CALLING FOR A STANDARD: WHY COURTS SHOULD APPLY A NEW BALANCING TEST IN CELL PHONE SEARCHES INCIDENT TO ARREST

Drew Liming*

You have just been stopped for driving with a revoked license. A police officer asks that you step out of your car and hand over your cell phone. When you comply, the officer scrolls through your personal information. First she looks at your recently called numbers. Then she accesses the names and phone numbers of your contacts. Finally, she begins browsing through your photographs.

The officer's search of your cell phone likely seems excessive because the cell phone has nothing to do with the validity of your license. However, such an intrusion would frequently be permitted under the search incident to arrest exception to the warrant requirement of the Fourth Amendment.[1]

But now consider a different scenario: officers arrest a major drug kingpin after witnessing the kingpin using his cell phone to show photos, which the officers suspect depicted drugs, to an associate. When arresting the kingpin, officers seize but do not search his cell phone. By the time they procure a warrant to search the phone, the officers find that it has been reset to factory settings; they suspect that another associate of the arrestee remotely erased the phone's hard drive. The suspected drug photos, which would have served as key evidence against the kingpin at trial, are lost. In this case, allowing officers to search the cell phone at the time of the arrest might have been an effective policy.

These different scenarios demonstrate that what could seem excessive in some circumstances might seem necessary in others. This calculation will continue to change as technology develops and more information is stored on or accessed through cell phones. As the scenarios indicate, deciding whether a particular cell phone should be searchable incident to arrest turns on the reasonableness of an officer's search and the arrestee's expectation of privacy in the information stored on the phone.

Courts have struggled to apply the search incident to arrest exception to cell phone searches. Many Circuits have allowed law enforcement officers to search

---

* Georgetown University Law Center, J.D. expected 2015; University of Virginia, B.A. 2007. The author wishes to thank the ACLR Staff, Martha Stansell-Gamm, and Jessica Finkel for their comments and review.

1. *See, e.g.*, United States v. Robinson, 414 U.S. 218, 236 (1973) (holding that a suspect arrested for driving with a revoked license could be searched incident to arrest); Evans v. Solomon, 681 F. Supp. 2d 233, 248–49 (E.D.N.Y. 2010) (holding that a search of a suspect stopped for a traffic violation was legitimate because probable cause to arrest existed at the time of the search and the search was valid as a search incident to arrest).

cell phones incident to arrest if the searches were conducted at or shortly after the time of arrest and the arrestee's phone was on his person.[2] However, other jurisdictions have held that cell phones cannot be searched without a warrant.[3] As cell phone searches are now a common investigatory tool, the U.S. Department of Justice has asked the Supreme Court to resolve this Circuit split and provide clear guidance to courts and law enforcement about when such searches are permitted.[4] In the wake of the Circuit split, this Note will argue that the Supreme Court should adopt a balancing test because cell phone technology develops too swiftly to be governed by a bright-line rule. Only a balancing test properly accommodates both the relevant privacy concerns and the needs of law enforcement.

Part I of this Note provides background on the search incident to arrest exception to the Fourth Amendment. Part II analyzes the history of cell phone searches and many of the rationales courts have used in permitting or prohibiting warrantless searches of cell phones incident to arrest. Part III suggests how the Supreme Court should resolve the issue of warrantless cell phone searches and explains why a balancing test would be the best option for a rapidly developing technology like cell phones.

I. HISTORY OF THE SEARCH INCIDENT TO ARREST EXCEPTION

The Fourth Amendment protects the right to be secure "against unreasonable searches and seizures."[5] In most situations, law enforcement officers must either procure a warrant or demonstrate probable cause sufficient to attain a warrant before proceeding with a search or seizure. However, there are a number of exceptions to the warrant requirement.[6]

One prominent exception pertains to searches incident to arrest, which were first mentioned by the Court in dictum in 1914.[7] In *Weeks v. United States*, the Court indicated that English and American law had always recognized the ability of police officers to search the person of a legally arrested suspect.[8]

---

2. *See, e.g.*, United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009); United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007); *see also* People v. Diaz, 244 P.3d 501, 511 (Cal. 2011).

3. *See, e.g.*, United States v. Wurie, 728 F.3d 1, 14 (1st Cir. 2013); Smallwood v. State, 113 So. 3d 724, 738 (Fla. 2013); State v. Smith, 920 N.E.2d 949, 956 (Ohio 2009).

4. Petition for Writ of Certiorari, United States v. Wurie, No. 13-212 (S. Ct. Aug. 15, 2013), 2013 WL 2129119, *cert. granted*, 134 S. Ct. 999 (2014).

5. U.S. CONST. amend. IV.

6. These exceptions include, among others, plain view, consent, and exigencies. *See generally* WAYNE R. LAFAVE, SEARCH AND SEIZURE (5th ed. 2012).

7. *See* Weeks v. United States, 232 U.S. 383, 392 (1914).

8. *Id.* ("It is not an assertion of the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime.").

The Supreme Court clarified the search incident to arrest doctrine in *Chimel v. California*.[9] In *Chimel*, officers asked a burglary suspect for permission to search his house when they served him with an arrest warrant.[10] Although the suspect denied their request, the officers proceeded to search his entire house, including the attic and garage, and found evidence of burglary.[11] After the trial court admitted the evidence and its decision was affirmed by the California Supreme Court, the suspect appealed to the United States Supreme Court, claiming the search violated his Fourth Amendment rights.[12]

The Supreme Court held that the officers had no justification for searching the suspect's house absent a warrant.[13] However, the Court also indicated that it was reasonable for police officers, upon making an arrest, to conduct a warrantless search of an arrestee's person and the area "within his immediate control."[14] Such searches were justified in order to prevent the arrestee from destroying evidence or to discover if the arrestee had any weapons that could threaten the safety of the arresting officers.[15]

The Court expanded the search incident to arrest exception in *United States v. Robinson*.[16] In *Robinson*, officers arrested the suspect for driving a car with a revoked license.[17] When the officer conducted a search incident to arrest, he pulled a crumpled cigarette package out of the suspect's coat pocket.[18] The officer opened the package and found capsules of what he believed—and later confirmed—to be heroin.[19] When the suspect challenged the admission of the heroin into evidence at his trial, the Court ruled that warrantless search or seizure of objects on the person of an arrested suspect is reasonable under the Fourth Amendment.[20] The Court stated that the long history of searches incident to arrest indicted that this practice does not require "such a case-by-case adjudication," and that after a lawful arrest, a search incident to arrest that examines the suspect's person "requires no additional justification."[21] In *Robinson*, the Court established a bright-line rule that officers may seize and search any item or container—open or closed—on the person of the arrested suspect when conducting a search incident to arrest.[22]

---

9. 395 U.S. 752, 772–73 (1969).
10. *Id.* at 753.
11. *Id.* at 753–54.
12. *Id.* at 754–55.
13. *Id.* at 768.
14. *Id.* at 762–63.
15. *Id.* at 763.
16. 414 U.S. 218, 235 (1973).
17. *Id.* at 220.
18. *Id.* at 221–23.
19. *Id.* at 223.
20. *Id.* at 236–37.
21. *Id.* at 235.
22. *Id.*

After *Robinson*, the courts slowly expanded the search incident to arrest doctrine and created bright-line rules permitting searches in areas other than on an arrested suspect's person, such as inside the passenger compartment of automobiles.[23] Police officers have frequently used the expanding search incident to arrest exception in investigations and arrests.[24]

However, use of the search incident to arrest exception changed dramatically in 2009 after the Supreme Court's decision in *Arizona v. Gant*.[25] In *Gant*, police arrested a suspect for driving with a suspended license.[26] After officers restrained Gant and put him in the back of a patrol car, they searched his car's back seat, where they found a bag of cocaine in the pocket of a jacket.[27] When Gant argued that this evidence should be suppressed because the search violated his Fourth Amendment rights, the Court agreed with the Arizona Supreme Court that the officers could not justify their search under either of the *Chimel* rationales permitting searches incident to arrest.[28] Because the officers had already locked Gant in their patrol car when the search took place, they had no reason to suspect that there was a risk of evidence being destroyed or a threat to their safety.[29] The Court explained that officers "may search a vehicle incident to a recent occupant's arrest only if the arrestee is within reaching distance of the passenger compartment at the time of the search or it is reasonable to believe the vehicle contains evidence of the offense of arrest."[30] Barring these circumstances, officers need a warrant or another exception to the warrant requirement to search an arrestee's vehicle.[31]

Since *Gant* was decided, however, lower courts have differed on how to apply the new search incident to arrest rule.[32] Some have limited the holding of *Gant* to searches incident to arrest involving vehicles.[33] Other courts have read *Gant* as a reaffirmation of the *Chimel* rationales and have held that all searches incident to arrest should be subject to the same requirements.[34] Reconciling *Chimel*, *Robin-*

---

23. *See* Thornton v. United States, 541 U.S. 615, 623 (2004) (holding that the passenger compartment of the vehicle of an arrestee may be searched incident to arrest); New York v. Belton, 453 U.S. 454, 462–63 (1981) (holding that officers may search a container in the vehicle of an arrestee incident to arrest).

24. *See, e.g.*, United States v. Osife, 398 F.3d 1143, 1146–47 (9th Cir. 2005) (holding that officers could search a truck incident to arrest after the driver was arrested for public urination); Brown v. State, 24 So. 3d 671, 677 (Fla. Dist. Ct. App. 2009) (holding that an officer could search a car incident to arrest after the driver was arrested for outstanding warrants).

25. 556 U.S. 332 (2009).

26. *Id.* at 336.

27. *Id.*

28. *Id.* at 337–38.

29. *Id.* at 344.

30. *Id.* at 351.

31. *Id.*

32. *Compare* United States v. Brewer, 624 F.3d 900, 905–06 (8th Cir. 2010) (interpreting *Gant* as applying only to searches of vehicles), *with* United States v. Shakir, 616 F.3d 315, 318 (3d Cir. 2010) (interpreting *Gant* as applying to searches incident to arrest more generally).

33. *See, e.g.*, *Brewer*, 624 F.3d at 905–06; United States v. Perdoma, 621 F.3d 745, 751–52 (8th Cir. 2010).

34. *See, e.g.*, *Shakir*, 616 F.3d at 318; United States v. Gordon, 895 F. Supp. 2d 1011, 1019 (D. Haw. 2012).

son, and *Gant* and applying them to searches incident to arrest of highly sophisticated smartphones has resulted in courts reaching wildly different conclusions as to whether the Fourth Amendment permits warrantless searches of cell phones.

II. RATIONALES FOR AND AGAINST CELL PHONE SEARCHES INCIDENT TO ARREST

Many courts that have considered searches of cell phones incident to arrest have held that the searches did not violate the Fourth Amendment when the phone was on the arrestee's person at the time of arrest.[35] However, in several cases, courts have held that police officers violated arrestees' Fourth Amendment rights by searching cell phones without a warrant.[36] And recently, in *United States v. Wurie*, the First Circuit established a bright-line rule that searches of cell phones never fall within the search incident to arrest exception to the warrant requirement.[37] In light of the difficulty of applying existing legal principles to new technologies, courts have considered a variety of arguments when deciding if a cell phone search was legitimate: (A) whether cell phone searches are permitted under the *Chimel* rationales; (B) whether cell phones are analogous to containers found on an arrestee's person; (C) whether cell phones are analogous to pagers; (D) whether the quantity and personal nature of information stored on cell phones creates a heightened expectation of privacy that requires unique analysis; and (E) whether *Gant* applies to searches of cell phones. None of these arguments has produced consistent results. For each rationale, courts have split on whether it permits searches incident to arrest.

A. Cell Phone Searches can be Justified by the Chimel *Rationales*

In deciding the legality of cell phone searches, some courts have applied the *Chimel v. California* rationales, which would allow cell phone searches incident to arrest if the purpose of the searches was to protect officer safety or preserve destructible evidence.[38] In *United States v. Flores-Lopez*, the Seventh Circuit briefly considered the possibility that officers might need to seize a cell phone to protect officer safety because what appears to be a cell phone could actually be a stun gun in disguise.[39] However, the Seventh Circuit concluded that once officers determined that the seized item was in fact a cell phone and not a stun gun, no further search could be justified by officer safety.[40] Other courts have either

35. *See, e.g.*, United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009); United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007); People v. Diaz, 244 P.3d 501, 511 (Cal. 2011).

36. *See, e.g.*, United States v. Wurie, 728 F.3d 1, 14 (1st Cir. 2013), *cert. granted*, 134 S. Ct. 999 (2014); Smallwood v. State, 113 So. 3d 724, 738 (Fla. 2013); State v. Smith, 920 N.E.2d 949, 956 (Ohio 2009).

37. *Wurie*, 728 F.3d at 13.

38. *See supra* note 15 and accompanying text.

39. 670 F.3d 803, 806 (7th Cir. 2012).

40. *Id.*

quickly dismissed or not addressed arguments that warrantless cell phone searches are necessary to protect officer safety.[41]

Most analyses of whether *Chimel* permits a cell phone search have focused on the second rationale: whether the search was necessary to preserve destructible evidence. Many courts have held that the need to preserve evidence permits the search of cell phones incident to arrest.[42] For example, in *United States v. Young* and *United States v. Santillan*, the courts held that law enforcement officers had a need to search cell phones incident to arrest because the agents were concerned that incoming calls or text messages might be self-deleting or could overwrite existing information.[43]

Courts have also recognized that the threat to evidence stored on cell phones extends beyond overwriting. In *Flores-Lopez*, the Seventh Circuit held that cell phones of arrested methamphetamine distributors could be searched incident to arrest because there was a risk that the phones' data might be remotely erased.[44] The court suggested that a confederate of the defendants could potentially wipe "the cell phones remotely before the government could obtain and execute a warrant and conduct a search pursuant to it for the cell phone's number."[45] This threat to the evidence stored on the cell phone merited an exception to the warrant requirement in order to preserve destructible evidence.[46]

However, other courts have held that searches of cell phones incident to arrest are unnecessary to preserve evidence.[47] In *Wurie*, the First Circuit held that the remote wiping of cell phones was not a serious threat,[48] and said that searches of cell phones incident to arrest were never necessary to preserve evidence because officers had other, less intrusive methods of conserving the cell phone's data.[49] It suggested that officers could prevent a phone from being remotely wiped by turning it off, removing its battery, putting it inside a Faraday cage,[50] or mirroring

---

41. *See, e.g.*, *Wurie*, 728 F.3d at 10; United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007).

42. *See, e.g.*, United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009); United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007).

43. United States v. Young, 278 F. App'x. 242, 245–46 (4th Cir. 2008) (per curiam); United States v. Santillan, 571 F. Supp. 2d 1093, 1102–03 (D. Ariz. 2008).

44. *Flores-Lopez*, 670 F.3d at 808–10. A remote wipe erases the data stored on a cell phone from afar. Remote wiping is available through a number of commercially available programs. Jamie Lendino, *How to Remotely Disable Your Lost or Stolen Phone*, PCMAG (Apr. 12, 2012), http://www.pcmag.com/article2/0,2817,2352755,00.asp.

45. *Flores-Lopez*, 670 F.3d at 808.

46. *Id.* at 810 (reserving the question for another case of "what level of risk . . . to the preservation of evidence would be necessary to justify a more extensive search of a cell phone without a warrant"). The search at issue in *Flores-Lopez* was only for the defendant's phone number. *Id.*

47. *See, e.g.*, United States v. Wurie, 728 F.3d 1, 11 (1st Cir. 2013).

48. *Id.* ("[T]he possibility of remote wiping here was 'remote' indeed.").

49. *Id.* at 13.

50. *Id.* at 11. A Faraday cage is a metallic enclosure that blocks electric fields, and cell phones placed within a Faraday bag do not receive any signal. Kelsey D. Atherton, *Hide From GPS With This Signal-Blocking*

its contents.[51] The First Circuit believed that the use of these tactics would leave police unable to justify the search of a cell phone incident to arrest under either *Chimel* rationale.[52]

B. A Cell Phone Is Analogous to a Container on an Arrestee's Person

Some courts have held that cell phones can be searched incident to arrest because they are a type of closed container.[53] In *New York v. Belton*, the Supreme Court held that police could search any containers—open or closed—on the person or within arm's reach of an arrestee without any justification beyond a lawful arrest.[54] Some courts have extended the *Belton* rule from traditional containers to apply it to cell phones, which likewise contain evidence not immediately discernible.[55]

In *People v. Diaz*, the California Supreme Court used the rule from *Belton* to cover warrantless searches of cell phones.[56] In *Diaz*, police officers arrested the defendant for selling Ecstasy to an undercover officer.[57] The officers searched the defendant's cell phone without a warrant and found coded text messages discussing the sale of the drug.[58] Though the defendant sought to have the text messages suppressed, the trial court rejected his arguments and admitted the text messages into evidence.[59] On appeal, the California Supreme Court held that the rule from *Belton* was not limited to physical containers but could be applied more broadly to property or belongings.[60] The court believed that under the rule of *Belton*, the defendant's cell phone could be searched incident to arrest as a belonging on the person of the arrestee.[61]

However, other courts have strongly rejected the notion that cell phones are

---

Phone Case, POPULAR SCI. (Aug. 6, 2013 1:15 PM), http://www.popsci.com/gadgets/article/2013-08/how-protect-yourself-your-phone.

51. *Wurie*, 728 F.3d at 11. Some tools, such as one of Cellebrite's Universal Forensic Extraction Devices, can extract and copy (or "mirror") the data stored on cell phones. *See generally* CELLEBRITE, http://www.cellebrite.com/mobile-forensics (last visited Mar. 30, 2014).

52. *Wurie*, 728 F.3d at 13.

53. *See, e.g.*, United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007); People v. Diaz, 244 P.3d 501, 505 (Cal. 2011).

54. 453 U.S. 454, 461 (1981) ("Such a container may, of course, 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.").

55. *See, e.g.*, *Diaz*, 244 P.3d at 507 (citing *Belton*, 453 U.S. at 460).

56. *Id.*

57. *Id.* at 502.

58. *Id.* at 502–03.

59. *Id.* at 503.

60. *Id.* at 507.

61. *See id.* at 506–07, 509–10 ("[I]n determining the validity of a search incident to arrest, there is no legal basis for distinguishing the contents of an item found upon an arrestee's person from either the seized item itself or 'the arrestee's actual person.'").

analogous to closed containers and can be searched incident to arrest.[62] In *State v. Smith*, the Ohio Supreme Court distinguished the search of a cell phone from the search in *Belton* by noting that in *Belton*, the Supreme Court's definition of container "implie[d] that the container must actually have a physical object within it."[63] The Ohio Supreme Court held that the rule from *Belton* did not apply to cell phone searches because cell phones contain data, not physical objects.[64] Thus, the court believed that cell phones were different from traditional closed containers.[65]

There is no clear consensus on whether cell phones should be considered closed containers for purposes of the search incident to arrest exception.[66] Many courts considering the legality of a cell phone search incident to arrest have thus decided the case on other grounds.[67]

C. A Cell Phone is Analogous to a Pager

Some courts have held that police can search cell phones incident to arrest because cell phones are analogous to pagers, which were previously found to fall within the exception.[68] There are two primary rationales courts used to permit the search of pagers incident to arrest: the need to preserve evidence[69] and the similarity between pagers and closed containers.[70] These rationales permitting searches of pagers are similar to those discussed in the previous sections.[71]

Courts have allowed officers to search pagers incident to arrest to preserve the telephone numbers on the pagers.[72] In *United States v. Hunter*, the defendant, who was convicted of dealing cocaine and crack cocaine, appealed the admission of telephone numbers taken from his pager without a warrant.[73] However, the court upheld the admission, reasoning that pagers have a finite memory and incoming pages could have deleted stored telephone numbers.[74] The court also noted that the

---

62. *See, e.g.*, State v. Smith, 920 N.E.2d 949, 956 (Ohio 2009).

63. *Id.* at 954.

64. *Id.*

65. *Id.*

66. *Compare Diaz*, 244 P.3d at 509–10 (holding that a "container" extends to property and belongings found on the person of the arrestee), *with Smith*, 920 N.E.2d at 954 (holding that a cell phone is not a container because it does not hold a physical object within it).

67. *See, e.g.*, United States v. Murphy, 552 F.3d 405, 411–12 (4th Cir. 2009) (holding that a cell phone search incident to arrest was legal because of the need to preserve evidence).

68. *Murphy*, 552 F.3d at 411 (citing United States v. Hunter, No. 96-4259, 1998 WL 887289, at *3 (4th Cir. Oct. 29, 1998)); United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007) (citing United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996)).

69. *Ortiz*, 84 F.3d at 984 (discussing the need for evidence preservation).

70. United States v. Chan, 830 F. Supp. 531, 536 (N.D. Cal. 1993) (analogizing pagers to closed containers).

71. See *supra* Part II.A for more information on the need to preserve evidence. See *supra* Part II.B for more information on searches of closed containers.

72. *See, e.g.*, *Hunter*, 1998 WL 887289, at *3; *Ortiz*, 84 F.3d at 984.

73. *Hunter*, 1998 WL 887289, at *1.

74. *Id.* at *3.

information on some pagers could be destroyed with a single button.[75] It therefore held that police could search pagers incident to arrest in order to prevent the loss of necessary evidence.[76]

Warrantless searches of pagers were also permitted because courts found that pagers were a kind of closed container.[77] In *Belton*, the Supreme Court suggested that officers could search any containers—open or closed—within reach of an arrestee.[78] In *United States v. Chan* and *United States v. Ortiz*, the courts applied this rule to pagers, holding that pagers could be searched incident to arrest because pagers are a type of closed container.[79] Many courts that permitted the search of cell phones incident to arrest have cited *Hunter*, *Chan*, or *Ortiz* to support their decisions.[80]

However, other courts have held that the decisions in *Hunter*, *Chan*, and *Ortiz* should have no bearing on the legality of cell phone searches incident to arrest because cell phones are not analogous to beepers and pagers.[81] In *Park* and *Smith*, for example, courts believed that the pager searches allowed by other courts implicated fewer privacy rights than a search of a cell phone due to a cell phone's increased data storage capabilities.[82] Although most courts do not consider an arrestee's expectation of privacy in items on his person when applying the search incident to arrest doctrine to searches of those items, *Park* and *Smith* appear to argue that cell phone searches should require such analysis.[83] In *Park*, the court also found that cell phones, unlike pagers, could store numerous previously called numbers.[84] It held that the government failed to show that officers had to search the cell phone in order to prevent the destruction of evidence.[85] Both courts rejected the argument that the legality of warrantless searches of pagers can be applied to warrantless searches of cell phones.[86] Although some courts seemed more willing

75. *Id.*

76. *Id.*

77. *See, e.g.*, United States v. Chan, 830 F. Supp. 531, 536 (N.D. Cal. 1993).

78. 453 U.S. 454, 460–61 (1981).

79. *See* United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996); *Chan*, 830 F. Supp. at 536.

80. *See, e.g.*, United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009) (citing *Hunter*, 1998 WL 887289, at *3); United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007) (citing *Ortiz*, 84 F.3d at 984).

81. *See* United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *9 (N.D. Cal. May 23, 2007); State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009).

82. *Park*, 2007 WL 1521573, at *9; *Smith*, 920 N.E.2d at 954.

83. *Compare* United States v. Robinson, 414 U.S. 218, 235 (1973) (no requirement that officers consider an arrestee's expectation of privacy in items on his person before conducting a search incident to arrest of those items), *with Park*, 2007 WL 1521573, at *5 n.3 ("The government appears to concede that defendants have a reasonable expectation of privacy in their cell phones . . . ."), *and Smith*, 920 N.E.2d at 955 ("[Cell phones] have the ability to transmit large amounts of data . . . likening them to laptop computers, which are entitled to a higher expectation of privacy.").

84. *Park*, 2007 WL 1521573, at *8.

85. *Id.*

86. *Id.* at *9; *Smith*, 920 N.E.2d at 954.

to analogize cell phones to pagers, as cell phones became more sophisticated, courts appear to be less persuaded by this comparison.[87]

D. The Quantity or Personal Information Stored on Cell Phones Creates a Heightened Expectation of Privacy That Requires Unique Analysis

Some courts that have allowed cell phones searches incident to arrest have held that the quantity of information stored on cell phones is irrelevant, finding that the amount of data that can be stored on cell phones does not implicate a heightened expectation of privacy.[88] In *United States v. Murphy*, an officer found evidence of cocaine after arresting the defendant for providing a fake driver's license.[89] In the subsequent inventory of the defendant's car, officers found several cell phones.[90] A Drug Enforcement Administration Special Agent accessed the defendant's cell phone and found several text messages from someone who identified the defendant as his drug supplier.[91] When the defendant moved to suppress the evidence resulting from the cell phone search, the trial court held that the evidence could be admitted.[92] On appeal, the defendant argued that officers should only be allowed to search cell phones with low storage capacities because cell phones with a high storage capacity implicate an increased expectation of privacy.[93] However, the Fourth Circuit held that officers could not be expected to discern the storage capabilities of a phone before searching it.[94] Even if a phone was capable of storing large quantities of information, the court reasoned, the amount of information stored on a cell phone was not determinative of a heightened expectation of privacy in that information.[95]

In permitting cell phone searches incident to arrest, some courts have held that the possible personal nature of information stored on cell phones does not immunize them from searches incident to arrest.[96] These courts have analogized cell phones to diaries, which can be searched incident to arrest.[97] In *Diaz*, the

---

87. *Compare Smith*, 920 N.E.2d at 954 ("[P]agers . . . bear little resemblance to the cell phones of today."), *with* United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007) (holding that a cell phone search was legal because a pager search was legal).

88. *See, e.g.*, United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009); People v. Diaz, 244 P.3d 501, 507–08 (Cal. 2011). Other courts have suggested that the heightened expectation of privacy in cell phones should result in a departure from traditional search incident to arrest doctrine. *See supra* notes 82–87 and accompanying text.

89. *Murphy*, 552 F.3d at 408.

90. *Id.* at 409.

91. *Id.*

92. *Id.* at 410.

93. *Id.* at 411.

94. *Id.*

95. *Id.*

96. *See, e.g.*, United States v. Flores-Lopez, 670 F.3d 803, 807 (7th Cir. 2012); People v. Diaz, 244 P.3d 501, 507–08 (Cal. 2011).

97. *See Flores-Lopez*, 670 F.3d at 807 ("If police are entitled to open a pocket diary to copy the owner's address, they should be entitled to turn on a cell phone to learn its number."); *Diaz*, 244 P.3d at 507–08 (comparing cell phones to "photographs, letters, or diaries").

California Supreme Court noted that a cell phone might contain more personal information than a diary.[98] However, the court also recognized that any small container officers could search incident to arrest might contain "highly personal, intimate and *private* information" beyond that found in a cell phone.[99] Thus, the court believed that cell phones searches did not warrant any extra protections to prevent discovery of private information.[100] Officers were able to search the cell phone without a warrant because the cell phone was located on the person or in the immediate control of the arrestee.[101]

As with the other rationales, many courts have rejected the argument that cell phone data is indistinguishable from other forms of information discovered in a search incident to arrest.[102] Some have held that the information stored in cell phones is fundamentally different from that in diaries or address books.[103] In *Park*, for example, the court noted that both the quantity and personal nature of data stored on cell phones requires unique analysis.[104] It recognized that that "modern 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."[105]

The courts in *Wurie* and *Smallwood v. State* agreed with the *Park* court that warrantless searches of cell phones implicated higher privacy expectations than searches of diaries or other closed containers, and argued that cell phone searches incident to arrest should be held to a higher standard.[106] In *Wurie*, the First Circuit held that most of the information stored on cell phones is "of a highly personal nature."[107] In *Smallwood*, the Florida Supreme Court believed that the personal nature of this data made the search of a cell phone incident to arrest more similar to a warrantless search of a home office than of a diary.[108] The Florida Supreme Court said that "[p]hysically entering the arrestee's home office without a search warrant

---

98. *Diaz*, 244 P.3d at 507–08.

99. *Id.* at 508.

100. *Id.*

101. *Id.* at 505.

102. *See, e.g.*, United States v. Wurie, 728 F.3d 1, 9 (1st Cir. 2013); United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007); Smallwood v. State, 113 So. 3d 724, 738 (Fla. 2013).

103. *See Wurie*, 728 F.3d at 9 ("In short, individuals today store much more personal information on their cell phones than could ever fit in a wallet, address book, briefcase, or any of the other traditional containers that the government has invoked."); *Park*, 2007 WL 1521573, at *8 (finding that modern cell phones are "[u]nlike pagers or address books").

104. *Park*, 2007 WL 1521573, at *8.

105. *Id.*

106. *Wurie*, 728 F.3d at 8; *Smallwood*, 113 So. 3d at 738.

107. *Wurie*, 728 F.3d at 8. Although the First Circuit agreed that "the Supreme Court has never found the constitutionality of a search of the person incident to arrest to turn on the kind of item seized or its capacity to store private information," it also believed that "the nature and scope of the *search itself*" distinguished a cell phone search from the search of a physical object. *Id.* at 9.

108. *Smallwood*, 113 So. 3d at 738.

to look in his file cabinets or desk, or remotely accessing his bank accounts and medical records without a search warrant through an electronic cell phone, is essentially the same for many people in today's technologically advanced society."[109] Privacy concerns have convinced some courts that traditional rules governing the search incident to arrest exception should not apply to cell phones.[110]

In sum, courts do not consistently believe that the quantity and personal nature of data stored on cell phones distinguishes cell phone searches from searches of other items.[111] Although some courts have held that cell phones searches implicate a higher expectation of privacy than searches of physical items, others have denied this distinction.[112]

E. Gant *Applies to Searches of Cell Phones*

In *Gant*, the Supreme Court changed the analysis of the search incident to arrest exception.[113] Earlier courts had relied on *Robinson* and subsequent decisions that allowed police to search any object located on the person or within the immediate control of an arrestee.[114] However, in *Gant*, the Supreme Court reemphasized that a search incident to arrest, at least when conducted in a vehicle, should only be permitted if it fulfilled one of the *Chimel* rationales of preserving officer safety or preventing the destruction of evidence.[115] In *Gant*, the Court held that a search of a vehicle incident to arrest could only take place if it was reasonable to believe the vehicle held evidence of the offense for which the defendant was arrested.[116]

Many decisions permitting warrantless searches of cell phones did not consider *Gant* because they were either issued before the *Gant* ruling or the officers searched the cell phone before *Gant*, making the searches fall under the "good faith exception."[117] However, even in some decisions after *Gant*, courts asserted that the opinion did not change their analysis.[118] For example, in both *Diaz* and *Flores-*

---

109. *Id*.

110. *Wurie*, 728 F.3d at 13; *Park*, 2007 WL 1521573 at *8–9; *Smallwood*, 113 So. 3d at 738.

111. *Compare Wurie*, 728 F.3d at 8–9 (holding that cell phones are unlike other items carried on the person because "individuals today store much more personal information on their cell phones than could ever fit in a wallet, address book, [or] briefcase"), *with* People v. Diaz, 244 P.3d 501, 507–08 (Cal. 2011) (holding that there is no reason why the "sheer quantity of personal information should be determinative").

112. *Compare Wurie*, 728 F.3d at 8–9, *with Diaz*, 244 P.3d at 507–08.

113. *See* Arizona v. Gant, 556 U.S. 332, 335 (2009) (holding that a search was legitimate only if it was reasonable for an officer to have believed that the vehicle contained evidence of the offense for which the defendant was arrested).

114. Before *Gant*, courts usually limited their analysis of the search incident to arrest exception to *Chimel v. California*, 395 U.S. 752 (1969), *United States v. Robinson*, 414 U.S. 218 (1973), *New York v. Belton*, 453 U.S. 454 (1981), and *Thornton v. United States*, 541 U.S. 615 (2004).

115. *Gant*, 556 U.S. at 343.

116. *Id*. at 351.

117. *See, e.g.*, United States v. Curtis, 635 F.3d 704, 713–14 (5th Cir. 2011) (holding that the search was legitimate under the "good faith exception").

118. *See, e.g.*, United States v. Flores-Lopez, 670 F.3d 803, 806 (7th Cir. 2012); People v. Diaz, 244 P.3d 501, 507 n.9 (Cal. 2011).

Lopez, the courts distinguished *Gant* as a special rule applying to vehicles and held that *Belton* should govern cell phone searches because the cell phones were on the person of the arrested suspect.[119]

However, other courts read *Gant* more broadly, applying the opinion to cell phone searches.[120] In *Wurie*, for instance, the First Circuit interpreted *Gant* as "emphasiz[ing] the need for 'the scope of a search incident to arrest' to be 'commensurate with its purposes,' which include 'protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy.'"[121] The First Circuit believed that the same rule should apply to cell phones and that they could only be searched to protect officers or preserve evidence.[122]

In *Smallwood*, the Supreme Court of Florida also read *Gant* as removing the use of the search incident to arrest exception after the arrestee is separated from any possible weapons or evidence.[123] In *Gant*, the search incident to arrest of the arrestee's vehicle was unreasonable because the arrestee had been separated from the vehicle before the search began.[124] Similarly, the Florida Supreme Court believed that *Gant* prohibited cell phone searches after the cell phone had been separated from the arrestee, because at the time of the arrest, the cell phone could not be used as a weapon or to delete evidence after being seized.[125] However, there is currently no consensus on the extent of *Gant*, including whether it applies to cell phone searches incident to arrest.[126]

III. COURTS SHOULD USE A BALANCING TEST TO EVALUATE SEARCHES OF CELL PHONES INCIDENT TO ARREST

As the discussion above demonstrates, the rules governing searches of cell phones incident to arrest are currently in conflict. For each of the rationales that courts have used to uphold warrantless searches of cell phones, other courts have disagreed.

This problem has become more pressing as cell phones become ubiquitous. From May 2011 to May 2013, the percentage of Americans who owned a cell

---

119. *Flores-Lopez*, 670 F.3d at 806; *Diaz*, 244 P.3d at 507 n.9.

120. *See, e.g.*, United States v. Wurie, 728 F.3d 1, 9 (1st Cir. 2013); Smallwood v. State, 113 So. 3d 724, 736 (Fla. 2013).

121. *Wurie*, 728 F.3d at 9 (quoting Arizona v. Gant, 556 U.S. 332, 339 (2009)).

122. *See id.* at 12 (applying the *Gant* rule and *Chimel* rationales to searches of cell phones).

123. *Smallwood*, 113 So. 3d at 736.

124. *Gant*, 556 U.S. at 344.

125. *Smallwood*, 113 So. 3d at 736.

126. *Compare* United States v. Flores-Lopez, 670 F.3d 803, 806 (7th Cir. 2012) (holding that *Gant* is a special rule that only applies to searches after officers stop a vehicle), *with Smallwood*, 113 So. 3d at 735 (applying *Gant* to searches of cell phones).

phone increased from eighty-three to ninety-one percent.[127] And by May 2013, fifty-six percent of American adults owned smartphones,[128] which can store more data,[129] increasing the potential for privacy violations. As more people carry and use cell phones—and smartphones, in particular—law enforcement officers and courts will increasingly struggle with how to apply the search incident to arrest exception to this technology.

At the same time, cell phone technology has developed rapidly. The first cell phones date back to 1983,[130] but contemporary consumers would hardly recognize those early models as cell phones. The first version of Apple's iPhone, a popular smartphone released in June 2007,[131] would now seem obsolete. Cell phones with new capabilities are released regularly.[132] As new features are added, people will likely store more information on their phones. A court evaluating cell phone searches incident to arrest in 2009 considered a very different device than that of even a few years earlier.

Many of the most innovative—and potentially invasive—advances in technology are not in cell phone hardware but in their software. Numerous developers produce new software applications ("apps") for smartphones.[133] And many popular apps store personal information and messages on cell phones that could be exposed in a search incident to arrest.[134] For example, some users access their bank accounts through smartphones;[135] others might save their username and password information for websites in a phone's memory.[136] Without reasonable limits, searches incident of cell phones to arrest could permit law enforcement officers to browse this vast array of personal information without a warrant. And

---

127. AARON SMITH, PEW RESEARCH CTR., SMARTPHONE OWNERSHIP—2013 UPDATE, at 2 (2013), *available at* http://pewinternet.org//media//Files/Reports/2013/PIP_Smartphone_adoption_2013_PDF.pdf.

128. *Id.*

129. Mike Isaac, *Survey Finds Smartphone Apps Store Too Much Personal Data*, WIRED (Aug. 8, 2011, 4:45 PM), http://www.wired.com/2011/08/smartphone-local-data-storage/.

130. *The Evolution of Cell Phone Design Between 1983–2009*, WEB DESIGNER DEPOT (May 22, 2009), http://www.webdesignerdepot.com/2009/05/the-evolution-of-cell-phone-design-between-1983-2009/.

131. *Id.*

132. Cell phones are now commonly used to take photographs and record video—features that were unavailable even a few years ago—and may replace traditional cameras. Swapnil Mathur, *How the Camera Phone Is Killing the Point and Shoot*, THINK DIGIT (Nov. 20, 2013, 5:56 AM), http://www.thinkdigit.com/Digital-Cameras/How-the-Camera-Phone-is-killing-the_18475.html.

133. As of May 2013, it was estimated that there were over 800,000 apps on each of the Apple App Store and Google Play. *Top iOS and Android Apps Largely Absent on Windows Phone and Blackberry 10*, CANALYS (May 23, 2013), http://www.canalys.com/newsroom/top-ios-and-android-apps-largely-absent-windows-phone-and-blackberry-10.

134. *See* Isaac, *supra* note 129.

135. *See, e.g.*, *Bank of America—Mobile Banking*, ITUNES, https://itunes.apple.com/us/app/bank-america-mobile-banking/id284847138 (last visited Mar. 31, 2014).

136. In a recent survey, 18% of cell phone users admitted to storing password information on their cell phones. *Sprint + Lookout: Survey Reveals Consumers Exhibit Risky Privacy Behavior Despite Valuing Their Privacy on Mobile Devices*, SPRINT (Oct. 22, 2013), http://newsroom.sprint.com/news-releases/sprint-+-lookout-survey-reveals-consumers-exhibit-risky-privacy-behaviors-despite-valuing-their-privacy-on-mobile-devices.htm.

the rapid pace of app development has made it impossible to know what information will be accessible through cell phones in even the near future.

To resolve the pressing issue of when a cell phone may be searched incident to arrest, the Supreme Court should establish a balancing test.[137] A balancing test would most effectively weigh the needs of law enforcement against the Fourth Amendment's guarantee of freedom from unreasonable searches and seizures and would provide a more feasible solution than many proposed bright-line rules. The benefits of adopting a balancing test to address whether cell phones may be lawfully searched incident to arrest are clear. First, a balancing test weighs the legitimate interests of both law enforcement and arrestees. Second, bright-line rules do not provide courts with enough flexibility to respond to new developments in cell phone technology. Third, the proposed balancing test would not be difficult for officers to apply in the field.

A. A Balancing Test Best Weighs the Interests of Law Enforcement Against Those of Arrestees

Many of the existing rationales used to justify cell phone searches incident to arrest rely on strained analogies. For example, the many differences between a smartphone used to access digital information and a closed container that only contains a finite number of physical objects suggest that cell phone searches incident to arrest should not be governed by the rule from *United States v. Robinson*.[138] Instead of relying on dubious analogies, a balancing test, similar to that used by the Seventh Circuit in *United States v. Flores-Lopez*,[139] would be the best mechanism for deciding when officers can search a cell phone incident to arrest. The quantity and sensitive nature of personal information on cell phones means that warrantless searches of cell phones might threaten arrestees' privacy. However, a blanket ban on any searches of cell phones incident to arrest could significantly hamper law enforcement officers, who rely on data collected from

---

137. The Supreme Court will have an opportunity to do so in two cases currently pending before it. *See* United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), *cert. granted*, 134 S. Ct. 999 (2014); People v. Riley, No. D059840, 2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013), *cert. granted*, 134 S. Ct. 999 (2014).

138. *Robinson* suggests that any item on the person of the arrestee can be searched. United States v. Robinson, 414 U.S. 218, 235 (1973) ("[W]e hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search . . . ."). In *Smallwood*, the Florida Supreme Court held that the rule from *Robinson* did not apply to cell phones. Smallwood v. State, 113 So. 3d 724, 732 (Fla. 2013) ("Thus, we agree and conclude that the electronic devices that operate as cell phones of today are materially distinguishable from the static, limited-capacity cigarette packet in *Robinson* . . . .").

139. Although the Seventh Circuit claimed not to have established a balancing test, United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012) ("Toting up costs and benefits is not a feasible undertaking to require of police officers conducting a search incident to arrest."), it weighed the officers' rationales for conducting the cell phone search against the invasiveness of the search. *Id.* ("Thus, even when the risk either to the police officers or to the existence of the evidence is negligible, the search is allowed . . . provided it's no more invasive than, say, a frisk, or the search of a conventional container.").

cell phones in their investigations, if the data were wiped before the officers could acquire a warrant. A balancing test could properly consider both the legitimate needs of law enforcement and the powerful privacy interests of arrestees. To resolve this issue, the Supreme Court should craft a test that weighs the total reasonableness of a cell phone search against an arrestee's reasonable expectation of privacy.

The reasonableness of a cell phone search could be determined by two separate questions derived from current Fourth Amendment jurisprudence. Extending the Supreme Court's rule from *Gant* to cell phones, a court should first ask whether it is reasonable for an officer to believe that there was evidence of the crime on the cell phone. In *Arizona v. Gant*, the Court held that officers could search a car only when "it is reasonable to believe that evidence relevant to the crime of arrest might be found in the vehicle."[140] This rule could also be applied to searches of cell phones; for some crimes, it might be reasonable to believe that there could be evidence of the crime on the arrestee's cell phone. For example, it is reasonable to believe that suspects arrested for dealing drugs might have incriminating text messages and photographs on their cell phones.[141] However, if someone were arrested for driving with a revoked license, it is less reasonable to believe that there would be evidence of this crime on the arrestee's cell phone because there is no evidence on a cell phone that would alter the validity of the driver's license.[142]

However, an officer's belief that an arrestee's cell phone contains evidence should not solely determine whether a search of a cell phone is reasonable.[143] If an officer reasonably believed that a cell phone contained evidence of the crime for which the arrestee was arrested, the court should then ask whether it is reasonable to believe that a search of the cell phone was necessary to preserve that evidence. Consideration of this second factor would be similar to existing analysis of how

---

140. 556 U.S. 332, 343 (2009) (quoting Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring in judgment)).

141. *See, e.g.*, United States v. Quintana, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2009) ("The courts recognized that the [electronic] devices may have been used to communicate with others participating in . . . drug-trafficking.").

142. *Cf. Gant*, 556 U.S. at 351 (holding that police could not be expected to find evidence of driving with a suspended license in the passenger compartment of a vehicle).

143. Professor Kerr suggests that the *Gant* rule by itself could be used to decide if a cell phone search incident to arrest was legal. Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 406–07 (2013). However, Professor Gershowitz notes that solution could lead to expansive searches by law enforcement officers as cell phones begin to store new kinds of information. Adam M. Gershowitz, *Why* Arizona v. Gant *Is The Wrong Solution To The Warrantless Cell Phone Search Problem*, 94 B.U. L. REV. (forthcoming 2014), *available at* http://ssrn.com/abstract=2334977. Additionally, Kerr's proposal suggests that if it were reasonable to believe that a cell phone contained any evidence of the arrestee's crime, all data on the cell phone would be searchable. *See* Kerr, *supra.* This solution fails to distinguish between the different data stored on cell phones. According to it, there is no difference between using an arrestee's phone to find the phone's number or using the phone's iCam app to access a remote camera, so long as there were a reasonable belief of some evidence of the crime somewhere on the cell phone. This proposal could lead to significant privacy violations.

the *Chimel v. California* rationales apply to cell phone searches.[144] Although cell phone searches incident to arrest might not be necessary to protect officer safety, they could be justified to preserve destructible evidence. For example, if an arrestee were known to be a member of a sophisticated crime syndicate, law enforcement officers might have a more reasonable belief that a search of the arrestee's cell phone incident to arrest would be necessary to gather information before the cell phone could be wiped. However, if officers arrested a lone suspect of a drug crime, there might be a less reasonable belief that the cell phone would need to be searched incident to arrest to preserve destructible evidence. To meet the *Chimel* rationale, officers would need to explain to a court why their belief that the evidence could be deleted was legitimate.

To determine whether a search was reasonable under both the *Gant* and *Chimel* rules requires two different lines of inquiry. The analysis under the *Gant* prong would focus specifically on the crime the arrestee allegedly committed and the reasonableness of whether evidence of this crime could be on a cell phone.[145] The subsequent test from *Chimel* would consider the likelihood that any evidence might be destroyed.[146] If this balancing test was adopted, there might be situations in which the *Gant* prong was satisfied but the *Chimel* prong was not. For example, the warrantless search of the cell phone of a lone, unsophisticated drug dealer might appear reasonable under the *Gant* test, because it is reasonable to believe that a drug dealer might keep text messages and photographs that are evidence of his guilt on his cell phone. However, the search of this unsophisticated arrestee's cell phone might fail to meet the *Chimel* rationale because it would be unnecessary to search the cell phone incident to arrest if officers were not able to express a reasonable fear that the data could be deleted.

The total reasonableness of a cell phone search could be determined by both its justifications under the rule from *Gant* and its justifications under the *Chimel* rationale. A search in which both the *Gant* and *Chimel* requirements were met would be considered more reasonable because the search would have been conducted in accordance with existing Fourth Amendment jurisprudence. However, in circumstances in which the requirements of neither *Gant* nor *Chimel* were met, it would be unreasonable for officers to search a cell phone incident to arrest. In between the two extremes of this spectrum, there could be searches that met the requirements of only *Gant* or *Chimel* but not both. The reasonableness of such searches would be determined by where they lie between the two poles of the reasonableness spectrum.

Courts would then have to consider the arrestee's reasonable expectation of privacy in the information searched. The arrestee's reasonable expectation of privacy

---

144. *See, e.g.*, United States v. Wurie, 728 F.3d 1, 10 (1st Cir. 2013) ("We therefore find it necessary to ask whether the warrantless search of data within a cell phone can ever be justified under *Chimel*.").

145. *Gant*, 556 U.S. at 351.

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

would depend on what data officers accessed during their search. Although early decisions on the question of cell phone searches incident to arrest did not appear to distinguish between the types of data stored on cell phones, more recent court decisions have recognized that accessing some information on a cell phone without a warrant could be extremely intrusive.[147] These more recent decisions have also stressed that some data on cell phones might raise more privacy concerns than other types of data.[148] For example, an arrestee would have a low expectation of privacy if officers limited their search to looking up which phone numbers had called the arrestee recently. However, a search would be significantly more intrusive if officers used iCam[149] or a similar app to access an arrestee's home camera and view the arrestee's home.[150] When considering an arrestee's reasonable expectation of privacy in the data searched, courts should inquire into the personal data that officers accessed and determine whether that data deserves a higher or lower degree of privacy.

Using this balancing test, courts would then weigh the total reasonableness of the search against the arrestee's expectation of privacy in the data to determine whether the search of a cell phone incident to arrest was legitimate. For example, under this balancing test, officers would not be able to open a banking app and read the financial statements of someone arrested for reckless driving. Such a search would be extremely intrusive and would probably not be reasonable under either the *Gant* or *Chimel* rules. Less clear-cut cases would be very fact-specific and would be adjudicated on a case-by-case basis. The Supreme Court would need to provide general guidance on how much weight to give the arrestee's reasonable expectation of privacy versus the reasonableness of the search, and courts would need to decide exactly where the balance lay in each case.

In short, courts would apply the proposed balancing test by asking several questions. First, the court would consider the reasonableness of a search by asking whether officers had a reasonable belief that there was evidence of the crime on the cell phone and whether it was reasonable to believe that a search of the was necessary to preserve that evidence. Then, the court should determine the arrestee's expectation of privacy in the data accessed. The court would weigh the arrestee's expectation of privacy against the reasonableness of the officers' search to determine whether the search violated the arrestee's Fourth Amendment rights.

---

147. *See supra* Part II.D.

148. *See, e.g.*, United States v. Flores-Lopez, 670 F.3d 803, 810 (7th Cir. 2012) (exploring the ramifications of a search of the contents of a phone beyond obtaining a cell phone's phone number).

149. With iCam, officers could conceivably access an arrestee's home computer and use its camera to look into the arrestee's home. *See generally iCam—Webcam Video Streaming*, ITUNES, https://itunes.apple.com/us/app/icam-webcam-video-streaming/id296273730 (last visited Apr. 1, 2014) ("iCam allows you to remotely monitor multiple live video and audio webcam feeds from your [mobile electronic devices] . . . .").

150. *See Flores-Lopez*, 670 F.3d at 806 (comparing intrusiveness of the use of iCam to access an arrestee's home camera to the intrusiveness of obtaining a cell phone's phone number).

B. A Balancing Test Would Provide Courts With Flexibility to React to New Cell Phone Technologies

The balancing test is superior to proposed bright-line rules. Many courts generally lack the necessary technical knowledge to create effective bright-line rules for new technologies. Although some judges are able to clearly explain how technology impacts law,[151] courts are frequently criticized for their perceived ignorance of new technologies.[152] Some of this criticism might be unfair,[153] but, even so, the Supreme Court has been reluctant to change Fourth Amendment jurisprudence in reaction to specific technologies.[154] For example, in *City of Ontario v. Quon*, the Supreme Court considered whether a city's review of an employee's text messages on a city-issued pager was a violation of the Fourth Amendment.[155] In its decision, the Court admitted that a broad holding involving developing technologies was ill-advised because it could have unintended consequences far beyond those the Court could predict.[156]

Courts also struggle to create rules for quickly developing technologies, such as cell phones, because of the length of time it takes cases to be litigated. If a court crafts a rule that is too technology-specific, the technology might dramatically evolve shortly after the court's decision and render the court's rule moot. For example, the First Circuit decided *Wurie* in 2013, but the search at issue in the case occurred in 2007, meaning that the defendant's cell phone would be able to store and access significantly less data than a cell phone from 2013.[157] In creating a bright-line rule that cell phone searches incident to arrest could never be reasonable, the First Circuit considered cell phone technology beyond what the defendant possessed because the defendant's cell phone was already obsolete and any rule

---

151. In *Lorraine v. Markel Am. Ins. Co.*, Judge Grimm clearly explained how electronically stored information might be admissible as evidence. 241 F.R.D. 534, 537–38 (D. Md. 2007).

152. *See, e.g.*, Eric Goldman, *Ninth Circuit Groaner About Metatags*—Art Attacks v. MGA, TECH. & MARKETING L. BLOG (Sept. 16, 2009), http://blog.ericgoldman.org/archives/2009/09/ninth_circuit_g.htm; Mike Masnick, *Judge Who Doesn't Understand Technology Says WiFi Is Not a Radio Communication*, TECHDIRT (July 1, 2011, 12:44 PM), http://www.techdirt.com/blog/wireless/articles/20110701/12225114934/judge-who-doesnt-understand-technology-says-wifi-is-not-radio-communication.shtml.

153. *See* B.G., *Yes, The Justices Are Old*, THE ECONOMIST (Apr. 23, 2010, 1:26 PM), http://www.economist.com/blogs/babbage/2010/04/judges_and_technology (arguing that the judiciary will become technologically fluent in due time).

154. *See, e.g.*, United States v. Jones, 132 S. Ct. 945 (2012). In *Jones*, the Supreme Court struggled with how to reconcile GPS technology with the Fourth Amendment. Justice Sotomayor and Justice Alito's concurrences suggest that GPS tracking might be different from traditional surveillance. *Id.* at 955 (Sotomayor, J., concurring); *id.* at 961 (Alito, J., concurring in judgment). However, the majority's decision avoided any consideration of how technology alters traditional Fourth Amendment jurisprudence. *Id.* at 953–54 (majority opinion).

155. 130 S. Ct. 2619, 2624–26 (2010).

156. *See id.* at 2629 ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

157. *See* United States v. Wurie, 728 F.3d 1, 1 (1st Cir. 2013).

tailored to it would have been meaningless.[158] However, despite the First Circuit's best efforts, part of the reasoning of *Wurie* was dated within months of the decision's release.[159]

Other proposed bright-line rules have similarly become obsolete shortly after their creation. For example, the open application test would restrict arresting officers to searches of a phone's open application.[160] This rule seemed reasonable when cell phones could only have a single open application; however, it is already obsolete because cell phones now permit multiple applications to run at the same time.[161] Another proposed bright-line rule would restrict officers to search only information stored on a phone's hard drive.[162] This alternative was also quickly made obsolete, as cloud services have blurred the distinction between information stored on a phone's hard drive and on a network.[163]

Other bright-line rules prohibiting the search of cell phones incident to arrest could fall victim to the same issue as cell phone technology evolves. For example, in *Wurie*, the First Circuit determined that cell phone searches incident to arrest were never necessary to preserve evidence because officers could take other measures, such as powering the phone off, mirroring its contents, or putting it in a Faraday bag.[164] However, these rationales would quickly collapse if new technology rendered these measures ineffective.[165] A bright-line rule, such as that in *Wurie* or the open application test, could lead to subsequent diverging decisions between the circuits as each attempts to accommodate new technologies in different ways. Then the Supreme Court might be asked to revisit this issue every time cell phone technology changes.

The proposed balancing test avoids this problem by relying on broad legal principles instead of technology-specific, bright-line rules. If a court used the balancing test, weighing the reasonableness of a search against an arrestee's reason-

---

158. Instead, the First Circuit considered smartphones, specifically the iPhone 5. *Wurie*, 728 F.3d at 8. Such sophisticated phones did not exist when the defendant was arrested in 2007. *See supra* note 130.

159. In *Wurie*, the First Circuit stated that the government did not have a legitimate concern that the defendant's phone could have been erased remotely. *Wurie*, 728 F.3d at 11. However, since the First Circuit's decision in May 2013, remote wiping was added as a standard feature on iPhones with the "Find My iPhone" app. *Find My iPhone*, ITUNES, https://itunes.apple.com/us/app/find-my-iphone/id376101648 (last visited Apr. 1, 2014).

160. Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 53–54 (2008).

161. *E.g.*, IPHONE USER GUIDE FOR IOS 7.1 SOFTWARE, APPLE 22 (2013) [hereinafter USER GUIDE], *available at* http://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf.

162. Gershowitz, *supra* note 160, at 56–57.

163. *See, e.g.*, USER GUIDE, *supra* note 161, at 17–18 (showing that services like iCloud allow data to exist on both a cell phone and on a network).

164. United States v. Wurie, 728 F.3d 1, 11 (1st Cir. 2013). See *supra* note 50 for information on how Faraday bags work.

165. For example, Faraday cages might be circumvented in the future. *See* Richard Wilson, *Cambridge Team Cracks Faraday Cage*, ELECTRONICSWEEKLY.COM (Sep. 9, 2013), http://www.electronicsweekly.com/news/research/device-rd/cambridge-team-cracks-faraday-cage-2013-09/ (showing progress in efforts to bypass Faraday enclosures).

able expectation of privacy would require the court to carefully consider the unique facts of the case. Cell phone data that might be inappropriate for officers to seek in one scenario might appear reasonable in a completely different situation. The emergence of new cell phone technologies might shift the balance between a search's reasonableness and an arrestee's expectation of privacy, but the framework of the balancing test would remain intact. In short, the strength of the balancing test is its flexibility.

The balancing test also provides courts with the flexibility to respond to any shifts in the public's attitude towards data privacy. Although it appears that current generations share similar attitudes about data privacy,[166] these could diverge in the future. If ideas of privacy shift, a search of cell phone data that would be considered intrusive now might later be found to be less intrusive. The balancing test is flexible enough to accommodate shifts in public attitudes towards privacy without requiring courts to create a new rule.

This balancing test is also broad enough to cover devices other than cell phones that might be searched incident to arrest. The test could be applied to similar new technologies, such as "smartwatches"[167] or Google Glass.[168] As developers create new devices that challenge our traditional notions of privacy and Fourth Amendment jurisprudence, it would be burdensome if courts had to create a rule for or analogize each new device. The balancing test appropriately weighs the needs of law enforcement and the privacy interest of arrestees in searches incident to arrest involving electronic data, whether accessible through a cell phone or another device.

C. Law Enforcement Officers Would Be Able to Apply the Balancing Test in the Field

The proposed balancing test might also be criticized as too difficult for law enforcement officers to implement in the field. However, law enforcement officers could quickly adapt to this new test. According to this test, officers would need to ask themselves three questions before searching a cell phone incident to arrest: (1) Is it reasonable to believe that there is evidence of the crime the arrestee was arrested for on this cell phone? (2) Is it reasonable to believe that this evidence might be deleted? (3) What reasonable expectation of privacy does the arrestee have in this evidence?

---

166. Chris Hoofnagle et al., How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies? 10 (Apr. 14, 2010) (unpublished working paper), *available at* http://ssrn.com/abstract=1589864.

167. *See generally* Andrea Chang, *Samsung Says It Sold 800,000 Galaxy Gear Smartwatches in Two Months*, L.A. TIMES (Nov. 19, 2013, 10:52 AM), http://www.latimes.com/business/technology/la-fi-tn-samsung-gear-smartwatch-20131119,0,6970985.story (showing that smart watches might become widely available).

168. Google Glass is a "wearable Android-powered computer built into spectacle frames." Stuart Houghton, *Google Glass: Release Date, News and Features*, TECHRADAR (Nov. 7, 2013), http://www.techradar.com/us/news/video/google-glass-what-you-need-to-know-1078114.

None of these questions would require law enforcement officers to undertake any new analysis. The first question is drawn from *Gant*, and officers should be experienced at applying it to searches of vehicles.[169] The second question is drawn directly from *Chimel*, which law enforcement officers have considered in searches incident to arrest since 1969.[170] And the third question is similar to that of traditional *Katz* analysis, in which courts and police inquire into a suspect's reasonable expectation of privacy.[171]

Admittedly, balancing the results of the first two questions against the third to resolve when a search of a cell phone incident to arrest is reasonable might temporarily confuse law enforcement officers. However, law enforcement agencies would quickly adjust and devise general policies and best practices in response to courts' application of the balancing test.[172] When faced with evidence suppression, agencies would likely caution their officers to search cell phones conservatively, if at all. Officers would be trained to follow manuals and department procedures when deciding whether to conduct cell phone searches incident to arrest.

Rather than hampering law enforcement efforts, the proposed balancing test would actually aid law enforcement by allowing officers to react swiftly to new technologies without having to rely on outdated bright-line rules. For example, if officers became aware of suspects using new counter-measures through which arrestees or their associates could remotely wipe a cell phone, the reasonableness of an officer's search would increase. In response, law enforcement agencies would be able to modify their policies to authorize more frequent searches of cell phones incident to arrest. Or, if law enforcement agencies developed tactics to prevent the deletion of data, they could alter their policies to restrain searches.[173] Law enforcement agencies can react more swiftly to technological changes than courts because the agencies can alter their search procedures in response to real-world changes, while courts are burdened with time-consuming litigation.

---

169. *See* Arizona v. Gant, 556 U.S. 332, 351 (2009).

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

171. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold 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." (internal quotation marks omitted)).

172. For example, the Federal Law Enforcement Training Centers have created a presentation explaining how officers can apply *Gant* in the field. Arizona v. Gant *Slide Presentation*, FED. L. ENFORCEMENT TRAINING CTRS., http://www.fletc.gov/training/programs/legal-division/videocasts/4th-amendment/Arizona-v-Gant.pdf/view (last visited Apr. 1, 2014). If the proposed balancing test were adopted, the FLETC could add it to the existing presentation teaching officers how to conduct cell phone searches incident to arrest. *Cf. Warrantless Searches of Cell Phones Slide Presentation*, FED. L. ENFORCEMENT TRAINING CTRS., http://www.fletc.gov/training/programs/legal-division/videocasts/4th-amendment/cellphone-slide-presentation.pdf/view (last visited Apr. 1, 2014).

173. For example, officers might be able to recover data from a cell phone even after a user has erased it. *See* Mat Honan, *Break Out a Hammer: You'll Never Believe the Data 'Wiped' Smartphones Store*, WIRED (April 1, 2013, 6:30 AM), http://www.wired.com/gadgetlab/2013/04/smartphone-data-trail/.

IV. CONCLUSION

Searches of cell phones incident to arrest pose a novel and perplexing question for the courts. The rationales of earlier search incident to arrest cases are difficult to analogize to searches of cell phones, and the decisions vary dramatically among circuits. The Supreme Court should resolve this circuit split by adopting a balancing test in cases involving searches of cell phones incident to arrest. This balancing test should weigh the reasonableness of the search—as expressed by the rules from *Arizona v. Gant* and *Chimel v. California*—against the privacy interest of the arrestee. Such a balancing test would appropriately consider both the investigatory needs of law enforcement and the privacy interests of arrestees. This balancing test would be flexible enough to accommodate new cell phone technologies and could serve as an effective model for adapting existing Fourth Amendment jurisprudence law to other developing technologies.