.

> [W]eb-based email accounts or other material that an individual accesses over the internet are not typically downloaded to the phone and are instead . . . simply floating around on electronic servers in cyberspace. Because such data is not physically present on the [cell phone] without proactively seeking it out, courts and legislatures could draw a line forbidding such searches incident to arrest while allowing police to search applications that have data permanently on the [cell phone].[290]

However, even coding information on a cell phone may be "deserving of much greater Fourth Amendment protection than it has heretofore received"[291] because, for example, a photograph stored only locally on one phone may be transmitted remotely to another party that may, in turn, be accompanied by coding information from the sender.[292] The demarcation between the types of information becomes "essentially artificial and may sometimes be quite blurry[,]" so "[c]ategorizing the data found on a smart phone both clarifies and confuses."[293]

The expectation of privacy in different sets of data within the phone

Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones, 38 HASTINGS CONST. L.Q. 169, 178 (2010) (distinguishing between data stored on the phone and data stored remotely, as well as visible and hidden data).

287. Orso, *supra* note 282, at 193–94; Zamani, *supra* note 286, at 178–79.

288. Orso, *supra* note 282, at 192–93.

289. *See* Zamani, *supra* note 286, at 178–79 ("Courts and commentators have generally concluded that content-based information ought to receive more protection than coding information.").

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

291. Zamani, *supra* note 286, at 181.

292. *See id.* at 179–80 (providing a hypothetical to explain a situation in which content-based and coding information would be present).

293. *Id.* at 197.

motivated a pair of commentators to urge limiting a warrantless search specifically to "call logs and text messages."[294] Searches of other features, "such as pictures, videos, and Internet browsing history, should be conducted only with a search warrant, as this type of evidence is afforded a higher expectation of privacy, is unlikely to be destroyed, and can be viewed at a later date or time."[295]

4. *A Number of Unsatisfactory Limitations Have Been Proposed Onto Warrantless Cell Phone Searches Generally, and Some Limits Need to Be Imposed*

The fourth group of commentators points out the muddled state of current Fourth Amendment jurisprudence and identifies several options.[296] In addition to the relatedness and content-coding options, one scholar suggested a compromise approach in which the search of the phone would be limited to "five levels deep" into the phone's contents but no further without a warrant.[297]

Ultimately, the commentators view all the suggested approaches as problematic, but it is suggested that "all are likely preferable to doing nothing and allowing police to search thousands of pages of electronic data without probable cause or a warrant."[298]

5. *Synopsis*

The cell phone is such a complex device that it is indeed difficult to create a standardized rule for its search without seeming to violate some

294. Jeffrey T. Wennar & Jamie Brinkmeyer Perry, *Cellular Telephones and the Fourth Amendment*, 6 CRIM. L. BRIEF 20, 22 (2011).

295. *Id.*

296. *See, e.g.*, Gershowitz, *supra* note 290, at 48–49 (explaining a possible change where officers may only search for "evidence of the crime for which the suspect was arrested"); Mark L. Mayakis, Comment, *Cell Phone—A "Weapon" of Mass Discretion*, 33 CAMPBELL L. REV. 151, 164–71 (2010) (outlining four different options concerning cell phones and the Fourth Amendment).

297. Gershowitz, *supra* note 290, at 55. Professor Gershowitz suggests:

> [P]olice could (1) turn on the phone; (2) open the internet browser; (3) type in a web-based email account such as www.hotmail.com; (4) log into the account (if the user id and password are saved); and (5) open a folder of messages. If the officer completes the fifth step without finding anything incriminating that could be destroyed, the officer would need to stop searching.

Id.

298. *Id.* at 58.

privacy expectation, contradict precedent, or both.

While the first group of commentators assumes the cell phone must fit in the traditional container analysis,[299] this Article proposes a rule that resolves this incongruous framework[300] by placing the cell phone in its own unique category of "hybrid." Additionally, the position many of these commentators share—that the risk of losing data is resolved by the cell phone being in law enforcement's exclusive control[301]—demands actual investigation into the technology to be substantiated. The second group of commentators focuses on the officer's belief that evidence related to the reason for arrest will be found on the cell phone, but this approach offers very little direction as to what types of arrests and what types of data may comprise a reasonable, related search.[302] The differing expectations of privacy in the cell phone's multitude of data present a demarcation that the third group of commentators suggests may help place a limit on access.[303] But this basic content-coding distinction should, however, be followed up with a more subtle consideration of the differing data's methods of transmission, access, and storage.

Rather than viewing the warrantless searchability of the cell phone through a convenient prism that focuses on one or more of the five points,[304] the proposed hybrid rule offered by this Article incorporates the spectrum of rationales and addresses concerns unresolved by the caselaw and the literature.

IV. PROPOSAL FOR A RULE THAT BALANCES THE FIVE-POINT SPECTRUM WITH MODERN TECHNOLOGY'S FOURTH AMENDMENT CHALLENGES: THE CELL PHONE AS HYBRID

The cell phone has replaced many traditional tangible items; yet, many of its functions are akin to a computer. Because the range of technological offerings and manner of use diverge from the dichotomy, a

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

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

301. *See supra* Part III.C.1.

302. *See supra* Part III.C.2.

303. *See supra* Part III.C.3.

304. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 688 (2011) ("[D]etermining reasonable expectations of privacy is challenging, at best, particularly in the context of new communications technology. Lower courts have tended to avoid conducting a full-scale expectations-of-privacy analysis by resorting to the same analytical short cuts that the government urged the Third Circuit to use. . . .").

cell phone should be treated neither as a traditional tangible item nor as a computer.

The genesis of the container concept was an interest in segregating items closely associated with the person from more distant possessions in which the arrestee cannot claim an expectation of privacy.[305] The hybrid category incorporates this tradition, which seeks to preserve privacy in items that should be protected, while accommodating and anticipating the incongruousness of current and unknown digital technologies.

Determining how to approach the search and seizure of a cell phone has ramifications for all such hybrid devices, notably touchscreen tablet computers such as iPads, in which supreme mobility is combined with computer technology, including Internet access, connectivity to multiple devices, and vast memory capacity.[306]

Any individual who is arrested would find the search of his cell phone objectionable, just as one would find the search of a purse, wallet, or jacket objectionable. Nonetheless, unless we accept that conversion into electronic form acts as a shield, the cell phone has replaced many of the tangible items formerly carried on one's person, and at least certain aspects of the phone must be allowed to be searched in accordance with the traditional justifications for the search-incident-to-arrest exception.[307] Thus, the question should not be whether the phone should be searched at all, but what aspects of the phone should be searched, and on what grounds.

This Article proposes a rule that protects the privacy rights embodied in the Fourth Amendment while remembering the origins of the search-incident-to-arrest exception. This rule is one law enforcement officers can uniformly apply to all cell phones, smart or not, and other hybrid devices. As the Ohio Supreme Court already observed, "[b]ecause basic cell phones in today's world have a wide variety of possible functions, it would not be helpful to create a rule that requires officers to discern the capabilities of a cell phone before acting accordingly."[308]

305. *See* United States v. Chadwick, 433 U.S. 1, 11, 14 (1977).

306. *See iPad*, APPLE INC., http://www.apple.com/ipad/features (last visited Mar. 14, 2012) (detailing features of iPad tablet computer, including lightweight design, retina display, camera, and Internet access).

307. *See* Chimel v. California, 395 U.S. 752, 763 (1969) (providing the twin rationales for search incident to arrest as recognized in *Robinson*).

308. State v. Smith, 902 N.E.2d 949, 954 (Ohio 2009).

The uniform rule should consider each point of the five-point spectrum that has emerged from the courts. It should provide both a bright-line rule that can be readily applied by officers in the field without making ad hoc, subjective judgments for each scenario,[309] yet it should allow officer discretion where an immediate safety concern demands it. The proposed rule satisfies each of these goals.

To wit: the expectation of privacy in the cell phone should be trumped by the search-incident-to-arrest exception when the search is reasonably expected to yield evidence related to the reason for arrest, but the search should be limited to specified data only. If an exigency exists that threatens the immediate safety of either the officer or others, then the officer may search additional data if the exigency is reasonably related to the need to search that additional data.

A. *Presumption Should Be Most Recent Text Messages, Call Logs, and E-mail Logs*

1. *Most Likely to Be Related to Reason for Arrest*

Limiting the warrantless cell phone search to data reasonably related to the reason for arrest and, more specifically, reasonably likely to yield evidence related to the reason for arrest, provides a fair and rational basis for distinguishing among a cell phone's immense data.

> Just because an officer has the authority to make a search of the data stored on a cell phone . . . does not mean that he has the authority to sift through *all* of the data stored on the phone . . . . Instead, his search must be limited as much as is reasonably practicable by the object of the search.[310]

Requiring relatedness prevents a law enforcement officer from searching a cell phone when an individual has been arrested, for example, for a minor traffic infraction in which no evidence could reasonably be expected to be found in the phone. The requirement also prevents an officer who pulls an individual over for a traffic violation, notices the smell of narcotics, and suspects drug trafficking, but is without probable cause,

309. *See* People v. Diaz, 244 P.3d 501, 509 (Cal. 2011) (refusing to adopt an "inherently subjective and highly fact specific" approach for officers).

310. Hawkins v. State, 704 S.E.2d 866, 891–92 (Ga. Ct. App. 2010) (citing United States v. Ross, 456 U.S. 798, 824 (1982)).

from immediately conducting a search of the phone in the hope of unearthing incriminating proof.

Justice Scalia, in his concurrence in *Thornton*, stated "[a] motorist may be arrested for a wide variety of offenses; in many cases, there is no reasonable basis to believe relevant evidence might be found in the car."[311] Similarly, there are a wide variety of offenses for which one may be arrested and in which there is no reasonable basis to believe that relevant evidence might be found in the cell phone. Hence, just as Justice Scalia would have held the search of Gant's jacket found in the backseat of the car unlawful "[b]ecause respondent was arrested for driving without a license (a crime for which no evidence could be expected to be found in the vehicle),"[312] a cell phone search should be found unlawful where no evidence of the reason for the arrest could be expected to be found in the cell phone.

Scalia's proposed rule "that a vehicle search incident to arrest is *ipso facto* 'reasonable' only when the object of the search is evidence of the crime for which the arrest was made, or of another crime that the officer has probable cause to believe occurred"[313] could arguably be translated as follows: "[A cell phone] search incident to arrest is *ipso facto* 'reasonable' only when the object of the search is evidence of the crime for which the arrest was made, or of another crime that the officer has probable cause to believe occurred."[314]

Specifically, if a warrantless cell phone search is indeed supported by the reason for arrest, the proposed rule is that the police may search *only* the *most recent* text messages, to and from e-mail addresses, and call logs.[315]

311. Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring).

312. Arizona v. Gant, 129 S. Ct. 1710, 1724–25 (2009) (Scalia, J., concurring).

313. *Id.* at 1725.

314. *See id.*

315. Certainly the term "most recent" can be subjectively interpreted and is subject to manipulation. Different time frames should be considered within the range of "most recent" for different arrests, and different cell phone technologies may present different quantities of information on each screen. In *United States v. Santillan*, the court pointed out that the cell phone "search was limited in scope, as agents accessed only the *recent* contacts," but the court did not define "recent." United States v. Santillan, 571 F. Supp. 2d 1093, 1104 (D. Ariz. 2008) (emphasis added). However, as a starting point, this Article suggests that once the officer views no more than two screens, with each screen likely holding several lines of data, the need for immediate inquiry will be satisfied.

It is in this data that, as a general matter, the presence of related evidence is most probable and the search can be limited to a reasonable intrusion. In a typical drug trafficking arrest, for example, a quick review of recent call logs, e-mails logs, and text messages can be expected to reveal evidence of related illegal activity in accordance with drug traffickers' preferred means of communication.[316]

A search limited to this data would create a bright line, if not perfect, rule that gives access to a clearly defined set of data that is most likely to yield evidence related to the reason for arrest. This rule would serve better than expecting an officer to decide which files or apps within one of numerous rapidly evolving cell phone models are most likely to yield evidence related to the reason for arrest. This can be complicated even if the officer is familiar with how to use the particular phone.

The officer's judgment, training, and experience, on the other hand, should be allowed a role. If the officer has probable cause for suspecting incriminating evidence beyond the recent text messages, e-mail logs, and call logs, the officer can obtain a warrant and search additional specified files, such as photo logs, contact lists, and Internet browser history.[317] Similarly, an officer with reason to suspect gang membership, for instance, can obtain a warrant to search photo logs for photos of the suspect with other gang members or with gang monikers and contact lists to show affiliation with the gang. An officer with reason to suspect child exploitation can obtain a warrant to search photo logs and Internet browser history.[318]

If there is no probable cause for obtaining a search warrant in the first place, then the officer's actions in searching through extraneous files incident to arrest would be exactly the kind of "'general rummaging in order to discover incriminating evidence'" the Fourth Amendment prohibits.[319]

316. *See supra* notes 215–20 and accompanying text.

317. *See* U.S. CONST. amend. IV ("[N]o 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.").

318. *See infra* Part IV.B.1 (discussing the safety exigency that may arise when the officer suspects the arrestee with minors in his actual presence is involved in ongoing crimes of child exploitation).

319. *See* United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) (quoting Florida v. Wells, 495 U.S. 1, 4 (1990)).

2. *Relevant and Limited Intrusion*

Limiting the search to the most recent text messages, call logs, and e-mail logs will also naturally limit what can be presumptively viewed because text messages tend to be brief and a scan of call and e-mail logs can quickly disclose the presence or absence of evidence related to the reason for arrest.

In contrast, other data within the phone can be difficult to limit in scope and is less likely to be immediately relevant. Contact lists and photo logs cannot be limited by the most recent activity and can be extensive; thus, they are harder for an officer to scan quickly. Also, while possibly pertinent to a drug trafficking charge, such information is more static. The same logic applies to Internet browser history. If there is probable cause to investigate the contact list, photo logs, or Internet browser history, a warrant can still be obtained and the phone can be searched pursuant to that warrant.

Gracie v. Alabama exemplifies this proposed rule.[320] There, the detective saw the suspect using the cell phone immediately after an armed robbery.[321] After arresting him, the detective searched the call logs and text messages to determine if the defendant had an accomplice, and in doing so, the detective observed incriminating information.[322] This cell phone search was limited to easily perusable information that was related to the specific reason for arrest.[323]

Based on the principle that the search should be relevant and limited, the *Newhard* search would have violated the Fourth Amendment.[324] There, the reason for arrest was completely unrelated to the sexually compromising photos found in the cell phone a police officer later distributed to others in the community "'for their viewing and enjoyment.'"[325] The court, which described this action as "'deplorable, reprehensible, and insensitive,'" resignedly held the cell phone search "did not violate any constitutional rights that were 'clearly established' at the

320. Gracie v. State, No. CR-10-0596, 2011 WL 6278304 (Ala. Crim. App. Dec. 16, 2011).

321. *Id.* at *1.

322. *Id.* at *2 (footnotes omitted).

323. *See id.* ("Detective Soronen then conducted a warrantless search of the call log and the text messages contained in Gracie's cellular telephone in order to find evidence of accomplice participation." (footnote omitted)).

324. *See* Newhard v. Borders, 649 F. Supp. 2d 440, 444 (W.D. Va. 2009).

325. *Id.*

time."[326] Under the proposed relevant and limited search principle, the court in *Newhard* could have found the search did violate clearly established constitutional rights, as the court in *Schlossberg v. Solesbee* would have.[327]

3. *Diminished Expectation of Privacy*

Individuals do not send text messages or make phone calls with a conscious awareness they are "giving" this information away and thereby relinquishing any claim of privacy they may have otherwise had.[328] Individuals have no choice but to rely upon third-party servers if they wish to be a cell phone using member of mainstream society. "[T]he premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[329]

Nonetheless, recognizing we cannot banish the entirety of a cell phone from the purviews of a search incident to arrest, we can accept that the expectation of privacy in communications made via third-party servers is, relative to other kinds of data within the cell phone, diminished. From the ubiquitous, recurring stories of political sex scandals unearthed by explicit text messages or photos on social-networking sites,[330] bullying

326. *Id.* at 450.

327. *See* Schlossberg v. Solesbee, No. 10-6014-TC, 2012 WL 141741, at *3–4 (D. Or. Jan. 18, 2012) (observing that "[s]earches such as the one conducted in *Newhard* do not fit within the Fourth Amendment Warrant Clauses's [sic] purpose of preventing unreasonable searches by law enforcement").

328. *See* Beckwith v. Erie Cnty. Water Auth., 413 F. Supp. 2d 214, 224 (W.D.N.Y. 2006) (finding plaintiff "lost any reasonable expectation of privacy in the existence and identity of [his] calls" when he used his cellular telephone because "he 'voluntarily conveyed numerical information to the telephone company,'" though he may not have realized it, (quoting Smith v. Maryland, 442 U.S. 735, 744 (1979))); *see also Smith*, 442 U.S. at 743–44 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." (citations omitted)).

329. United States v. Jones, No. 10-1259, slip op. at 5 (U.S. Jan. 23, 2012) (Sotomayor, J., concurring). Justice Sotomayor observed, "People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers." *Id.*

330. *See Top 10 Political Sex Scandals*, TIME, http://www.time.com/time/specials/2007/article/0,28804,1721111_1721210_1906894,00.html (last visited Mar. 14, 2012).

arising from teenage sexting,[331] and Facebook predation,[332] there is a general awareness that information in cyberspace is susceptible to viewing by a broad audience. The fact that some information is sent via third-party servers provides a distinguishing line in assessing privacy expectations on a cell phone. Text messages, call logs, and e-mail logs on cell phones are delivered via the service provider, just as the numbers dialed on a landline phone[333] and the outside of physical mail[334] are expected to be viewed by outside parties in order for the phone call to be made and the mail to be delivered.

Among these forms of data, text messages, though transmitted by a third-party server, can be considered more personal than e-mail logs and call logs because of the substantive nature of the communication. Even in *Quon*, which worked under the assumption that the officer had a reasonable expectation of privacy in his text messages, the Court nonetheless held the city's review of those messages on the city pager was reasonable.[335] The search-incident-to-arrest exception similarly should trump the arrestee's expectation of privacy in regard to the most recent text messages, in addition to the e-mail logs and call logs, as a standardized way of limiting the warrantless search. This rule provides a balance between law enforcement access to the relevant, most commonly used functions of the cell phone and the arrestee's privacy by protecting the more personal, and generally less relevant, data from a presumptive search. If the officer sees something in the to or from lines of the e-mail log, call log, or text messages that raises suspicions, the officer can still obtain a warrant and search more substantively later.

In contrast, the content of the e-mail, although transmitted through a third-party server, should be private; like the substance of a telephone conversation or the contents of sealed mail, the individual has a heightened expectation of privacy in the actual text of the substantive e-mail.[336] Often

331. *See* Michael Inbar, *'Sexting' Bullying Cited in Teen's Suicide*, MSNBC.COM (Dec. 2, 2009 10:26 AM), http://www.today.msnbc.msn.com/id/34236377/ns/today-today_people/t/sexting-bullying-cited-teens-suicide/#.T2TpObRFs15.

332. *See* Brad Stone, *New Scrutiny for Facebook Over Predators*, N.Y. TIMES (July 30, 2007), http://www.nytimes.com/2007/07/30/business/media/30facebook.html.

333. *See* United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1276 (D. Kan. 2007) (citing *Smith*, 442 U.S. at 744).

334. *See* United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2002).

335. City of Ontario v. Quon, 130 S. Ct. 2619, 2631 (2010), *rev'g* Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008).

336. *See Forrester*, 512 F.3d at 510–11.

a recipient must click on the e-mail icon, then the e-mail inbox and, finally, select the specific e-mail received in order to read its substance, which is akin to opening a sealed envelope. Text messages, unlike e-mail, often do not require paring away this extra layer to view the substantive communication which can appear on the initial display screen along with the name of the sender. Moreover, any privileged communications the arrestee may have received, such as medical results or a communication from an attorney, are more likely to reside in e-mail, likely as an e-mail attachment—analogous to yet another envelope within a mailed package—rather than as a direct text message.

Photo logs and contact lists, on the other hand, may be saved only on the cell phone's individual memory. In those situations in which this information is only stored on the phone's individual memory, one may send a photo or contact information to another cell phone or computer, thereby altering its status from locally saved to cyber-transmitted; however, such an alteration requires an additional affirmative step that cannot be assumed. Unlike data that requires satellite technology to implement, photo logs and contact lists stored locally on a personal handset do not necessitate a third-party transmission and are not stored on a remote server. Accordingly, the presumption should be that this information has a higher expectation of privacy and should not be subjected to a warrantless search.

4. *What About Password Protection?*

The concept of password protection initially seems to pose a challenge to the argument that the expectation of privacy is diminished in data that requires third-party transmission. Besides *United States v. D'Andrea*—in which the government conceded, for purposes of the appeal, that defendants' privacy expectation in their password-protected online account "was, at least initially, reasonable"[337]—at least one other court has suggested there may be a higher expectation of privacy if the cell phone's contents are password protected.[338] Although "there are already a handful of cases where police have encountered password-protected phones,"[339] there seems to be no explicit discussion of whether an enhanced

337. United States v. D'Andrea, 648 F.3d 1, 6 (1st Cir. 2011).

338. *See Mercado-Nava*, 486 F. Supp. 2d at 1275 (considering that "[n]o evidence suggests that the contents of the phones were protected by a password").

339. Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1154 (2011).

expectation of privacy exists by virtue of the password.[340] While the *Chadwick* footlocker was deemed a possession with a higher expectation of privacy by virtue of being double-locked and thereby required a warrant to be searched,[341] that analysis does not seem to translate to protecting password-protected cell phones.[342] Professor Gershowitz noted that although a password may make searching the phone incident to arrest more difficult for police officers, it does not necessarily prevent them from attempting to decipher the password or obtaining it from the arrestee simply by asking.[343]

As cell phone use continues to increase and consumers become more technologically savvy, the use of passwords will undoubtedly grow. Perhaps in the near future, practically everyone will be using a password, making the existence of password protection meaningless when determining whether a particular individual has demonstrated a heightened expectation of privacy. Most individuals would probably strongly attest they have a privacy expectation in the contents of their cell phones, regardless of whether they actually implemented password-protection. Thus, the question inevitably returns to what information can reasonably be searched incident to a lawful custodial arrest notwithstanding that the information may be password-protected or that an officer might decipher or obtain it from the arrestee without violating the arrestee's *Miranda* rights. Again, the proposed rule is a search limited to text messages, e-mail logs, and call logs, which will provide the bright line that balances the need for law enforcement to perform their duties effectively with a citizen's right to privacy for information in their cell phone by permitting a limited search of the information that is most likely to be related to the reason for arrest, can be scanned quickly, and already exhibits a diminished expectation of privacy.

B. *Safety Exigency Only Permits Access to Other Data*

Exigent circumstances may justify a warrantless search. The only

340. *See id.* at 1153–54 (noting only two courts have had to determine whether individuals must turn over their passwords (footnote omitted)).

341. *See* United States v. Chadwick, 433 U.S. 1, 11, 13–14 n.8 (1977).

342. *See* Gershowitz, *supra* note 339.

343. *Id.* at 1149–50, 1154. Although "[i]n most cases, before requesting a cell-phone password, police should be obligated to read the arrestee his *Miranda* rights . . . failure to read the warnings will not result in suppression of any illegal evidence found on the cell phone because the fruit-of-the-poisonous-tree doctrine never applies to *Miranda* violations." *Id.* at 1130 (footnotes omitted).

exigency that justifies a search beyond the presumptive cell phone data immediately related to the reason for arrest is safety.[344]

1. *Safety*

Caselaw already establishes that when a safety exigency exists, the officer is not required to wait for a warrant to search the validly arrested arrestee and the area in his immediate control.[345] Conducting an expanded warrantless search of the arrestee's cell phone for the likely-infrequent safety exigency conforms to this standard. "Exigent circumstances arise when the inevitable delay incident to obtaining a warrant must give way to a need for immediate action."[346] Moreover, to justify the more expansive cell phone search, such a search—consistent with the search of the presumptively allowed data—should be limited to cell phone data that is reasonably related to the reason for the exigency.

The real question is what type of exigency may be posed that would justify a more expansive cell phone search. The danger of the phone is not in its use as an assault weapon or escape device but in the information within it and how it will be used to commit a crime.

Although when the exigency justification arises the focus has been on the safety of the officer, even the early *Chadwick* Court observed there was "no reason to believe that the footlocker contained explosives or other inherently dangerous items" in explaining why no exigency existed to permit an immediate search.[347] Had there instead been reason to believe the footlocker posed a threat of explosion or other harm to not only the officer but to the innocent public outside the train terminal, this threat would have weighed in favor of an immediate search.

This principle of protecting the safety of the general public and the officer should apply in cell phone cases to enable the officer to thwart or impede an ongoing or imminent crime, and to help produce consistent, equitable results in warrantless searches incident to arrest. A more

344. *See infra* Part IV.B.

345. *See, e.g.*, United States v. Forker, 928 F.2d 365, 370 (11th Cir. 1991) ("[A] delay in arresting the suspect creates risk to the police, to other persons in the motel where the suspect is staying, and to innocent passers-by. The police should be entitled to act without delay in order to defuse an inherently volatile situation before the danger materializes in the form of injury to persons . . . .").

346. *Id.* at 368 (citing United States v. Satterfield, 743 F.2d 827, 844 (11th Cir. 1984)).

347. United States v. Chadwick, 433 U.S. 1, 4 (1977).

deliberate consideration of the public's safety, in addition to the police officer's, is more consistent with both the letter and the spirit of the law than rigidly focusing only on the police officer's safety when cell phones themselves pose no real physical danger. The *Lottie*[348] and *Santillan*[349] courts aptly provided this broadened understanding of exigent circumstances as including both officer and public safety.

In the relatively infrequent situations where a safety exigency arises, the officer's training and experience must guide what additional data should reasonably be immediately accessed, such as photo logs and contact lists, in addition to the presumptive call log, e-mail log, and text messages, depending on the nature of the arrest and specific exigency.[350] Justice Scalia's concurring comments, though directed specifically to police officer safety, recognized the need for the officer's discretion in his observation that when safety "is at issue, officers should not have to make fine judgments in the heat of the moment."[351] He contrasted such an exigency to "a general evidence-gathering search, [in which] the state interests that might justify any overbreadth are far less compelling."[352]

One can imagine an extreme situation in which a police officer, suspecting the arrestee is a terrorist, decides to search the data in the cell phone more expansively and is able to avert an immediate command to detonate a bomb. Such a search beyond the presumptive call logs, e-mail logs, and text messages would be validated by the need to search the additional data as reasonably related to the safety exigency.

Similarly, in perhaps a less drastic scenario, an officer may develop probable cause to suspect an arrestee, who was initially detained for a traffic violation and who has a minor in the vehicle, is involved in a network of child exploitation so that the children's safety is immediately

348. United States v. Lottie, No. 3:07cr51RM, 2008 WL 150046, at *3 (N.D. Ind. Jan. 14, 2008) ("Concern for officer safety and for the public in the midst of a large drug transaction entitled the officers to immediately search the cellular phone . . . .").

349. United States v. Santillan, 571 F. Supp. 2d 1093, 1103 (D. Ariz. 2008) (stating a warrantless cell phone search may be necessary and justified to prevent physical harm to officers or others).

350. *See, e.g.*, *id.* at 1104 (holding the exigency justified the call log search); *Lottie*, 2008 WL 150046, at *3 (holding the exigency justified the search of the "recently recorded phone numbers"). In contrast, this Article proposes that call logs should be presumptively searchable if related to the reason for arrest.

351. Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring).

352. *Id.*

imperiled. Believing the cell phone was being used to transact the criminal activity, the officer may determine an immediate search of the arrestee's cell phone's photo logs is reasonably related to the exigency of the children's safety and necessary to halt or avert imminent harm. Rather than being a "general evidence-gathering search,"[353] such a search would be immediately justified to protect the safety of the minors.[354]

Conversely, the rule requiring a safety exigency to search beyond the presumptive data would have protected the teacher in *Newhard*, the case in which one officer searched and another officer distributed sexually explicit personal photos found on Newhard's cell phone that were unrelated to the reason for Newhard's arrest and posed no threat to anyone's safety.[355]

This rule, which allows officer discretion to search extended data in the cell phone that is reasonably related to the reason for the exigency, relieves the officer from having to make the restrictive "fine judgments in the heat of the moment" that Justice Scalia disfavors when immediate safety is threatened.[356] This rule also protects an arrestee from being subjected to an unlimited cell phone search unrelated to the reason for the arrest when no exigency exists.

2. *Evidence Destruction: Not an Exigency*

The threat of evidence destruction because of limited storage capacity on the cell phone as an exigency has previously been refuted in this Article.[357] The only other source of evidence destruction—by remote wipe or automatic deletion—cannot be considered an exigency.

From a practical standpoint, once the phone is seized and the individual is in custody, the danger of the individual manipulating the phone to delete incriminating evidence is nonexistent. The battery can also be removed or the phone can be powered down, thus eliminating the possibility of the phone receiving the signal needed to activate the remote wipe command, even if a signal could be sent.

353. *Id.*

354. *Cf.* United States v. Schuttpelz, No. 10-1846, 2012 WL 34376, at *4 (6th Cir. Jan. 9, 2012) (denying defendant's motion to suppress cell phone evidence in child exploitation case because the officer's search was undertaken in reasonable reliance on existing pre-*Gant* law at the time of the search).

355. Newhard v. Borders, 649 F. Supp. 2d 440, 444 (W.D. Va. 2009).

356. *See Thornton*, 541 U.S. at 632.

357. *See supra* Part III.B.2.c.

However, once the arrestee has been released, remote wipe poses a real risk of evidence destruction on the cell phone. Moreover, automatic deletion settings can delete text messages at regular intervals without any additional action by the arrestee. It is the very universality and unavoidability of these risks, however, that renders remote wipe and automatic deletion threats meaningless for assessing whether an exigency exists in a particular situation.

There are several ways to remote wipe, "such as installing apps on the handset, using a management console on the IT side, or signing up for a cloud-based service."[358] A remote wipe will reset the cell phone to factory default condition, deleting photos, applications, other personal data, and also "any data on any storage card that's inserted in the [cell] phone."[359] "After a remote device wipe has occurred, data recovery is very difficult," although some residual data may possibly be recovered using sophisticated tools.[360]

Once turned back on and again able to receive a signal, some phones can still receive a remote wipe command that may be waiting. "When a Wipe action is specified for a device, it stays active until the administrator specifies otherwise. This means that, after the initial remote wipe has been completed, the server continues to send a remote wipe directive if the same device ever tries to reconnect."[361] Thus, it is entirely possible—despite the officer's precautions in removing the cell phone's battery or powering down the cell phone and thinking such action will disable a potential remote wipe command while he obtains a warrant to conduct a further

358. Jamie Lendino, *Kill Your Phone Remotely*, PCMAG.COM (Sept. 11, 2009), http://www.pcmag.com/print_article2/0,1217,a=243990,00.asp?hidPrint=true.J.

359. *Understanding Remote Device Wipe*, MICROSOFT EXCHANGE SERVER, http://technet.microsoft.com/en-us/library/bb124591.aspx (last updated Nov. 24, 2009) (explaining the Microsoft Exchange Server 2010 remote device wipe feature).

360. *Id.*

361. MICROSOFT CORPORATION, STEP-BY-STEP GUIDE TO DEPLOYING MICROSOFT EXCHANGE SERVER 2003 SP2 MOBILE MESSAGING WITH WINDOWS MOBILE 5.0-BASED DEVICES 49 (2006), *available at* http://www.o2.co.uk/assets2/PRODImages/PDF/detaileddepolymentguide.pdf; *see also* Henrik Walther, *Exchange 2003 Mobile Messaging Part 3—Installing, Administering, and Using the Microsoft Exchange Server ActiveSync Web Administration Tool*, MSEXCHANGE.ORG (May 18, 2006), http://www.msexchange.org/tutorials/exchange-2003-mobile-messaging-part3.html ("When you initiate a remote wipe action, it will remain active until you cancel it . . . . [T]his means that the server will continue to send a remote wipe to a device (even though the device has been remotely wiped already), so remember to cancel the remote wipe action after a lost or stolen device has been recovered.").

search into the phone's contents—that when the officer powers the cell phone back up, warrant now in hand, the remote command will be triggered and the wipe will begin.[362]

On the iPhone and iPhone 3GS, the remote command "take[s] approximately one hour for each 8 GB of device capacity."[363] The iPhone 3GS has eight gigabytes (GB) of memory[364]; the iPhone 4S has sixteen, thirty-two, or sixty-four GB of memory.[365] Thus, the remote wipe could take place in as little as one hour.[366]

In the worst case scenario, if the remote wipe is effective and deletes all the incriminating data before the officer has a chance to search it, options that still remain for data retrieval include the memory card file system—sometimes called a "SIM card"[367]—third-party server, and the hard drive computer back-up.[368] Thus, in addition to powering down the phone, the law enforcement officer can remove the memory card on phones that have them[369] so that data on the card will not potentially be

362. *See supra* note 361.

363. APPLE INC., IPHONE OS: ENTERPRISE DEPLOYMENT GUIDE 9 (2d ed. 2010) [hereinafter DEPLOYMENT GUIDE], *available at* http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf. "Devices can also be configured to automatically initiate a wipe after several failed passcode attempts." *Id.*

364. *iPhone 3GS Tech Specs*, APPLE INC., http://www.apple.com/iphone/iphone-3gs/specs.html (last visited Mar. 25, 2012).

365. *iPhone 4S Tech Specs,* APPLE INC., http://www.apple.com/iphone/specs.html (last visited Mar. 25, 2012).

366. *See* DEPLOYMENT GUIDE*, supra* note 363, at 9 (providing eight GB of memory can be wiped in an hour, which is the memory available to an iPhone 3GS).

367. *See An Overview of SIM Cards*, AT&T WIRELESS SUPPORT, http://www.att.com/esupport/article.jsp?sid=kb64891&cv=820#fbid=8JGKYXVTZOC (last visited Feb. 28, 2012); Andrew Mikael, *Information on Cell Phone SIM Cards*, TECH TIPS, http://techtips.salon.com/information-cell-phone-sim-cards-4465.html (last visited Feb. 29, 2012) (indicating a SIM card stores information about the phone, such as telephone number and service provider connections as well as other personal information like contacts or call histories).

368. *See* Scott Knickelbine, *Can Information in a Lost Cell Be Retrieved for a New Phone?*, TECH TIPS, http://techtips.salon.com/can-information-lost-cell-retrieved-new-phone-1837.html (last visited Feb. 25, 2012) (indicating a cell phone can be restored from phone-specific applications on a computer, through Microsoft Outlook if synced, web databases, and even a SIM card backup device).

369. *See* Alexander Poirier, *Smartphones That Use SIM Cards*, TECH TIPS, http://techtips.salon.com/smartphones-use-sim-cards-4467.html (last visited Feb. 29, 2012) (explaining that cell phone carriers using "GSM technology" provide SIM cards, which include AT&T and T-Mobile as the largest American networks).

wiped along with the rest of the data on the phone.[370] Alternatively, the officer can obtain a warrant to search the third-party server, which stores the data in case any information is still recoverable. Finally, if an iPhone was wiped, for example, iTunes can be used "to restore it using the device's latest backup."[371] Of course, the possibility also exists that any data may very well have already been deleted by the individual who had been arrested and now is fearful of prosecution.

Automatic deletion settings allow a user to set the phone to delete text messages when a certain message limit has been reached or after a certain number of days.[372] Users can also install an app that will delete a text message after a specified time has elapsed or upon reading through "a 'delete on read' setting, which counts down from sixty after a message is opened and erases its text at zero."[373] As consumers, and criminals in particular, become more skillful in their use of smart phones, they will more frequently take advantage of the remote wipe or automatic deletion feature to banish incriminating data from their phones.

These are risks that as a society we may decide we are willing to accept because the alternative is unrestrained search of the cell phone. If the omnipresent risk of remote wipe or automatic deletion is considered an exigency that allows a warrantless search of any cell phone incident to arrest, then there could be no restrictions to law enforcement's ability to search all the contents of the cell phone incident to arrest because this risk is constant and not unique to any particular situation. Such risk of evidence destruction cannot be a basis for warrantless cell phone searches. An exception may exist in the unlikely scenario "where an officer had credible information that a suspect's accomplice was at a remote location

370. *See supra* text accompanying note 359.

371. *See* DEPLOYMENT GUIDE, *supra* note 363, at 9 (providing for backup of device in encrypted format through iTunes, which is recoverable even when device is remotely wiped).

372. *See, e.g.*, BLACKBERRY, BLACKBERRY TORCH 9800 SMARTPHONE USER GUIDE 96 (2011), *available at* http://docs.blackberry.com/en/smartphone_users/deliverables/18579/BlackBerry_Torch_9800_Smartphone-User_Guide-T643442-941426-0810050917-001-6.0-US.pdf (providing advice on how to store messages to a card, block messages, or even set how long messages should be kept); GOOGLE, ANDROID 2.3.4 USER'S GUIDE 236 (2011), *available at* http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/help/hc/pdfs/mobile/AndroidUsersGuide-2.3.4.pdf (explaining how to change message settings, including deletion and message limit settings).

373. Belinda Luscombe, *TigerText: an iPhone App for Cheating Spouses*, TIME (Feb. 26, 2010), http://www.time.com/time/printout/0,8816,1968233,00.html.

and was planning to use [a] remote-wipe program."[374]

Thus, the proposed rule is restated as follows: law enforcement officers may search the contents of a cell phone seized incident to a valid custodial arrest if the contents are reasonably likely to yield evidence related to arrest, with a presumption that text messages, e-mail logs, and call logs are searchable. Law enforcement officers may search other reasonably related contents when an exigency exists regarding safety.

V. CONCLUSION

The rule this Article proposes helps to minimize the problem posed by the plain-view exception to the warrant requirement. It is easy to imagine that an officer may swipe, inadvertently or not, another icon, thereby unearthing a trove of information relating to a new crime—for example, child exploitation or distribution of controlled substances—that is now suddenly in plain view and may have been completely unrelated to the reason for the arrest. The government may now claim the "contents are in plain view and, if incriminating, the government can keep it."[375] To resolve this, the Ninth Circuit required that the government must "forswear reliance on the plain view doctrine" when the data was accessed only "because it was required to segregate seizable from non-seizable data."[376] Knott suggests the government could analogously "be required to waive use of the plain-view doctrine before conducting a search of the cell phone incident to a suspect's lawful arrest."[377] However, under the rule proposed in this Article, there is no need to "segregate" data because the data the officer can reasonably search has already been defined.

A more modern Pandora's box may be the growing prevalence of cloud computing, where information is stored on a third-party server rather than a local hard drive, presenting a twist to the dichotomy of locally saved information versus information on third-party servers.[378] For example, in June 2011, Microsoft rolled out Office 365, its online version of Microsoft

374. Schlossberg v. Solesbee, No. 10-6014-TC, 2012 WL 141741, at *4 n.3 (D. Or. Jan. 18, 2012).

375. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1004–05 (9th Cir. 2009).

376. *Id.* at 998.

377. Knott, *supra* note 273, at 478.

378. *See* Eric Knorr & Galen Gruman, *What Cloud Computing Really Means*, INFOWORLD, http://infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031?page=0,0 (last visited Feb. 28, 2012) (discussing the various forms of cloud computing, including storage services).

Office,[379] which allowed businesses to move their software "residing on local computers to remote data centers accessible from anywhere."[380] Apple's version of iCloud was launched in June 2011 as well.[381] Information that had been saved only on a hard drive may now be saved on remote servers that push the information to all one's devices automatically. It cannot be said that information once stored by cloud computing suddenly loses its Fourth Amendment protection and is subject to a warrantless search. The rule for a reasonable search proposed by this Article would not be undermined by the trend towards cloud computing.

The hope is that the rule the United States Supreme Court eventually adopts will put to rest the rather insidious-sounding "Universal Forensic Extraction Device" made by CelleBrite, which is in use by at least one police department.[382] A U.S. Department of Justice test of the device found it "could grab all of the photos and video off of an iPhone within one-and-a-half minutes. The device works with 3,000 different phone models and can even defeat password protections."[383] The device thus seems to copy faster than remote wipe can delete.[384] The ACLU has been trying to discover whether the state police are violating the privacy of individuals with this new, sophisticated technology.[385] If the Supreme Court adopts the rule proposed by this Article, then the answer is yes.

As technology continues to hurtle forward, the law also needs to move forward to ensure a balance between the individual and law enforcement. A rule governing cell phone searches must prevent either of

379. *What is Office 365?*, MICROSOFT OFFICE 365, http://www.microsoft.com/en-us/office365/what-is-office365.aspx (last visited Mar. 18, 2012).

380. David Sarno, *Microsoft Rolls Out Office 365 in Cloud Computing Race*, L.A. TIMES (June 29, 2011), http://articles.latimes.com/2011/jun/29/business/la-fi-microsoft-cloud-20110629.

381. *iCloud: What You Need to Know*, MACWORLD (June 8, 2011, 8:45 AM), http://www.macworld.com/article/160380/2011/06/icloud_what_you_need_to_know.html ("When Steve Jobs spoke about iCloud, he said that Apple was going to demote the computer to be 'just another device.' So, rather than your Mac being the digital hub for your media and personal information, that job would be taken over by online services—specifically, iCloud. Given that now that many of us have not only multiple computers but also one or more mobile computing devices such as the iPhone, iPod touch, and iPad, this makes a lot of sense.").

382. Sullivan, *supra* note 212.

383. *Michigan: Police Search Cell Phones During Traffic Stops*, THE NEWSPAPER.COM (Apr. 19, 2011), http://thenewspaper.com/news/34/3458.asp.

384. *See supra* text accompanying notes 363–66.

385. *See* Sullivan, *supra* note 212.

two extremes: widespread invasions of individual privacy for any arrest or unduly tying the hands of law enforcement officers. As citizens, while we do not wish law enforcement to have the ability to search our cell phones for merely rolling through a stop sign, we also do not wish law enforcement to be barred from searching relevant data within the cell phone of an arrestee whom the officer suspects poses an immediate threat to the public's safety. Given the rapidly evolving technology and the corresponding impact on society's behavior, attitudes, and expectations, whatever rule is established may need to be revisited in the future. This Article is part of the ongoing dialogue until the United States Supreme Court provides the working rule that is now needed on the issue of warrantless cell phone searches incident to arrest.