

Back to the Future: Returning to Reasonableness and Particularity Under the Fourth Amendment

*Adam Lamparello & Charles MacLean**

*ABSTRACT: Nothing speaks with more constitutional clarity than an unreasonable search. There can be no doubt—in an era of unprecedented technological advances—that individual privacy is under attack by state action that no honest jurist can consider reasonable. In *Riley v. California* and *United States v. Wurie*, the United States Supreme Court will have a golden opportunity to secure privacy rights for the future when it decides whether searches incident to arrest permit law enforcement officers to search, without a warrant, the contents of an arrestee’s cell phone. The answer to that question is no.*

I. INTRODUCTION.....	102
A. RILEY—A MISGUIDED APPLICATION OF THE SEARCH INCIDENT DOCTRINE TO SEARCHES OF A CELL PHONE’S CONTENTS.....	102
B. WURIE—THE RIGHT RESULT, BUT AN UNANSWERED QUESTION.....	103
II. CELL PHONES ARE THE MODERN DAY REPOSITORY FOR “PAPERS” AND “EFFECTS”	105
III. THE RILEY COURT GOT IT WRONG.....	107
A. THE UNFETTERED SEARCH OF RILEY’S CELL PHONE IMPERMISSIBLY INFRINGEMENTS UPON PERSONAL PRIVACY RIGHTS.....	107
B. TRADITIONAL EXCEPTIONS TO THE WARRANT REQUIREMENT DID NOT SUPPORT THE SEARCH OF RILEY’S CELL PHONE	109
C. HISTORICAL THIRD-PARTY DOCTRINE RULES ARE NOT APPLICABLE TO MODERN CELL PHONES.....	109
IV. RETURNING TO REASONABLENESS: THE SEIZE BUT DON’T SEARCH APPROACH.....	110

* Assistant Professors of Law, Indiana Tech Law School.

A.	<i>THE NARROW EXCEPTION: IMMINENT EXIGENCIES</i>	111
1.	Ongoing Crimes and Imminent Threats to Persons	111
2.	Remote Deletion	113
B.	<i>THE “REASONABLE RELATIONSHIP” DOCTRINE IS UNWORKABLE</i>	113
V.	CONCLUSION	114

I. INTRODUCTION

The Supreme Court recently granted certiorari in *Riley v. California*¹ and *United States v. Wurie*,² to consider whether evidence resulting from the warrantless search of an arrestee’s cell phone was properly admitted at trial. In *Riley*, the California Court of Appeals held that the search-incident-to-arrest doctrine³ permitted the search of an arrestee’s cell phone contents.⁴ In *Wurie*, the First Circuit reached the opposite result.⁵ By granting certiorari for both cases, the Court may be signaling that it intends to adopt a “middle ground” approach that strengthens privacy protections in the digital age, but gives law enforcement sufficient latitude to conduct warrantless searches where the facts warrant. This Essay argues that a “seize but don’t search” model, where officers are allowed to seize an arrestee’s cell phone to preserve evidence, but not search its contents without a warrant—or an imminent exigency—strikes the proper constitutional balance. Absent such a ruling, warrantless searches of cell phones, which house the “papers” and “effects” traditionally protected by the Fourth Amendment,⁶ will become the new general warrants, effectively trumping the Constitution’s written *and* unwritten guarantees of privacy.

A. RILEY—A MISGUIDED APPLICATION OF THE SEARCH INCIDENT DOCTRINE TO SEARCHES OF A CELL PHONE’S CONTENTS

David Leon Riley, a member of the Lincoln Park gang, was standing by his car when a rival gang member drove by and sparked a gunfight.⁷ Riley was later arrested and, during the arrest, the officers seized Riley’s cell phone

1. *People v. Riley*, No. Do59840, 2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013), *review denied* (May 1, 2013), *cert. granted in part*, *Riley v. California*, 134 S. Ct. 999 (2014).

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

3. *See Chimel v. California*, 395 U.S. 752, 762–63 (1969) (holding that a law enforcement officer could search areas “within the immediate control” of a suspect, for the purpose of: (1) protecting the officer’s safety; and (2) preventing the destruction of evidence); *Preston v. United States*, 376 U.S. 364, 367 (1964) (discussing the two justifications that permit searches incident to arrest).

4. *Riley*, 2013 WL 475242 at *6.

5. *Wurie*, 728 U.S. at 13.

6. *See* U.S. CONST. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”).

7. *Riley*, 2013 WL 475242, at *1.

from his person and briefly looked through the phone's various displays.⁸ After discovering evidence suggesting gang involvement, the arresting officers gave Riley's cell phone to a detective specializing in gangs.⁹ That gang officer found various incriminating photographs and video clips on Riley's cell phone.¹⁰

The trial court allowed the photographs and video clips seized from Riley's cell phone as well as locational data from his cell phone records to be admitted into evidence.¹¹ The California Court of Appeals affirmed, holding that "Riley's cell phone was immediately associated with his person when he was arrested, and therefore the search of his cell phone was lawful whether or not an exigency still existed."¹² The California Court of Appeals did not assess whether the search was necessary to protect the officer's safety or to preserve evidence, or whether Riley had a reasonable expectation of privacy in the contents of his phone. Most courts have reached a similar result.¹³ In *Wurie*, however, the First Circuit reached the opposite result and set the stage for a landmark Supreme Court decision.

B. WURIE—THE RIGHT RESULT, BUT AN UNANSWERED QUESTION

In *Wurie*, the defendant was arrested and charged with distributing cocaine.¹⁴ After being transported to the police station, officers noticed in plain view on the visible screen of one of Wurie's cell phones that his phone "was repeatedly receiving calls from a number identified as 'my house.'"¹⁵ A few minutes later, officers opened that cell phone, saw that a photo of a Black female was the screensaver, and by pushing two buttons on the phone determined that "my house" had a particular phone number associated with it.¹⁶ Officers then determined the address associated with the "my house" phone number and drove to that address; upon arrival, officers noted the mailbox indicated "Wurie and Cristal," and through the front window, officers saw a female matching the screensaver on Wurie's cell phone.¹⁷ Officers obtained a search warrant for that address and recovered 215 grams of crack

8. *Id.* at *1–2.

9. *Id.* at *3.

10. *Id.*

11. *Id.*

12. *Id.* at *6 (citing *People v. Diaz*, 244 P.3d 105, 110 (Cal. 2011)).

13. *See, e.g.,* *Silvan W. v. Briggs*, 309 Fed. Appx. 216, 225 (10th Cir. 2009); *United States v. Gomez*, 807 F. Supp. 2d 1134, 1145–46 (S.D. Fla. 2011); *United States v. McCray*, 2009 WL 29607, at *2–4 (S.D. Ga. Jan 5, 2009); *United States v. Cote*, 2005 WL 1323343, at *6 (N.D. Ill. May 26, 2005); *see also* Margaret M. Lawton, *Warrantless Searches and Smartphones: Privacy in the Palm of Your Hand?*, 16 UDC/DCSL L. REV. 89, 104, 105 & nn. 112–17 (2012); Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 38, 39 & n.82 (2008).

14. *State v. Wurie*, 728 F.3d 1, 2 (1st Cir. 2013).

15. *Id.*

16. *Id.*

17. *Id.*

cocaine, a firearm, and ammunition, among other items.¹⁸ Wurie moved to suppress the warrantless cell phone search and its fruit, but the trial court denied the suppression motion; a jury subsequently found Wurie guilty of all counts, and he was sentenced to over twenty-one years in prison.¹⁹

The First Circuit reversed, holding that neither officer safety²⁰ nor the preservation of evidence²¹ justified the search. The court held that “warrantless cell phone data searches are *categorically* unlawful under the search-incident-to-arrest exception, given the government’s failure to demonstrate that they are ever necessary to promote officer safety or prevent the destruction of evidence.”²² The court likened warrantless cell phone data searches to a “general evidence-gathering search,” providing a “convenient way for the police to obtain information related to a defendant’s crime of arrest—or other, as yet undiscovered crimes—without having to secure a warrant.”²³

Furthermore, the First Circuit recognized that the information stored on cell phones is “of a highly personal nature,” and includes “photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records.”²⁴ Simply stated, it was “the kind of information one would previously have stored in one’s home.”²⁵ The First Circuit held as follows:

[Allowing for searches of cell phone memories as a bright-line rule] would give law enforcement automatic access to “a virtual warehouse” of an individual’s “most intimate communications and photographs without probable cause” if the individual is subject to a custodial arrest, even for something as minor as a traffic violation.²⁶

Thus, “[a]llowing the police to search that data without a warrant any time they conduct a lawful arrest would, in our view, create ‘a serious and

18. *Id.*

19. *Id.*

20. The First Circuit found that cell phone memories virtually never pose a threat to officer safety. *See id.* at 10.

21. As the First Circuit found, evidence on cell phone memories can be easily and inexpensively safeguarded from destruction by (1) turning off the cell phone; (2) removing its battery; (3) placing the cell phone in a Faraday enclosure; or (4) copying the entire contents to preserve them for later search pursuant to a validly issued search warrant. *Id.* at 11; *see also* Charles E. MacLean, *But, Your Honor, a Cell Phone Is Not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 37, 50 (2012).

22. *Wurie*, 728 F.3d at 12.

23. *Id.* at 10 (quoting *Thornton v. United States*, 541 U.S. 615, 632 (2004) (Scalia, J., concurring)) (internal quotation marks omitted).

24. *Id.* at 8 (citation omitted).

25. *Id.*

26. *Id.* at 9 (citation omitted).

recurring threat to the privacy of countless individuals.”²⁷

So which court got it right? Neither. *Riley* made the problem worse, but *Wurie* left unanswered questions. Given that the Supreme Court granted certiorari in both cases, its decision is likely to fall somewhere in the middle. This Essay offers a solution that reflects the important privacy interests at stake, is consistent with the Fourth Amendment’s reasonableness and particularity requirements, and gives law enforcement sufficient discretion where the facts warrant.

II. CELL PHONES ARE THE MODERN DAY REPOSITORY FOR “PAPERS” AND “EFFECTS”

A cell phone cannot be analogized to a crumpled up cigarette package,²⁸ address book,²⁹ wallet,³⁰ or container.³¹ Even though *certain* features of a cell phone—for example, call logs and outgoing text messages, which are the primary functions of older, more basic cell phones—are somewhat similar, the storage capacities³² and technological capabilities of modern-day devices such as smartphones make them entirely dissimilar to traditional physical objects.

Unlike a container, for example, a cell phone is not an “object capable of holding another object.”³³ “Cell phone contents by contrast are limited to digital data, the intangible nature of which renders it unavailable for use as a weapon or as evidence that can be physically destroyed.”³⁴ In addition, “modern cell phones are capable of accessing almost limitless amounts of data,”³⁵ and “‘cloud’ technology means that to a growing extent cell phone contents are only available by linking wirelessly to a remote cellular relay tower.”³⁶ In fact, “[e]ven the more basic models of modern cell phones are capable of storing a wealth of digitized information wholly unlike any physical

27. *Id.* at 14 (quoting *United States v. Gant*, 556 U.S. 332, 345 (2009); *cf.* *United States v. Jones*, 132 S. Ct. 945, 950 (2011) (“At bottom, we must ‘assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’” (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001))).

28. *United States v. Robinson*, 414 U.S. 218, 236 (1973); *see also* MacLean, *supra* note 21, at 52–53.

29. *United States v. Rodriguez*, 995 F.2d 776, 778 (7th Cir. 1993).

30. *Id.*

31. Joshua Eames, Note, “*Can You Hear Me Now?*”: Warrantless Cell Phone Searches and the Fourth Amendment; *People v. Diaz*, 244 P.3d 501 (Cal. 2011), 12 WYO. L. REV. 483, 499–500 (2012).

32. *See* Mark L. Mayakis, Comment, *Cell Phone—A “Weapon” of Mass Discretion*, 33 CAMPBELL L. REV. 151, 161 (2010) (“Even the ‘more basic models of modern cell phones’ have the technological capabilities of storing and transmitting exponentially greater amounts of private information than that of a pager or any traditional closed container.” (citation omitted)).

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

34. Eames, *supra* note 31, at 499.

35. *Id.*

36. *Id.*

object found within a closed container.”³⁷

Additionally, cell phones are not merely objects capable of storing massive amounts of private data, and are not analogous to a car, an office, or even a house. Instead, they are a modern extension of the mind, and a vehicle for free speech. A cell phone’s contents often contain intimate and highly personal information, such as confidential documents, private messages, videos, data from internet searches, and *thoughts*.³⁸

[M]odern cellular phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures. 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.³⁹

As a result, “cell phones have quickly become a storehouse of sorts for holding such information as private correspondence, photographs, *personal thoughts*, and in some cases even the personal information of others.”⁴⁰ This, in turn “increases the likelihood that highly personal information, irrelevant to the subject of the lawful investigation, will also be searched or seized.”⁴¹

Thus, “[a]lthough information of this nature can now be stored electronically, in the past such information has traditionally been stored in one’s home office or desk and given protection by the Fourth Amendment.”⁴² In his dissent in *United States v. Seljan*, Judge Alex Kozinski acknowledged as follows:

The reference to papers [in the Fourth Amendment] is not an accident; it’s not a scrivener’s error. It reflects the Founders’ deep concern with safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the government. . . .

. . . [T]he Founders were as concerned with invasions of the mind as with those of the body, the home or personal property—which is why they gave papers equal rank in the Fourth Amendment litany. . . .

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

38. *See United States v. Park*, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007) (footnote omitted); Eames, *supra* note 31, at 499 (2012) (“[C]ell phone searches potentially expose to public scrutiny almost limitless information of the most private nature.”).

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

40. Jana L. Knott, Note, *Is There an App for That? Reexamining the Doctrine of Search Incident to Lawful Arrest in the Context of Cell Phones*, 35 OKLA. CITY U. L. REV. 445, 456 (2010) (emphasis added).

41. Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 105 (1994).

42. Knott, *supra* note 40, at 456.

....

... Papers contain people's most personal information, . . . "sealed up in silence, not to be broke, but with their own heart-strings," so that "some men would rather die" than submit to having their papers searched.⁴³

In many ways, cell phones are not phones at all. These devices are an amalgamation of so many things that have historically been considered essential to free expression and have thus been accorded the highest degree of constitutional protection. Searching a cell phone's memory is, in essence, searching "persons" *and* their "papers." The right to conduct such a search gives law enforcement license to rummage through an individual's private life—and *mind*. Given these realities, there can be no doubt that individuals have an objectively reasonable expectation of privacy in the contents of their cell phones—and that *Riley* should be reversed.

III. THE *RILEY* COURT GOT IT WRONG

The California Court of Appeals reached the wrong result. First, the court conflated the words "immediate association" with the purposes underlying a search incident to arrest. Even if the cell phone was immediately associated with Riley's "person," it neither threatened the officers' safety nor presented a risk that evidence would be destroyed. Of course, while a cell phone's contents can be erased by automatic or remote deletion, the likelihood is so rare that it does not justify warrantless searches incident to arrest.⁴⁴ Surprisingly, however, the Court of Appeals made no attempt to establish a nexus between the justifications for a search incident to arrest, and the subsequent search of Riley's cell phone. In addition, the California Court of Appeals failed to consider whether the search of Riley's cell phone should be limited in scope, purpose, or duration. For example, the court could have allowed law enforcement to search only those areas of the phone where evidence of the crime of arrest was likely to be found.

A. *THE UNFETTERED SEARCH OF RILEY'S CELL PHONE IMPERMISSIBLY INFRINGES UPON PERSONAL PRIVACY RIGHTS*

Moreover, the court could have restricted the search to those areas where Riley had a reduced expectation of privacy, such as the outgoing call log or text messages sent in the past 48 hours. Of course, there is nothing problematic about saying that a cell phone is "immediately associated" with the person, if this term is construed as an association with the person's

43. *United States v. Seljan*, 547 F.3d 993, 1014–17 (9th Cir. 2008)) (Kozinski, J., dissenting) (emphasis added) (citation omitted), *cert. denied*, 129 S. Ct. 1368 (2009).

44. See, e.g., 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, 394–96 (2013) (explaining that modern technology has all but eliminated the risk of remote deletion).

thoughts, private “papers,” and personal “effects.”⁴⁵

For all other, more personal areas of Riley’s cell phone, the court could have mandated that, in the absence of exigent circumstances, probable cause and a warrant were required. It did none of these things.

Instead, the California Court of Appeals permitted an unfettered search of Riley’s cell phone, essentially sanctioning a suspicionless fishing expedition into his personal life. Neither the search-incident-to-arrest doctrine, nor the text of the Fourth Amendment—which requires that searches be “reasonable”—countenances such an unbridled infringement on personal privacy. The court’s decision effectively meant that Riley sacrificed his privacy rights the moment they placed him under arrest. By way of analogy to the Fifth Amendment’s right against self-incrimination, such a result is tantamount to holding that a suspect surrenders his right to silence the moment police place him under arrest. The Constitution, however, does not allow for the forfeiture of fundamental rights, particularly when a suspect needs them the most.

To be sure, even if the California Court of Appeals believed that Riley had no expectation of privacy in his cell phone, it would not necessarily justify a warrantless and unrestricted search of his cell phone.⁴⁶ There is a constitutionally significant distinction between an individual’s expectation of privacy in a cell phone *as an object*, and as the safe keeper of the “papers” and “effects” that the Fourth Amendment has *always* deemed private. Surely, for example, an individual has at least *some* expectation of privacy in personal documents stored on a cell phone, videos downloaded from YouTube, or private emails sent from an email account.

Of course, this does not immunize the information from a valid search, but it does require law enforcement to have probable cause and to secure a warrant that delineates with particularity the places to be searched. Otherwise, information historically designated as worthy of the most stringent privacy safeguards would suddenly lose its constitutional protections simply because an individual decided to store it in a cell phone rather than a closet. Such a result cannot qualify as reasonable under the Fourth Amendment, because it would allow an individual’s efficient use of technology to constitute an implicit waiver of basic civil liberties.

B. TRADITIONAL EXCEPTIONS TO THE WARRANT REQUIREMENT DID NOT SUPPORT

45. United States v. Wurie, 728 F.3d 1, 10 (quoting U.S. v. Chadwick, 433 U.S. 1, 15 (1977), abrogated by California v. Acevedo, 500 U.S. 565 (1991)); U.S. CONST. amend. IV.

46. See, e.g., Howard E. Wallin, *Plain View Revisited*, 22 PACE L. REV. 307, 324 (2002) (stating that, places “where privacy is not protected by the Constitution,” garner no protection from the Fourth Amendment). This reasoning, however, does not apply to searches of a cell phone’s contents, because the contents themselves include items traditionally afforded protection by the Fourth Amendment.

THE SEARCH OF RILEY'S CELL PHONE

It is not surprising, therefore, that neither the search-incident-to-arrest doctrine, nor any other exceptions to the warrant requirement, supported the search of Riley's cell phone. After all, the Court's Fourth Amendment jurisprudence is based on whether, prior to a search, it would be *reasonable* to require law enforcement to obtain a warrant. Indeed, where the Court has created exceptions to the warrant requirement, they have been based on impracticability and inevitability. Impracticability, for example, exists when procuring a warrant would lead to the destruction of evidence or threaten the life or safety of others. Certainly, no one would argue that it would be unreasonable to proceed without a warrant under such circumstances.

While a bit more complicated, inevitability nonetheless reflects the primacy of reasonableness in the constitutional analysis. Inevitability is present when an officer sees an item in plain view in a place where the officer is *lawfully* present.⁴⁷ While police officers maintain a lawful presence when securing a valid arrest, and can seize the cell phone to preserve evidence, there is nothing to "see" in plain view *unless* the officer initiates a *second*, warrantless search of the cell phone's memory. This can occur by simply pushing buttons on the cell phone, which will allow law enforcement to search, among other things, an arrestee's email, text messages, or applications. In so doing, however, the officer's "presence" becomes unlawful; the officer has entered an "area" where the search for evidence includes objects traditionally afforded Fourth Amendment protection. And the officer has done so without impracticability, inevitably, or exigency. Law enforcement—and the courts—need another reason. They cannot find one, however, because it does not exist in precedent—or in the Fourth Amendment.

C. HISTORICAL THIRD-PARTY DOCTRINE RULES ARE NOT APPLICABLE TO MODERN CELL PHONES

Some courts have relied on the third-party doctrine⁴⁸ to hold that a cell phone user's Google searches constitute a voluntary disclosure (thus surrendering Fourth Amendment protections), because the user knows that the search will be transmitted through a server. Importantly, however, "the Supreme Court decisions that established the third-party doctrine are decades old,"⁴⁹ and cell phones, just as they are not containers or address books, are unlike bank records voluntarily conveyed to banks in the ordinary course of

47. *See id.* at 325 (the plain view exception applies only where "an officer has already justifiably intruded into a constitutionally-protected area, spots and then removes incriminating evidence").

48. Jeremy H. Rothstein, Note, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 506–11 (2012).

49. *Id.* at 506.

business.⁵⁰ The exposure of cell phone data is also not comparable to “exposing numerical information to the telephone company,”⁵¹ because cell phone data includes an exponentially higher volume of data than landlines did decades ago and that data is of a more diverse and personal nature. Further, individuals should not be required to “assum[e] the risk that the company would turn over that [amount of personal] information to the government.”⁵²

If this traditional reasoning were applied to cell phones, it would, in effect, condition the downloading and storage of traditionally private information—for example, confidential legal documents, upon the knowing waiver of constitutional rights. No conception of reasonableness can support this view, because it would result in an unconstitutional chill, through a de facto prior restraint, on speech and other expressive activity. It would also require the assumption, under *Katz v. United States*,⁵³ that individuals do not have an objectively reasonable expectation of privacy⁵⁴ in *otherwise private* material simply because they know it may be viewed by an unidentified third party, for whatever reason, and disclosed to the government. That logic might work for bank records that are given to tellers, or numbers that are dialed from a home phone.

It goes too far, however, when applied to private information that reveals intimate details about individuals, and embraces a concept of disclosure that is incompatible with the role cell phones play in the digital age. Individuals are not ‘disclosing’ information in the traditional sense; they are capitalizing on the efficiency cell phones offer and the ubiquitous role they play in modern human interaction. Comparing a Google search to the act of handing over bank records to a teller fails to appreciate these differences, and ignores the fact that “disclosure” in this context is not to a single person, but to the entire world. That requires more, not less, protection.

IV. RETURNING TO REASONABLENESS: THE SEIZE BUT DON’T SEARCH APPROACH

The “seize but don’t search” approach would: (1) allow law enforcement to seize an arrestee’s cell phone; (2) require a warrant and probable cause to search the phone’s contents; and (3) provide a narrow exception for imminent exigencies that threaten human life or safety. Most importantly, it would give life to the Fourth Amendment’s reasonableness and particularity requirements. It would also prevent an arrestee from destroying evidence or coordinating with third parties to remotely delete the cell phone’s memory,

50. *Id.* at 506–07 (discussing *United States v. Miller*, 425 U.S. 435 (1976)).

51. *Id.* at 507 (discussing *Smith v. Maryland*, 442 U.S. 735 (1979)).

52. *Id.*

53. 389 U.S. 347.

54. *Katz* advocated that the Fourth Amendment is triggered only where an individual can demonstrate both an objective and subjective expectation of privacy. *Id.* at 361 (Harlan, J., concurring).

while also prohibiting authorities opening a “door into the most private details of an arrestee’s life.”⁵⁵ For that, law enforcement needs probable cause, and a warrant detailing with particularity the areas of a phone to be searched.

The Supreme Court has already inched in this direction. In *Arizona v. Gant*, for example, police arrested the defendant for driving with a suspended license.⁵⁶ While the defendant was handcuffed and in the back of a police car, law enforcement searched his car and found a jacket containing cocaine.⁵⁷ The Court held that the search was improper because the officers’ safety was not at risk,⁵⁸ and, because they had no reason “to believe evidence relevant to the crime of arrest might be found in the vehicle.”⁵⁹ In so holding, the Court narrowed its prior decision in *New York v. Belton*,⁶⁰ which had endorsed a bright-line rule permitting law enforcement to search the entire interior of automobiles (except the trunk) following a valid arrest. The majority recognized that, where neither of the justifications for a search incident to arrest is present, law enforcement may not search a vehicle’s interior without probable cause.⁶¹

A. THE NARROW EXCEPTION: IMMINENT EXIGENCIES

Exigencies are likely to arise where law enforcement officers have an objectively reasonable belief that: (1) a crime is ongoing, and imminent threats to persons exist; and (2) a cell phone’s memory will be remotely deleted.⁶²

1. Ongoing Crimes and Imminent Threats to Persons

Where law enforcement officers have an objectively reasonable belief that

55. Casenote, *Criminal Procedure—Fourth Amendment—Florida Supreme Court Holds that Cell Phone Data Is Not Subject to the Search-Incident-to-Arrest Exception*—*Smallwood v. State* 113 So. 3d 724 (Fla. 2013), 127 HARV. L. REV. 1059, 1063 (2014).

56. *Arizona v. Gant*, 556 U.S. 332, 335 (2009).

57. *Id.*

58. *Id.* at 343 (holding a search of the passenger compartment would only be permissible if “the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search”).

59. *Id.* (quoting *Thornton v. United States*, 541 U.S. 615, 632 (2004) (Scalia, J., concurring)) (internal quotation marks omitted).

60. 453 U.S. 454 (1981).

61. *Gant*, 556 U.S. at 351; see also Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1136 (2011).

62. Mireille Dee, Notem *Getting Back to the Fourth Amendment: Warrantless Cell Phone Searches*, 56 N.Y.L. SCH. L. REV. 1129, 1160 (2012) (“[A] court deciding whether a particular warrantless cell phone search was lawful should engage in only one colloquy—whether there were exigent circumstances justifying the search, specifically, whether information on the cell phone was actually subject to remote deletion at the moment of the search.” (footnote omitted)); see also Beutler, *supra* note 44, at 393 (“The [exigent circumstances] exception requires the reasonable belief by a law enforcement officer that evidence is in imminent danger of being removed or destroyed.” (citation omitted)).

an “immediate threat to life or safety”⁶³ exists, they should be entitled to search a cell phone without a warrant. One scholar explains the exigent circumstances exception as follows:

[P]olice may enter premises and conduct a search without a warrant “to provide emergency assistance to an occupant,” or to “enter a burning building to put out a fire and investigate its cause.” In such cases, the law not only dismisses the warrant requirement—in appropriate circumstances, the police may act even in the absence of probable cause.⁶⁴

Of course, to invoke this exception, an officer “must have had probable cause for the intrusion,”⁶⁵ or, as applied to the cell phone context, the valid arrest.

Furthermore, to prevent the exception from swallowing the rule, law enforcement must demonstrate that the exigency presented an imminent threat to the life or physical safety of others. Otherwise, law enforcement might interpret “safety” in a manner that encompasses any threat, no matter how minor, attenuated, or speculative. This exception would apply in situations where law enforcement has an objectively reasonable belief that: (1) criminal behavior is ongoing; (2) a specific intent to harm others is present; (3) the harm, including loss of life, is likely to occur; and (4) the search is limited to areas that are likely to uncover evidence relating to the exigency.

In some situations, this may include initiating or responding to a call or text message, or reviewing the arrestee’s recent phone calls or emails.⁶⁶ It will not ordinarily (and perhaps never), include a search of, for example, the arrestee’s Google search history or purchases on Amazon.com. Additionally, the search must cease when the exigency dissipates, or when officers discover evidence—in the cell phone or elsewhere—that allows them to effectively address the problem. Simply stated, law enforcement officers must act reasonably.⁶⁷ If a warrantless search exceeds the narrow parameters delineated above, and no other recognized exception applies, then any resulting evidence should be suppressed at trial.

63. Clifford S. Fishman, *Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable Cause Requirements*, 65 RUTGERS L. REV. 995, 1002 (2013); see also Eunice Park, *Traffic Ticket Reasonable, Cell Phone Search Not: Applying the Search-Incident-To-Arrest-Exception to the Cellphone as “Hybrid”*, 60 DRAKE L. REV. 429, 488 (2012) (“Exigent circumstances arise when the inevitable delay incident to obtaining a warrant must give way to a need for immediate action.” (quoting *United States v. Forker*, 928 F.2d 365, 368 (11th Cir. 1991))).

64. Fishman, *supra* note 63, at 1002–03 (citations omitted) (footnote omitted).

65. *Id.* at 1003–04 (footnote omitted).

66. *Id.* at 1004–05 (discussing the scope of cell phone searches when officers are faced with exigent circumstances).

67. *United States v. Knights*, 534 U.S. 112, 118 (2001) (stating that the Court examines the “totality of the circumstances” to decide if a search is reasonable within the meaning of the Fourth Amendment” (citation omitted)).

2. Remote Deletion

With respect to the remote deletion problem, “[m]any courts have reasoned that a search of a cell phone or personal electronic device incident to arrest is lawful because it is a situation where an officer needs to preserve evidence from destruction.”⁶⁸ Importantly, however, “[r]apid improvements in technology . . . have obviated the . . . concern[]” that “incoming calls or messages will replace recent calls or messages in a phone’s memory.”⁶⁹ Indeed, “[m]odern cell phones no longer store only a handful of recent text messages and phone calls and greatly expanded digital memories eradicate any real risk of automatic deletion.”⁷⁰ Furthermore, since the possibility of remote deletion is unlikely—particularly if police seize the cell phone—law enforcement should be required to demonstrate an actual and *objectively* reasonable belief that such a risk was present.⁷¹ Without this standard, law enforcement could base warrantless cell phone searches on broad and unsubstantiated concerns that would not otherwise be covered under a recognized exception.

B. THE “REASONABLE RELATIONSHIP” DOCTRINE IS UNWORKABLE

Searches should not be allowed simply because the cell phone may contain evidence reasonably related to the crime of arrest.⁷² First, the risk that officers will simply rummage through all “rooms” of the cell phone in an unfettered search for evidence far outweighs the convenience to law enforcement. Second, given the minimal, even non-existent, risk that a cell phone’s memory will be destroyed, there exists no reason whatsoever that could justify such a search.

This second problem relates to the nexus between the crime of arrest and a search of the cell phone’s memory. An individual arrested for possessing images of child pornography, for example, may certainly have images stored in the cell phone interspersed among other, nonrelated data. A warrantless search of the cell phone’s memory, however, cannot be considered reasonable under the Fourth Amendment. Such a search leads to more questions than answers as well as to many potential violations of privacy. For example, would law enforcement be limited to searching the suspect’s incoming and outgoing calls, along with documents that have been downloaded, or can they search the suspect’s Facebook page, Twitter account, and purchases on Amazon.com?

68. Beutler, *supra* note 44, at 394 (citation omitted).

69. *Id.* (citations omitted)

70. *Id.* at 394–95 (citing *United States v. Gomez*, 807 F. Supp. 2d 1134, 1150 n.17 (S.D. Fla. 2011)).

71. *Id.* at 395 (citing *Gomez*, 807 F. Supp. 2d at 1150 n.17).

72. See Ben E. Stewart, Note, *Cell Phone Searches Incident to Arrest: A New Standard Based on Arizona v. Gant*, 99 Ky. L.J. 579, 596–97 (2011).

Likewise, if an individual is arrested for possessing marijuana, can law enforcement examine that individual's Google searches, make a record of that individual's Facebook friends, and analyze every text message that individual sent for the last six months? These questions highlight the temporal and spatial problems raised by vesting law enforcement with this kind of discretion. The resulting uncertainty would increase the likelihood of unnecessarily invasive and arbitrary searches, without any countervailing interest to justify dispensing with the warrant requirement. Procuring a warrant will allow a magistrate to confine the scope of every search, and describe with particularity the areas of a cell phone that are properly subject to a search.⁷³

V. CONCLUSION

The text and original meaning of the Fourth Amendment give individuals a reasonable expectation of privacy in their papers and effects, regardless of whether they are locked in a safe or stored on a cell phone. Technological advances do not give law enforcement the right to breach the constitutional separation between privacy and state action. The divide is there for a reason: to give individuals the freedom to engage in self-expression without the unnerving fear that the government may eavesdrop if they are arrested for, say, a misdemeanor traffic offense. Up to this point, however, the lower courts have largely relied on decades-old case law and principles of stare decisis to tear down the privacy wall. Decisions such as *Riley* have threatened to make privacy as obsolete as pre-digital era case law, and transform the infringements on individual privacy into an epidemic.

For that reason, much depends on the Court overturning *Riley*, and embracing *Wurie*'s reasoning. The Court's decision will have ramifications that extend far beyond cell phones and containers, influencing the Government's approach to border searches and surveillance. Ironically, the path to the future sits at the beginning, in a place where one word speaks for millions: reasonableness.

73. See Fabio Arcila, Jr., *The Death of Suspicion*, 51 WM. & MARY L. REV. 1275, 1294 (2010) (quoting the Fourth Amendment's requirement that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched* and the persons or things to be seized" (emphasis added)).