Harvard Journal of Law & Technology
Volume 27, Number 2 Spring 2014

SEARCHES OF CELL PHONES INCIDENT TO ARREST: OVERVIEW OF THE LAW AS IT STANDS AND A NEW PATH FORWARD

*Patrick Brown**

TABLE OF CONTENTS

I. INTRODUCTION

In a series of cases in the 1960s and 1970s, the Supreme Court established that, incident to a lawful arrest, police officers may search

* Harvard Law School, J.D. 2014; Georgetown University, A.B. 2009. Thanks to my friends on the Daniel K. Inouye Memorial Ames Team and to Professor Phil Malone, whose teaching and guidance shaped this Note. Special thanks to the editors and staff of the *Harvard Journal of Law & Technology*, especially James Sebel, Steven Horn, Ritu Gupta, and Amy Rossignol. Finally, thank you to Michelle Skinner, who listened to me talk about cell phone searches for two years.

items found on the arrestee's person.[1] In the past decade, however, courts have struggled with how to extend the search incident to arrest ("SIA") doctrine to searches of the contents of arrestees' smartphones. The confused state of the law is evident from four decisions in the Northern District of California. In 1993, the court held that although an arrestee had a "protected privacy interest in the contents of [a] pager's memory," those privacy interests became irrelevant when "the pager was searched incident to [a lawful] arrest."[2] In 2007, a different judge in the same district struck down police officers' search of an arrestee's cell phone in *United States v. Park* because "modern cellular phones have the capacity for storing immense amounts of private information" and therefore should be treated differently from other objects.[3] In 2011, a judge in the district declined to follow *Park* and instead upheld a nearly identical cell phone search because an arrestee's "iPhone should not be treated any differently than . . . a wallet taken from [an arrestee's] person."[4] However, in 2012, another judge in the district, without citing either previous case, again reversed course. That judge adopted *Park*'s reasoning in holding that "[i]ndividuals store highly personal information on their cell phones, including private thoughts, emails, photos, and voice messages," so cell phones found on an arrestee's person merit different treatment than other objects.[5]

The confusion within the Northern District of California has manifested itself nationally, most prominently in May 2013, when the First Circuit held the search of any cell phone incident to arrest unconstitutional[6] — breaking from every other federal circuit court to consider the issue. This Note attempts to clarify what has become a muddled and confusing area of the law and provides a principled, practical standard for governing searches incident to arrest. Section II briefly recounts the history of SIA cases before the Supreme Court and provides a basic overview of how cell phones fit into traditional SIA law. Section III identifies the four ways in which courts have attempted to apply the SIA doctrine to cell phone searches. Section IV articulates what the Author believes is the best path forward.[7] Section

1. *See* United States v. Chadwick, 433 U.S. 1 (1977) *abrogated by* California v. Acevedo, 500 U.S. 565 (1991); United States v. Edwards, 415 U.S. 800 (1974); United States v. Robinson, 414 U.S. 218 (1973); Chimel v. California, 395 U.S. 752 (1969).

2. United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993).

3. No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007).

4. United States v. Hill, No. CR 10-00261 JSW, 2011 WL 90130, at *7 (N.D. Cal. Jan. 10, 2011).

5. United States v. Gibson, No. CR 11-00734 WHA, 2012 WL 1123146, at *10 (N.D. Cal. Apr. 3, 2012).

6. United States v. Wurie, 728 F.3d 1, 13 (1st Cir. 2013), *cert. granted*, 134 S. Ct. 999 (2014).

7. Professor Adam Gershowitz wrote an article in the UCLA Law Review in 2007 with a similar purpose, but concluded that of the six approaches to the problem he identified, "all

V analyzes two cases addressing SIA and cell phones to be decided by the Supreme Court in the spring of 2014.[8]

II. SUPREME COURT HISTORY OF SEARCH INCIDENT TO ARREST LAW AND SOME CHALLENGES POSED BY CELL PHONES

In 1969, the Supreme Court held in *Chimel v. California* that when police officers lawfully arrest an individual, they may conduct "a search of the arrestee's person and the area within his immediate control" to protect officer safety and prevent the destruction of evidence.[9]

Four years later, in *United States v. Robinson*, the Court considered a search in which the arresting officer found a "crumpled up cigarette package" in the arrestee's pocket, opened the package, and discovered heroin capsules.[10] Although the Court concluded that the particular search was not conducted to safeguard officer safety or prevent the destruction of evidence, and thus did not fall within the previously delineated exceptions to the warrant requirement, it upheld the search because

> [t]he authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect. A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification.[11]

Indeed, in deference to the necessarily ad hoc judgments police officers must make in arrest situations, the *Robinson* Court established the bright line rule that "[i]t is the fact of the lawful arrest which establishes the authority to search."[12] Subsequent cases clarified whether a search qualified as incident to arrest or instead proved too

---

six approaches appear to be somewhat unsatisfying." Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 57 (2008).

8. *Wurie*, 728 F.3d 1, *cert. granted*, 134 S. Ct. 999 (2014); People v. Riley, D059840, 2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013), *cert. granted in part*, 134 S. Ct. 999 (2014).

9. 395 U.S. 752, 763 (1969) (internal quotation marks omitted).

10. 414 U.S. 218, 223 (1973) (internal quotation marks omitted).

11. *Id.* at 235.

12. *Id.*

"remote in time or place from the arrest."[13] The result of this line of cases was a relatively well-developed set of standards for determining the validity of searches of physical objects incident to arrest. This Note does not focus on the standards regarding where and when an SIA may occur. Rather, this Note assumes that the SIA exception to the warrant requirement does apply and, in this context, examines whether courts should treat cell phones differently than other objects.

While most circuit and district courts have upheld the search of cell phones found on an arrestee's person by treating them like any other object,[14] many lower courts and commentators have taken issue with the application of pre-digital Supreme Court precedent — meant to govern physical objects — to the search of digital data on cell phones.[15] Further, courts have struggled to apply traditional SIA rules to cell phones because, unlike most physical objects, cell phones are "dynamic, [and] subject to change without warning."[16] In the SIA context, delay in searching a phone once it is seized may lead to evidence — namely the data stored within — being destroyed in one of two ways. First, evidence may be destroyed by the arrestee or the arrestee's confederates through a "remote wipe," in which the arrestee sends a signal to a seized phone causing it to destroy stored data.[17] Officers may fully prevent this only by removing the battery from a seized phone or by enclosing the phone in a Faraday bag that blocks electromagnetic radiation.[18] Second, phone numbers and contact information stored on a phone may prove time-sensitive; delay in accessing those numbers may be equivalent to their destruction. To frustrate law enforcement efforts, many criminals change their telephone numbers frequently and by a variety of creative methods.[19] In

13. United States v. Chadwick, 433 U.S. 1, 15 (1977) (invalidating the search of a locked footlocker found in the trunk of an arrestee's car when the search occurred an hour after the arrest and in a different location) (quoting Preston v. United States, 376 U.S. 364, 367 (1964)); *see also* Arizona v. Gant, 556 U.S. 332, 351 (2009) (setting forth the standard for searches incident to arrest in the vehicle context); United States v. Edwards, 415 U.S. 800, 805 (1974) (upholding search of an arrestee's clothes for evidence of the crime of arrest ten hours after the arrest occurred). *Gant* is discussed in more detail in Section III. D., *infra*.

14. *See, e.g.*, United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007).

15. *See, e.g.*, United States v. Park, No. CR 05-375 SI, 2007 WL 1521573 at *8 (N.D. Cal. May 23, 2007); Marty Koresawa, *Pay Phone Protections in a Smartphone Society: The Need To Restrict Searches of Modern Technology Incident to Arrest*, 45 LOY. L.A. L. REV. 1351, 1351 (2012) ("[I]ndividuals have a much greater expectation of privacy in their cell phones than they do in physical containers stored on their persons.").

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

17. *See, e.g.*, *Find My iPhone, iPad, and Mac*, APPLE, http://www.apple.com/icloud/features/find-my-iphone.html (last visited Mar. 2, 2014). If a remote wipe signal is sent when a phone is off-network or powered down, the wipe will commence once the phone connects to either the cellular network or the Internet. *iCloud: Erase Your Device*, APPLE SUPPORT (Feb. 17, 2014), https://support.apple.com/kb/ph2701#.

18. United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012).

19. These methods include the use of anonymous, prepaid cell phones, *see* United States v. Mamalis, 498 F. App'x 240, 243 (4th Cir. 2012) (defendant coordinated robbery with co-

this context, the delay necessary to obtain a warrant could transform a treasure trove of promising leads on an arrestee's phone into a list of deactivated, meaningless, ten-digit numbers. Given the myriad ways criminals can leverage cell phone technology to organize their activities and the ease and frequency with which they can change phone numbers to mask their identity, the speed with which law enforcement officials can learn of an arrestee's recently contacted phone numbers governs their effectiveness in investigating the case and their ability to make sense of evidence on the phone. When officers seize a cell phone, the passage of time poses a risk of destruction of evidence just as surely as the risk of a co-conspirator wiping a hard drive remotely.

III. THE FOUR FLAWED, COMPETING APPROACHES TO CELL PHONE SEARCHES INCIDENT TO ARREST

A. Applying Supreme Court Precedent for Physical Objects to Cell Phones

Traditional SIA jurisprudence does not discriminate between seized items; officers may search wallets, private diaries, or address books found on an arrestee's person.[20] Applying this precedent to electronic devices should be simple: Officers who seize a cell phone on an arrestee's person may search the entire phone's contents and preserve any evidence they find, in the same way that they may search the contents of a diary, address book, or photo album. This approach would create the type of bright-line rule for law enforcement officers counseled by the Supreme Court[21] and provide consistent treatment for individuals who store information digitally and physically. Indeed,

---

conspirators using prepaid cell phones); United States v. Lawrence, 449 F. App'x 713, 715 (10th Cir. 2011) (fraudulent scheme in which defendant gave victims the number to his prepaid telephone, then disconnected the phone), replacing the subscriber identity module ("SIM") card in a phone, *see* United States v. Moreno, 701 F.3d 64, 71 (2d Cir. 2012) (referencing testimony that "a cellular phone user can effectively change her number at will by using a new card"); Adrian Chen, *The Mercenary Techie Who Troubleshoots for Drug Dealers and Jealous Lovers*, GAWKER (Jan. 25, 2012), http://gawker.com/5878862/ (describing a system whereby, if law enforcement officials gain access to a gang member's cell phone, "[t]he crew can just replace their SIM cards"), or even installing phone number masking software on smart phones, *see e.g.*, Ad Hoc Labs, Inc., *Burner-Disposable Phone Numbers*, APPLE ITUNES, https://itunes.apple.com/us/app/burner-disposable-phone-numbers/id505800761?mt=8&ign-mpt=uo%3D4 (last visited Mar. 2, 2014) (describing an application for iPhone that allows user to mask true phone number with temporary number).

20. *See, e.g.*, United States v. Frankenberry, 387 F.2d 337, 339 (2d Cir. 1967) (allowing prosecutors to read passages from a diary searched incident to arrest); United States v. Hill, No. CR 10-00261 JSW, 2011 WL 90130, at *7 (N.D. Cal. Jan. 10, 2011) (upholding search of a wallet incident to arrest); United States v. Vaneenwyk, 206 F. Supp. 2d 423, 426 (W.D.N.Y. 2002) ("[A]n object such as a day planner, address book or the like is subject to seizure as part of . . . a search incident to arrest.").

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

these merits have led five federal circuit courts,[22] many federal district courts,[23] and numerous state courts[24] to reason simply that "[t]raditional search warrant exceptions apply to the search of cell phones,"[25] and therefore "if a cellphone is lawfully seized, officers may also search any data electronically stored in the device."[26] The Supreme Court recently heard oral argument for one case in which the lower court employed this logic: *People v. Riley*.[27]

There are two major problems with applying traditional SIA law to cell phones, however. The first and perhaps most obvious problem is that the practical effect would be to increase the scope of searches incident to arrest. While arrestees in the pre-digital era might occasionally have carried notebooks or diaries on their persons, today over ninety percent of Americans carry devices that record their photographs, intimate communications, and even whereabouts.[28] The practical effect of extending traditional SIA law would be to grant a license to police to peruse the cell phones — and maybe even laptops or tablets — of the majority of those arrested. More troubling, many courts allow the photocopying of papers found on an arrestee.[29] Direct application of this line of cases would allow police to copy and preserve the contents of arrestees' electronic devices on police databases. Were this practice to proliferate, police officers could cross-reference information stored on arrestees' phones with other publicly available information to assemble nuanced pictures of arrestees' lives. Justice Sotomayor has hinted that such aggregations of search data may constitute an unconstitutional search under the Fourth Amendment, even when no individual search was similarly violative.[30]

---

22. United States v. Pineda-Areola, 372 F. App'x 661, 663 (7th Cir. 2010); United States v. Fuentes, 368 F. App'x 95, 99 (11th Cir. 2010); Silvan W. v. Briggs, 309 F. App'x 216, 225 (10th Cir. 2009); United States v. Murphy, 552 F.3d 405, 411–12 (4th Cir. 2009); United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007).

23. *See* United States v. Wurie, 612 F. Supp. 2d 104, 109–10 (D. Mass. 2009) (collecting cases) (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") *rev'd and remanded*, 728 F.3d 1 (1st Cir. 2013), *cert. granted*, 134 S. Ct. 999 (2014).

24. *See, e.g.*, Commonwealth v. Phifer, 979 N.E.2d 210, 211–12 (Mass. 2012); People v. Diaz, 244 P.3d 501, 502 (Cal. 2011) *cert. denied*, 132 S. Ct. 94 (2011).

25. United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1277 (D. Kan. 2007).

26. United States v. Deans, 549 F. Supp. 2d 1085, 1094 (D. Minn. 2008).

27. D059840, 2013 WL 475242, at *6 (Cal. Ct. App. Feb. 8, 2013) ("Riley's cell phone was immediately associated with his person when he was arrested, and therefore the search of the cell phone was lawful whether or not an exigency still existed." (citations omitted)), *cert. granted in part*, 134 S. Ct. 999 (2014).

28. *Mobile Technology Fact Sheet*, PEW RES. INTERNET PROJECT (Dec. 27, 2013), http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.

29. *See, e.g.*, United States v. Napolitano, 552 F. Supp. 465, 482–83 (S.D.N.Y. 1982).

30. In her concurrence in *United States v. Jones*, Justice Sotomayor wrote, "[a]wareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." 132 S. Ct. 945, 956 (2012). *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

The second and less obvious problem with directly applying Supreme Court precedent to searches of phones seized incident to arrest is that, while the SIA doctrine contemplates search of items seized on an arrestee's person, much (and perhaps most) of the information available through a smartphone is not actually stored on the device, but rather retrieved from "the cloud" — remote servers across the world. In the same way that an officer who seizes an arrestee's house keys is not thereby entitled to search the arrestee's house, an officer who seizes a phone capable of accessing an arrestee's remote information is not thereby entitled to search that information. For most phone users, the distinction between information stored locally and remotely is meaningless, unless perhaps the user is stuck in a train tunnel with no Internet connectivity. For searches incident to arrest, however, the distinction is dispositive of whether a search is constitutional because, according to the Supreme Court, an officer may search only the information actually on the arrestee's person at the time of arrest.[31]

Applying traditional doctrine to searches of smartphones therefore requires officers to determine whether information on a smartphone is stored locally or remotely. This proves hugely problematic. Information stored on a smartphone is often displayed side-by-side with information retrieved from the Internet. For example, iPhone and Android users can utilize an application called Instagram to share pictures with other mobile device users.[32] When an Instagram user views photos through the application, she sees locally stored pictures alongside photos that the application retrieves from Instagram's remote servers, with no indication of where each photo is stored.[33] Under traditional doctrine, however, these two types of photos are constitutionally distinct — locally stored data is fair game for SIA, but remotely stored data is not on an arrestee's person at the time of arrest and is therefore unsearchable. Similarly, an officer could search an iPhone's "Stocks" application for stored company names (saved locally) but would be constitutionally prohibited from obtaining the same information from the "eTrade" application (which stores information remotely).[34] Moreover, the current technological trend is toward devices that access more information from the cloud, so while most cell phones currently store text messages on the phone itself, they may not in the future. Apple, Blackberry, Samsung, and HTC

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

32. *Frequently Asked Questions*, INSTAGRAM, http://instagram.com/about/faq/ (last visited Mar. 12, 2014).

33. *See Instagram Takes Up Too Much Space on My Phone*, INSTAGRAM, http://help.instagram.com/186754094794097/ (last visited Mar. 12, 2014).

34. *See* E*Trade Securities, *E*Trade Mobile for iPhone*, APPLE ITUNES (Dec. 12, 2013), https://itunes.apple.com/us/app/e*trade-mobile-for-iphone/id313259740?mt=8 ("[N]one of your personal information is stored on your device . . . .").

phones already feature cloud-based text message replacements.[35] To complicate matters further, many applications that access remote information use cache memory to improve their performance by locally storing small amounts of information retrieved from remote servers.[36]

Given the number, variety, and faddish nature of smartphone applications, it seems unlikely that an officer could make fine-grained distinctions between information stored locally versus remotely in order to avoid violating the Constitution.[37] Widespread application of traditional doctrine would require an officer to master the distinctions between "BBMs,"[38] "FBMs,"[39] and "SMSs"[40] and to stay abreast of the critical constitutional difference between the photo applications Snapseed[41] and Snapchat.[42] Cabining searches incident to arrest through a complex technical standard seems far from the Supreme Court's stated preference for bright-line rules for police officers.[43]

B. Prohibiting Searches of Cell Phones Incident to Arrest Unless the Danger of Destruction of Evidence Exists

While the Supreme Court justifies the SIA exception to the warrant requirement by citing the need to protect officer safety and preserve evidence from destruction, neither rationale need be present in any specific case to justify a search: The Supreme Court intentionally defines SIA broadly to create administrable bright-line rules for law

35. *See BBM for Android and iPhone Is Here for Free*, BLACKBERRY, http://us.blackberry.com/bbm.html (last visited Mar. 2, 2014); *iOS7 — Messages*, APPLE, https://www.apple.com/ios/messages/ (last visited Mar. 2, 2014); Casey Johnston, *New Phones from Samsung, HTC To Support "Facebook Home" App Family*, ARS TECHNICA (Apr. 4, 2013), http://arstechnica.com/gadgets/2013/04/facebook-reveals-family-of-apps-named-facebook-home/.

36. Carter Dotson, *How To: Free Up Space by Deleting Apps' Cache Files*, 148APPS (June 10, 2013), http://www.148apps.com/news/free-space-deleting-apps-cache-files/ (explaining how to speed up a phone by deleting cached data).

37. Currently, the two major mobile operating systems each have over a million applications designed for them. Trevor Mogg, *Apple Hit $10 Billion in App Store Sales for 2013, December Most Successful Month Ever*, DIGITAL TRENDS (Jan. 8, 2014), http://www.digitaltrends.com/mobile/apple-hits-10-billion-app-store-sales-2013/.

38. BlackBerry's messaging application. *BBM for Android and iPhone Is Here for Free*, BLACKBERRY, http://us.blackberry.com/bbm.html (last visited Mar. 2, 2014).

39. Colloquial term for Facebook messages. *The New Messages*, FACEBOOK, https://www.facebook.com/about/messages/ (last visited Mar. 24, 2014).

40. An acronym for "Short Message Services," also known as text messages. *SMS Definition*, OXFORD ENGLISH DICTIONARY, http://www.oed.com/view/Entry/266845 (last visited Mar. 24, 2014).

41. A mobile photography application. *Snapseed*, APPLE ITUNES, https://itunes.apple.com/us/app/snapseed/id439438619?mt=8 (last visited Mar. 24, 2014).

42. An application for sending images, which are deleted after a set amount of time, to other users. *Snapchat*, APPLE ITUNES, https://itunes.apple.com/us/app/snapchat/id447188370?mt=8 (last visited Mar. 24, 2014).

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

enforcement officers.[44] Entirely independent from the SIA exception, "the need to prevent the imminent destruction of evidence" may also justify a warrantless search through the exigency exception to the warrant requirement.[45] In two related lines of cases, courts have evaluated whether a cell phone seized incident to arrest may be searched by departing from the SIA doctrine and instead inquiring whether there existed a threat to officer safety or a risk that evidence might be destroyed.

In the first line of cases, courts have conducted this inquiry as to all cell phones and asked whether the risk of destruction of evidence or harm to officers can ever justify a warrantless search of an arrestee's cell phone. Most prominently, the First Circuit employed this reasoning in *United States v. Wurie* — currently before the Supreme Court — to hold that "warrantless cell phone data searches are *categorically* unlawful under the search-incident-to-arrest exception" because neither rationale underlying the exception applies.[46] The *Wurie* court noted that phones store huge amounts of intimate, highly personal information and reasoned that Supreme Court precedent did not envision that cell phones, which store a qualitatively different amount of information than "a wallet, address book, briefcase, or any of the other traditional containers," should fall within the ambit of the SIA exception.[47] However, *Wurie* explicitly held open the possibility of officers conducting cell phone searches under the exigent circumstances exception to the warrant requirement.[48] The Ohio Supreme Court employed similar reasoning in *State v. Smith*, holding that "because an individual has a privacy interest in the contents of a cell phone that goes beyond the privacy interest in an address book or pager, an officer may not conduct a search of a cell phone's contents incident to a lawful arrest without first obtaining a warrant."[49] Instead, the court considered whether the search was lawful under the exigency exception to the warrant requirement, but found that "the state

44. *Id.*

45. Kentucky v. King, 131 S. Ct. 1849, 1856 (2011) (citations and quotations omitted). For example, when a cell phone search was not contemporaneous with arrest, the court in *United States v. Wall* still considered whether an actual risk of evidence destruction triggered the exigency exception to the warrant requirement. No. 08-60016-CR, 2008 WL 5381412 (S.D. Fla. Dec. 22, 2008) *aff'd*, 343 F. App'x 564 (11th Cir. 2009).

46. United States v. Wurie, 728 F.3d 1, 12 (1st Cir. 2013) *cert. granted*, 134 S. Ct. 999 (2014).

47. *Wurie*, 728 F.3d at 9.

48. *Id.* at 13 ("[T]he exigent circumstances exception would allow the police to conduct an immediate, warrantless search of a cell phone's data where they have probable cause to believe that the phone contains evidence of a crime, [and] a compelling need to act quickly that makes it impracticable . . . to obtain a warrant . . . .").

49. 920 N.E.2d 949, 955 (Ohio 2009). The Supreme Court of Florida took a similar approach. Smallwood v. State, 113 So. 3d 724, 732 (Fla. 2013).

failed to present any evidence that the call records and phone numbers were subject to imminent destruction."[50]

In the second line of SIA exception cases, courts have blurred the line between the exigency and SIA exceptions by considering whether the justifications underlying the SIA doctrine actually justified the particular search in question.[51] These cases stray from precedent because, in the SIA context, the Supreme Court explicitly rejects retrospective judicial analysis of the probability of destruction of evidence.[52] If an actual danger of destruction of evidence were required to trigger the SIA exception to the warrant requirement, then SIA would be a mere subset of the exigency exception. This cannot be true; the exceptions are separate and distinct. The reasoning in these cases is therefore flawed because it silently reads the SIA exception out of existence by rendering it a restatement of the exigency exception.

Requiring officers and courts to evaluate the danger of evidence destruction on a case-by-case basis — either through the exigency exception, as in *Wurie*, or through a misapplication of the SIA exception — contradicts Supreme Court precedent.[53] Practically, in the absence of a clear standard, evaluating the danger of destruction of evidence proves immensely difficult. As noted, cell phone storage may be wiped remotely, or the numbers stored on a phone may lose their relevance as the owners of the stored numbers change phone numbers. The exigency standard requires imminent danger of destruction of evidence, but it seems unclear what evidence would establish this danger and justify an officer searching a phone, especially because the officers would have to evaluate these dangers before searching the phone. Similarly, it remains unclear what specific evidence would justify searching a phone to protect officer safety, despite the ever-present threat that an arrestee may have communicated with vio-

50. *Smith*, 920 N.E.2d at 955. In essence, the *Smith* court held that cell phone searches should be considered under the rubric of the exigency exception to the warrant requirement, not the SIA exception.

51. *See* United States v. DiMarco, No. 12 CR 205(RPP), 2013 WL 444764 at *12 n.11 (S.D.N.Y. Feb. 5, 2013) (holding a search of a cell phone invalid when the prosecution failed to prove that destruction of evidence "was a credible or reasonable concern underlying the search in this case"); United States v. Rodriguez-Gomez, No. 1:10-CR-103-2-CAP-GGB, 2010 WL 5524891 (N.D. Ga. Nov. 15, 2010), *report and recommendation adopted in part*, No. 1:10-CR-103-2-CAP-GGB, 2011 WL 39003 (N.D. Ga. Jan. 4, 2011) (adopting the magistrate's final report and recommendation on grounds other than search incident to arrest); United States v. Quintana, 594 F. Supp. 2d 1291, 1300 (M.D. Fla. 2009) ("The search of the contents of Defendant's cell phone had nothing to do with officer safety or the preservation of evidence related to the crime of arrest."); United States v. Santillan, 571 F. Supp. 2d 1093, 1102 (D. Ariz. 2008).

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

53. *Id.* ("A police officer's determination as to how and where to search the person of a suspect whom he has arrested is necessarily a quick *ad hoc* judgment which the Fourth Amendment does not require to be broken down . . . into an analysis of each step in the search.").

lent co-conspirators prior to arrest or even summoned a flash mob to confront police.[54] This pallor of uncertainty could routinely force officers to choose between preserving evidence and protecting their safety on the one hand, and risking suppression of evidence found on the phone on the other.[55]

Both *Wurie* and *Smith* responded to concerns about the information contained in cell phones by creating a carve-out to the Supreme Court's SIA doctrine and disallowing searches of cell phone devices. However, responding to concerns about information access by creating rules about devices that contain the information, rather than about the information itself, seems like an imperfect solution. Cases like *Wurie* necessarily contemplate binary categorization of items on an arrestee's person as either cell phones or traditional objects. Innovation promises to blur these distinctions, however, through wearable technology and the "Internet of things."[56] For example, under *Wurie*, an officer conducting an arrest in the near future may struggle with whether she may search a credit card replacement that digitally stores credit card numbers,[57] a watch connected to the Internet,[58] or a brassiere that digitally measures stress.[59] While the *Wurie* court envisioned its categorical prohibition of cell phone searches incident to arrest as providing a clear bright line rule for law enforce-

54. *See, e.g.*, Sunil Bhave, *Warrantless Cell Phone Searches in the Age of Flash Mobs*, 12 CONN. PUB. INT. L.J. 263, 266 (2013) (arguing that "limited searches of cell phones to determine whether flash mob communications were made immediately prior to arrest are lawful under the officer safety justification"). The Oxford English Dictionary defines "flash mob" as "[a] large group of people organized by means of the Internet, or mobile phones or other wireless devices, who assemble in public to perform a prearranged action together and then quickly disperse." *Flash Mob Definition*, OXFORD ENGLISH DICTIONARY, http://www.oed.com/view/Entry/390783 (last visited Mar. 2, 2014).

55. *See* United States v. Brown, CRIM.A. No. 12-79-KKC, 2013 WL 1185223, at *4–5 (E.D. Ky. Mar. 20, 2013) (drawing "a fine distinction based on the evolving facts and circumstances unique to this incident" in order to suppress evidence gained from a cell phone search as "fruit of the poisonous tree").

56. Bill Wasik, *Welcome to the Programmable World*, WIRED (May 14, 2013, 6:30 AM), http://www.wired.com/gadgetlab/2013/05/internet-of-things/ (describing "the language of the future: tiny, intelligent things all around us, coordinating their activities. Coffeepots that talk to alarm clocks. Thermostats that talk to motion sensors. Factory machines that talk to the power grid and to boxes of raw material."); *see also* Cyrus Farivar, *Intel Debuts a Host of "Smart" Devices, Including a "Charging Bowl,"* ARS TECHNICA (Jan. 6, 2014, 10:27 PM), http://arstechnica.com/gadgets/2014/01/intel-debuts-a-host-of-smart-devices-including-a-charging-bowl/ (discussing in-development wearable technologies).

57. Ellis Hamburger, *Wallet Hack: Can Coin Replace Your Credit Cards?*, THE VERGE (Nov. 14, 2013, 12:00 PM), http://www.theverge.com/2013/11/14/5103820/coin-electronic-card-to-hold-all-your-credit-cards.

58. *See, e.g.*, *Discover Pebble*, PEBBLE, https://getpebble.com/discover (last visited Mar. 8, 2014).

59. Rick Aristotle Munarriz, *Forget Smartwatches: The Future of Wearable Tech Is the Smartbra*, DAILY FINANCE (Dec. 12, 2013, 5:54 PM), http://www.dailyfinance.com/on/smartbra-smartwatches-future-wearable-tech/.

ment, technology will soon render the line quite murky and significantly less practical.[60]

C. Creating a Legal Fiction To Strike Down Cell Phone Searches

The Supreme Court distinguishes between items seized on an arrestee's person and items within an arrestee's immediate control. Under *Edwards* and *Robinson*, officers may legally search items on an arrestee's person (like an arrestee's clothes, or an item in his pocket) even after the arrest and in a different location.[61] In contrast, under *Chadwick*, officers may not search items within an arrestee's immediate control (like a locked footlocker in the trunk of a car) absent exigent circumstances.[62]

In *United States v. Park*,[63] a court in the Northern District of California considered the search of a cell phone seized on an arrestee's person and searched at the police station — exactly the type of search allowed by *Edwards*.[64] In an effort to avoid applying *Edwards*, the *Park* court cited the privacy interests implicated by searching cell phones with large memories and decided to treat the phone as within Park's immediate control, under *Chadwick*, instead of on his person.[65] This legal fiction allowed the court to strike down the search because of its timing and location, thereby avoiding the more difficult question of whether the privacy interests it identified would bar or limit a search contemporaneous with arrest.

The *Park* precedent only marginally helps in the effort to forge a national standard for cell phone searches, for two reasons. First, *Park* dodges the question. Although the court makes an eloquent case that privacy interests in smartphones justify some deviation from traditional SIA jurisprudence, *Park* disregarded Supreme Court precedent by treating a phone on Park's person as if it were in his immediate control, but not on his person. Second, the *Park* court's distinction between electronic devices with smaller memories, like pagers, (searchable) and "modern cellular phones" with "the capacity for storing immense amounts of private information" (not searchable) proves immensely problematic.[66] While this distinction seemed clear in 2007 when *Park* was written, new and relatively inexpensive wearable computing technologies have already begun to blur this line. For example, the Fitbit One wearable activity tracker stores seven days of

60. United States v. Wurie, 728 F.3d 1, 12–13 (1st Cir. 2013).

61. United States v. Edwards, 415 U.S. 700, 808 (1974); United States v. Robinson, 414 U.S. 218, 236 (1973).

62. United States v. Chadwick, 433 U.S. 1, 16 (1977).

63. No. CR 05-375 SI, 2007 WL 1521573, at *5–10 (N.D. Cal. May 23, 2007).

64. *Edwards*, 415 U.S. at 808.

65. *Park*, 2007 WL 1521573, at *9.

66. *Id.* at *8.

"minute-by-minute" activity data and is probably searchable under *Park*;[67] its competitor, the Jawbone UP wristband, holds nine months of data and is likely not searchable under the same standard.[68] *Park* suffers from the same flaw as do *Wurie* and *Smith*: It relies on an imprecise technological proxy for privacy by limiting access to devices rather than access to information. In the coming world of low-cost wearable technology, requiring police officers to assess every mobile device and render a binary decision as to its capabilities before searching it will not work.[69]

D. Allowing Searches for Evidence of the Crime of Arrest Under Gant

In *Arizona v. Gant*, the Supreme Court clarified the scope of the SIA doctrine as applied to automobile searches.[70] Specifically, the Court held that SIA of an automobile is justified in two scenarios.[71] First, when an arrestee has access to the vehicle, preservation of evidence and the need for officer safety justify a search.[72] Second, even when an arrestee does not have access to the vehicle, "circumstances unique to the vehicle context" still justify a search "when it is 'reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'"[73] Although the Supreme Court explicitly cabined the second prong of the *Gant* rule to the automobile context, many courts have extended the rule to cell phone searches by inquiring whether the search targeted evidence of the crime of arrest. Using logic typical in this line of cases, a federal district court in *United States v. Quintana* excluded evidence of drug crimes gained from an arrestee's phone searched incident to arrest for driving with a suspended license in Florida.[74]

---

67. *Fitbit One Specs*, FITBIT, https://www.fitbit.com/one/specs (last visited Mar. 15, 2014).

68. *How Much Data Can UP Hold?*, JAWBONE FORUMS, http://forums.jawbone.com/t5/LIVING-UP/How-much-data-can-UP-hold/td-p/48974 (last visited Mar. 15, 2014).

69. The Fourth Circuit rejected a similar proposal, noting that "to require police officers to ascertain the storage capacity of a cell phone before conducting a search would simply be an unworkable and unreasonable rule." United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009).

70. 556 U.S. 332, 335 (2009).

71. *Id.*

72. *Id.* at 338.

73. *Id.* at 343 (quoting Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring in judgment)).

74. 594 F. Supp. 2d 1291, 1300 (M.D. Fla. 2009) (analyzing the Justices' oral arguments in *Gant*); *see also* United States v. Nyuon, No. CR. 12-40017-01-KES, 2013 WL 1338192 (D.S.D. Mar. 29, 2013) (upholding search of a cell phone by finding that the government met its burden showing that the search sought to uncover evidence of the crime of arrest under the *Gant* standard, and noting that cell phones are searchable under the SIA doctrine irrespective of *Gant*); United States v. Rodriguez, Criminal No. C-11-344, 2011 WL 3924958, at *5 (S.D. Tex. Sept. 6, 2011) ("As the arrest was based on probable cause and the officers reasonably believed the cell phone contained evidence of the offense of arrest,

It remains unclear which crimes would justify searching a cell phone for evidence. While the *Quintana* court found that an arrest for driving with a suspended license did not justify searching the arrestee's phone, one can easily imagine how the court could have arrived at the opposite conclusion in a similar case. For instance, Florida law requires actual knowledge of license suspension before criminal liability attaches;[75] officers could have made a compelling case that they reasonably expected to find evidence that the arrestee's text messages, documents, or Internet browsing history stored on the phone established knowledge of his suspended license. The possibility for confusion is evident from other courts' attempts to extend *Gant* to the cell phone context. While one federal district court in Nebraska held that officers serving an arrest warrant for distribution of and conspiracy to distribute drugs were not justified in believing that a search of the arrestee's phone "would produce evidence related to the crime for which he was arrested,"[76] other courts have upheld cell phone searches of defendants in possession of drugs,[77] sometimes on the theory that "'cellular phones, complete with memory of numbers recently or frequently called, or their 'address books,' are a known tool of the drug trade.'"[78]

This elasticity could become problematic. While searches for evidence of the crime of arrest and judicially issued search warrants putatively require the same standard — probable cause — extending *Gant* may provide officers with a way to circumvent warrant requirements by executing arrest warrants when arrestees are likely in possession of their phones. Judges may prove more sympathetic to an officer's judgment in the heat of arrest than in the warrant authorization context; moreover, the good faith exception to the warrant requirement may allow judges to admit evidence even when a search does not quite meet the probable cause standard.[79]

---

the Court concludes that the search of the cell phone's contents was lawful."), *aff'd*, 702 F.3d 206 (5th Cir. 2012).

75. Quest v. State, 837 So. 2d 1106, 1107 (Fla. Dist. Ct. App. 2003).

76. United States v. McGhee, No. 8:09CR31, 2009 WL 2424104, at *3 (D. Neb. July 21, 2009). The *McGhee* court based its reasoning largely on its respect for McGhee's privacy interest in the contents of his phone and the fact that the offense occurred ten months before the arrest. *Id.* However, the court did not consider that any records on the phone at the time of the offense may have remained stored in the phone's memory.

77. *See Rodriguez*, 2011 WL 3924958, at *5; United States v. Davis, 787 F. Supp. 2d 1165, 1170 (D. Or. 2011) (sex trafficking case) (noting in dicta that "[c]ourts have generally permitted law enforcement officers to conduct warrantless searches of cell phones in cases involving drug-trafficking, where evidence of the crime is likely stored on the phones").

78. United States v. Pineda, Criminal Case No. 1:11-CR-00006-CAP-JFK, 2012 WL 2906758, at *19 (N.D. Ga. June 4, 2012) (quoting United States v. Wiseman, 158 F. Supp. 2d 1242, 1249 (D. Kan. 2001)), *report and recommendation adopted*, Criminal Action No. 1:11-CR-0006-CAP-JFK, 2012 WL 2907447 (N.D. Ga. July 16, 2012).

79. Under the good faith exception to the Fourth Amendment warrant requirement, police misconduct that is not meaningful or not culpable does not require suppression of evidence

Extending *Gant* to cell phone searches also creates serious problems regarding the scope of a permissible search for evidence of the crime of arrest, because the plain view doctrine applies to digital searches,[80] and evidence of drug distribution could exist in text messages, recent contacts, the address book, photographs, or even within downloaded applications. If an officer is authorized to search anywhere on the phone for evidence of the crime of arrest under *Gant*, and the plain view doctrine allows that officer to seize incriminating evidence unrelated to the crime of arrest from anywhere on the phone, then there would be little practical difference between extending *Gant* and allowing the search of an entire phone under *Edwards*.[81] Indeed, extending *Gant* would create a legal regime that suffers from the same issues related to distinguishing between information stored on the device and stored remotely as presently exist.

IV. A NOVEL, PRINCIPLED, PRACTICAL APPROACH: ALLOWING LIMITED SEARCHES FOR NON-PRIVATE INFORMATION

As established above, each of the four approaches courts have taken to solve the problem of searches of cell phones incident to arrest suffers from severe flaws: Direct application of extant precedent allows unlimited search of a phone's contents incident to any arrest; requiring actual danger of evidence destruction does away with the SIA doctrine entirely; the *Park* court's legal fiction misreads Supreme Court precedent; and extending *Gant* provides very few practical limitations on cell phone searches. Despite the conflicting standards, a few trends do emerge from the many cases: Courts consider cases within the SIA framework, attempt to recognize citizens' heightened expectation of privacy in their smartphones, and favor limited searches of a phone's contents over general searches. Although no courts or commentators have yet realized it, these general outcomes prove consistent with a more nuanced approach to the issue — one which asks first, whether police may seize and search an arrestee's phone incident to arrest, and second, whether the arrestee has a reasonable expectation of privacy in the specific information searched.

Recently, the Supreme Court unanimously held in *United States v. Jones* that the government's warrantless use of a GPS tracking device attached to the defendant's car constituted an unconstitutional

---

obtained through that misconduct. *See, e.g.*, Davis v. United States, 131 S. Ct. 2419, 2427–28 (2011).

80. *See, e.g.*, United States v. Highbarger, 380 F. App'x 127, 131 (3d Cir. 2010); United States v. Williams, 592 F.3d 511, 522–24 (4th Cir. 2010); United States v. Miranda, 325 F. App'x 858, 860 (11th Cir. 2009).

81. See infra Section IV for a discussion of the plain view doctrine.

search under the Fourth Amendment.[82] Writing for the Court, Justice Scalia explained that a citizen's protections under the Fourth Amendment derive from two different sources: (1) a common law right against physical trespass and (2) a citizen's reasonable expectation of privacy in information.[83] An individual has a reasonable expectation of privacy in information when "the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy,'" and "the individual's subjective expectation of privacy is 'one that society is prepared to recognize as reasonable.'"[84] Justice Scalia reasoned that attaching a device to Jones's car constituted a search under the trespassory test and declined to consider whether the government's actions also violated Jones's reasonable expectation of privacy.[85] Five justices writing in two separate concurrences, however, found that Jones had a reasonable expectation of privacy in detailed GPS records of his whereabouts and that the actions of officers monitoring this information without a warrant constituted an unconstitutional search.[86]

The SIA context differs critically from the facts of *Jones*. While the police in *Jones* had no right to physically access the defendant's car, police have an undisputed right to physically seize a phone found on an arrestee.[87] Once the common law trespassory prohibition against physically accessing a citizen's cell phone is removed incident to arrest, the citizen's reasonable expectation of privacy should govern the extent of the search. The reasonable expectation of privacy, in turn, may be conceptualized in one of two ways: (1) as one inquiry controlling whether all information contained in the phone may be searched or (2) as a series of inquiries governing whether specific information on the phone may be searched. The latter seems to make more sense — as Professor Orin Kerr noted, "[c]omputers are searched to collect the information they contain. When assessing how the Fourth Amendment applies to the collection of information, courts

82. 132 S. Ct. 945, 949 (2012).

83. *Id.* at 952.

84. Smith v. Maryland, 442 U.S. 735, 740 (1979) (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)) (internal quotation marks omitted).

85. *Jones*, 132 S. Ct. at 950.

86. *Id.* at 964 (Alito, J., concurring in the judgment); *see id.* at 955–56 (Sotomayor, J., concurring).

87. Justice Cardozo outlines the basic principle: "Search of the person is unlawful when the seizure of the body is a trespass, and the purpose of the search is to discover grounds as yet unknown for arrest or accusation." People v. Chiagles, 142 N.E. 583, 584 (N.Y. 1923) (Cardozo, J.) (citations omitted), *quoted in* United States v. Robinson, 414 U.S. 218, 232 (1973). He then elaborates that, "[s]earch of the person becomes lawful when grounds for arrest and accusation have been discovered, and the law is in the act of subjecting the body of the accused to its physical dominion." *Id.*

should focus on that information rather than the physical storage device that happens to contain it."[88]

The Supreme Court has held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[89] In *Smith v. Maryland*, Justice Blackmun's majority opinion concluded that the defendant had a reasonable expectation of privacy in the content of his telephone conversations but not in his dialed telephone numbers. The majority reasoned that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed," but would not expect someone to listen in on the content of the conversation.[90] This intuitive distinction dates back to the nineteenth century, when the Court held that "[l]etters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles."[91]

The Supreme Court's Fourth Amendment jurisprudence thus yields a simple, three-part test for searches of cell phones incident to arrest. Such searches are constitutional when: (1) police have a lawful physical right of access to the phone, (2) the information searched is stored on the phone, and (3) no reasonable expectation of privacy attaches to the information searched because that information has been exposed to third parties. Application of this test reveals three types of information stored on a phone that do not benefit from a reasonable expectation of privacy because they are necessarily disclosed to a phone's carrier: a cell phone's own number, dialed numbers, and texted numbers.[92] While not explicitly citing this reasoning, courts have consistently upheld limited searches when the government sought to introduce only this information in evidence. For example, in *United States v. Flores-Lopez*, Judge Posner held that an SIA was justified because "the police did not search the contents of the defendant's cell phone, but were content to obtain the cell phone's phone

88. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 556 (2005).

89. *Smith*, 442 U.S. at 743–44.

90. *Id.* at 742–43.

91. *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

92. Because this type of information benefits from no expectation of privacy, no warrant is required for law enforcement to access this data from the cell phone carrier — a subpoena suffices. *See* 8 U.S.C. § 2703(c)(2) (2012). Nearly all cell phone carriers preserve and store this data for at least one year. *Cell Phone Location Tracking Request Response — Cell Phone Company Data Retention Chart*, ACLU, http://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart (last visited Mar. 8, 2014). Moreover, this rule resolves concerns that a rule governing searches incident to arrest would also allow full searches of laptops or other computer-like devices.

number."[93] Other types of information on the phone, like the content of conversations, text messages, or photographs, would still benefit from reasonable expectation of privacy protection, as users do not necessarily disclose such information to third parties.[94]

If information disclosed to third parties may be searched on a cell phone incident to arrest, it seems to follow that the headers of email and Facebook messages would also be searchable because that data is disclosed to a third party messaging service.[95] However, a court can differentiate email and Facebook message information from dialed numbers, texted numbers, or a phone's own number on three principled bases. First, the Fourth Amendment allows targeted searches but not general searches.[96] In the cell phone context, all phone users have an assigned phone number, all presumably use their phones to make calls, and nearly all send or receive text messages.[97] An officer arresting an individual can conclude with a high degree of probability that the arrestee's cell phone contains recently dialed and texted numbers and of course has an assigned number. This dynamic renders searches for a phone's number, texted numbers, or dialed numbers highly likely to yield results and justifies creating a bright-line rule allowing

93. 670 F.3d 803, 810 (7th Cir. 2012); *see also* United States v. Gomez, 807 F. Supp. 2d 1134, 1149 (S.D. Fla. 2011) (upholding search of recently called numbers, and noting "we do not suggest that the search incident to arrest exception gives agents carte blanche to search indefinitely each and every facet of an arrestee's cell phone"); United States v. Santillan, 571 F. Supp. 2d 1093, 1104 (D. Ariz. 2008) (upholding search that was "limited in scope, as agents accessed only the recent contacts, or the incoming and outgoing calls"); United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008) ("Brenner limited his search to the phone's address book and call history. He did not listen to voice mails or read any text messages. As the magistrate judge noted, we can leave for another day the propriety of a broader search equivalent to the search of a personal computer." (footnote omitted)).

94. In the same way that the Court in *Smith* held that phone conversations were not disclosed to phone companies, text messages are not disclosed to cell phone carriers. In fact, most cell phone carriers do not store sent text messages, and those that do store them for a short period of time. *See* ACLU, *supra* note 92. Samuel Beutler argues that a "function-based rule" should allow the search of call history, text message content, and address book content incident to arrest. Samuel J. H. Beutler, Note, *The New World of Mobile Communication: Redefining the Scope of Warrantless Cell Phone Searches Incident to Arrest*, 15 VAND. J. ENT. & TECH. L. 375, 401 (2013). However, it seems unclear under Beutler's proposed rule why these items would be searchable while other cell phone contents with clear physical analogues like notes or photographs would not be. Moreover, text message contents are a close analogue to the telephone conversations protected under *Smith* and should merit similar protections.

95. *See* United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008).

96. Historically, in the context of the Fourth Amendment, "the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion *per se*, but of a general, exploratory rummaging in a person's belongings." Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

97. According to a study by the Pew Research Center's Internet & American Life Project, Eighty-one percent of cell phone users send or receive text messages. PEW RES. INTERNET PROJECT, *supra* note 28.

such searches.[98] In contrast, only half of cell phone users check email on their phones, and even fewer use their phones to access social networking sites.[99] Thus, officers cannot conclude without prior information that the arrestee has used a third-party communication service, and a search for such information would therefore approach the "general, exploratory rummaging" guarded against by the Fourth Amendment.[100] Second, even if officers did know that an arrestee used her phone to communicate through Facebook or email, many such third party communication applications store information in a remote location in the cloud and not on the phone itself.[101] But, as noted, the SIA doctrine contemplates searches of the person — not searches of remote information — and therefore precludes access to remote information incident to arrest.[102] Third, Congress has evidenced its intent that information stored on services like Facebook or email be treated differently from a cell phone's number or recently called and texted numbers. Under 18 U.S.C. §§ 2703(c)(2)(C) and (E) (2012), a governmental entity with an administrative, grand jury, or trial subpoena may require a phone company to disclose a subscriber's assigned phone number and recently called or texted numbers. In contrast, obtaining recent email or messaging contact information from services like Facebook or Gmail requires a warrant or court order under 18 U.S.C. §§ 2703(c)(1) and (d) (2012).

A rule built on the reasonable expectation of privacy test also addresses the potential for destruction of evidence. As noted above, the

---

98. This dynamic also resolves a problem identified by Professor Orin Kerr. *See* Orin Kerr, *Fourth Amendment Rights in Numbers Dialed Stored Inside a Cell Phone*, THE VOLOKH CONSPIRACY (Dec. 23, 2008, 9:15 AM), http://www.volokh.com/posts/1229998859.shtml. In *United States v. Fierros-Alavarez*, the court upheld a cell phone SIA because the search revealed only recently called numbers in which the defendant had no reasonable expectation of privacy under *Smith*. 547 F. Supp. 2d 1206, 1210–11 (D. Kan. 2008). Kerr criticized the ruling because it reviewed and vindicated an open-ended cell phone search ex post, while the Fourth Amendment requires specificity in the place or things to be searched ex ante. Kerr, *supra*. This Note's proposed solution avoids the problem Kerr identifies because it specifically identifies the three pieces of information sought ex ante.

99. PEW RES. INTERNET PROJECT, *supra* note 28. Forty percent of Americans use their phones to access social networking sites. *Social Networking Fact Sheet*, PEW RES. INTERNET PROJECT (Dec. 27, 2013), http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/.

100. *Coolidge*, 403 U.S. at 467.

101. Even though some applications may store information on the phone itself, it would seem unadvisable to create a rule whereby officers are required to understand how any application they wish to search stores data. Such a rule would effectively cause an arrestee's Fourth Amendment rights to expand and contract depending on the arresting officer's knowledge of a seized phone's software, or would require judges to speculate as to what a reasonable officer would know about the data storage proclivities of smart phone applications.

102. This requirement presents no problem for searches of dialed numbers, texted numbers, and the phone's own number, because phones store this information on the phone itself.

possibility of evidence destruction in the cell phone context arises from two dangers: (1) delay in searching the phone may render the phone numbers stored within obsolete and irrelevant, and (2) data in the phone may be erased through a remote wipe. Allowing officers immediately to search an arrestee's seized phone for recently contacted numbers would significantly diminish the danger of an arrestee's recently contacted numbers losing relevance because the searching officer could immediately act on whatever information she finds. The second danger, of remote wiping, occurs when someone sends a command to the cell phone that causes the phone to delete all data it contains. Police may foil remote wipes by preventing the seized phone from receiving the wipe signal in one of three ways. Police may simply turn off the phone or place it in "airplane mode."[103] However, phone owners may deceive officers by modifying their phones' software to render their power or airplane mode buttons useless, or they may even set them to trigger a wipe of the phone. Alternatively, officers may prevent remote wipes by removing a phone's battery. However, some phones may require a password when turned back on, and some phones (notably, the iPhone) do not allow removal of the battery. The third and most effective way to prevent remote wipes is to use a Faraday bag — a small pouch made of material that blocks signals to and from the phone.[104] Faraday bags are small, light, cheap, and reusable.[105] Officers could easily carry them on their belts or in their squad cars for immediate use; cost-conscious police departments could keep bags at headquarters. Once a seized phone is in a Faraday bag, a remote wipe is impossible, and officers can apply for a search warrant that allows them to search the contents of the phone.[106] Extending the reasonable expectation of privacy test to the cell phone context thus provides a thoroughly workable balance between law enforcement and privacy interests: It would prevent remote wipes, allow officers immediately to follow leads regarding an arrestee's criminal contacts, and require officers to obtain a warrant before conducting a more intrusive search of the phone's contents.

Perhaps the best objection to a rule allowing searches of information that is both stored in the phone and disclosed to third parties is that the process of accessing such information would reveal information in which an individual retains a right of privacy. Under the

103. *iOS: Understanding Airplane Mode*, APPLE (Sept. 19, 2012), http://support.apple.com/kb/HT1355.

104. *See* United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012).

105. *See, e.g.*, *Mobile Phone Blocking Bag*, FORENSIC STORE, http://forensicstore.com/product/isolation-solutions/mobile-phone-blocking-bag (last visited Mar. 8, 2014) (selling a mobile phone Faraday bag for ten dollars).

106. Any delay in waiting for a warrant to issue involves a danger that the phone's battery will die and that the phone will require a password to turn on again. But if police have some reason to believe this is likely on a phone they have seized, they might be able to search the phone without a warrant under the exigency requirement.

plain view doctrine, an officer may seize an item when he does not "violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed," the item's "incriminating character" is "immediately apparent," and the officer has a "lawful right of access to the object itself."[107] While some commentators have advocated eliminating or curtailing the plain view doctrine in the context of digital searches,[108] every federal circuit court to consider the issue has concluded that the plain view doctrine applies in the digital context.[109] The plain view doctrine's impact may prove minimal, however, because a cell phone's number, recently called numbers, and recently texted numbers are easily accessible from most phones' home screens.[110] Training law enforcement officers to access this information without opening unauthorized screens should prove simple on the vast majority of phones, as a small number of cell phone operating systems dominate the market.[111]

V. THE APPROACH APPLIED TO *WURIE* AND *RILEY*

In the spring of 2014, the Supreme Court will decide two cell phone SIA cases: *United States v. Wurie*[112] and *People v. Riley*.[113]

---

107. Horton v. California, 496 U.S. 128, 136–37 (1990) (internal quotation marks omitted).

108. *See, e.g.*, United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, C.J., concurring). Most of these criticisms, however, derive from the nature of warranted digital searches, in which law enforcement personnel copy a hard drive and use sophisticated forensics tools to analyze its contents. In contrast, a cell phone SIA retains greater similarity to physical analogues. Although a forensic search of a hard drive reveals the entire contents of the drive, *see id.* at 1179, a search of a cell phone incident to arrest requires the officer to click through various screens to find the object of her search, in the same way that an officer executing a warrant would walk up the stairs or pass through various rooms in a house to arrive at the area to be searched.

109. *See, e.g.*, United States v. Highbarger, 380 F. App'x 127, 131 (3d Cir. 2010); United States v. Williams, 592 F.3d 511, 522–24 (4th Cir. 2010); United States v. Miranda, 325 F. App'x 858, 860 (11th Cir. 2009).

110. *See, e.g.*, United States v. Flores-Lopez, 670 F.3d 803, 807 (7th Cir. 2012) (discussing the ease with which a searching officer may access a phone's assigned number).

111. *See* Press Release, International Data Corporation, Android and iOS Continue to Dominate the Worldwide Smartphone Market with Android Shipments Just Shy of 800 Million in 2013 (Feb. 12, 2014) http://www.idc.com/getdoc.jsp?containerId=prUS24676414. Many law enforcement agents will probably already be familiar with these operating systems because they run on the agents' phones, and in fact the two largest operating systems are so similar that they have given rise to high-profile litigation. *See* Paul M. Barrett, *Apple's War on Android*, BLOOMBERG BUSINESSWEEK (Mar. 29, 2012), http://www.businessweek.com/articles/2012-03-29/apple-s-war-on-android. In situations in which officers find incriminating evidence on phone screens they were not entitled to access, courts may either suppress the evidence gathered in the search or admit it pursuant to the good faith or inevitable discovery exceptions to the warrant requirement, just as they would when an officer exceeded the scope of a search warrant. *See, e.g.*, Camreta v. Greene, 131 S. Ct. 2020, 2038 (2011) (Kennedy, J., dissenting).

112. United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), *cert. granted*, 134 S. Ct. 999 (2014) (considering whether recently dialed numbers may be searched incident to arrest).

This Section discusses how, using the approach set forth in this Note, the Supreme Court should allow the search of the recently dialed numbers on Wurie's phone, allow the use of Riley's location data, and exclude photographic and video evidence found on Riley's phone.

To review, under the rule proposed by this Note, law enforcement officials may only search a cell phone for information exposed to third parties in which the arrestee has no reasonable expectation of privacy — this includes the phone's own number, recently called numbers, and text message envelope information, all of which are exposed to the phone company. It does not include contact lists, photographs, or videos that are stored on the phone. If, in the course of obtaining permissible information, an officer sees other incriminating evidence, he may seize or preserve it under the plain view doctrine.

A. Application to United States v. Wurie

Brima Wurie was arrested for distributing crack cocaine and had two phones, cash, and a set of keys seized from him.[114] At the police station, one of Wurie's phones "was repeatedly receiving calls from a number identified as 'my house' on the external caller ID screen on the front of the phone."[115] Officers opened the phone, revealing a wallpaper image of a woman holding a baby, viewed the phone's call log, and accessed the phone number associated with "my house."[116] Using the Internet, officers determined the address associated with the "my house" phone number, went to the address, and, through a window, saw a woman resembling the woman on Wurie's cell phone wallpaper.[117] The officers obtained a warrant and searched the residence, seizing drugs, drug paraphernalia, a firearm, ammunition, and cash.[118]

Under the theory set forth by this Note, every piece of evidence should be admissible against Wurie. Officers learned of the calls from "my house" when a notification appeared on the external screen, in their plain view. Because Wurie necessarily exposed contacted numbers to the telephone company and thereby surrendered his reasonable expectation of privacy in them, officers were entitled to search the phone for recently called numbers, including the number associated with "my home." Accessing a list of these calls required opening the phone and viewing the home screen, placing the wallpaper image in

113. People v. Riley, D059840, 2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013), *cert. granted in part*, 134 S. Ct. 999 (2014) (considering whether photographs and videos stored in a phone and carrier location data may be searched).

114. *Wurie*, 728 F.3d at 2.

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

plain view. Once officers discovered the number of "my home," they were entitled to determine the address associated with the number and use the information they had gathered through the phone search to obtain a search warrant.

B. Application to People v. Riley

A San Diego police officer stopped David Riley for driving with expired registration tags, and after learning that Riley was driving with a suspended license, the officer decided to impound Riley's Lexus.[119] In the course of the impoundment inventory check another officer discovered "a .40 caliber handgun and a .45 caliber handgun hidden in a sock inside the engine compartment."[120] Riley was arrested, and his phone was seized.[121] At the station, a detective opened Riley's cell phone and discovered evidence of gang affiliation in the contacts list, photographs, and videos stored on the phone.[122] Investigators later discovered through cell tower records that Riley's phone was used near the location of an unsolved shooting "at around the time of the shooting" and was used again near the location of the hidden car (owned by Riley) driven by the shooters.[123]

Under the approach outlined in this Note, the Supreme Court should allow the evidence regarding Riley's location but should suppress the evidence gained from the search of his phone. Riley exposed his location information to his cell phone provider, and under the third party rule, he enjoys no reasonable expectation of privacy in this information under the Fourth Amendment. To obtain cell tower location information, officers need only obtain a court order under the Stored Communications Act.[124] However, the Act has no suppression remedy, so even if the government violated the Act, the exclusionary rule would not bar the use of the location information at trial.[125] In contrast, Riley held a reasonable expectation of privacy in the information on his phone, including the names in his contact list and any photos or videos he stored on the phone. Indeed, the facts of *Riley* embody the fear that incident to any arrest police may engage in "exploratory

119. People v. Riley, D059840, 2013 WL 475242, at *2 (Cal. Ct. App. Feb. 8, 2013).
120. *Id.* at *1.
121. *Id.* at *2.
122. *Id.* at *3.
123. *Id.* at *2.
124. *See* 18 U.S.C. §§ 2703(c)(1), 2703(d) (2012). The legal standard for issuance of a court order is less burdensome than for issuance of a warrant; a court order requires only "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d).
125. *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 817 & n.61 (2003) (noting the lack of a suppression remedy in the Stored Communications Act).

rummaging" through the intimate information on an arrestee's phone.[126] Evidence of gang affiliation discovered by the detective should therefore be suppressed.

VI. CONCLUSION

Most courts to consider the treatment of cell phones seized incident to arrest have applied traditional SIA doctrine to uphold full searches of the phone. Perhaps unsurprisingly, many of these courts have expressed concern about the privacy interests implicated, but noted that, absent guidance from the Supreme Court, they can reach no other decision.[127] Courts that have taken a different tack in an attempt to protect privacy interests have created flawed rules that often rely on strained readings of precedent.

However, in the recent *Jones* case, the Supreme Court articulated two separate sources of Fourth Amendment protection: the common law trespassory test for physical searches and the reasonable expectation of privacy test for informational searches. Courts can fully adhere to SIA precedent and protect the privacy interests in arrestees' cell phones by giving meaning to both sources of protection: using the physical trespass test to determine whether officers may access a seized phone under traditional SIA doctrine, and using the reasonable expectation of privacy test to cabin any resulting searches. As evidenced by application to *Wurie* and *Riley*, the rule allows for limited searches of the information an arrestee has already exposed to third parties (like the recently called numbers in *Wurie*) but precludes officers from sifting through the photographs and videos on an arrestee's phone (as occurred in *Riley*). This rule provides a faithful reading of Supreme Court precedent, upholds the privacy interest in an arrestee's cell phone, and permits officers to prevent the destruction of evidence.

126. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

127. *See* United States v. Gomez, 807 F. Supp. 2d 1134, 1146 (S.D. Fla. 2011) ("Even though we may disagree with the application of [Supreme Court precedent] to the ever-advancing technology of cell phones . . . we are constrained to apply the law as the Supreme Court currently pronounces it."); United States v. Hill, No. CR 10-00261 JSW, 2011 WL 90130, at *7 (N.D. Cal. 2011).