Brigham Young University Journal of Public Law

Volume 31 | Issue 2 Article 6

4-1-2017

OMG - Not Something to LOL about: The Unintended Results of Disallowing Warrantless Searches of Cell Phones Incident to a Lawful Arrest Comments

Parker Jenkins

OMG—Not Something to LOL About: The Unintended Results of Disallowing Warrantless Searches of Cell Phones Incident to a Lawful Arrest

INTRODUCTION

The Supreme Court addressed the issue of whether police officers must obtain a warrant prior to searching an individual's cell phone incident to a lawful arrest, answering the question with a resounding yes.[1] While the bright-line rule established by the Supreme Court's recent decision in *Riley v. California* appears to be a victory for privacy protection, the rule may also have several negative consequences. Although the decision appeared to be an easy one for the Court to reach, lower courts will now be tasked with sorting out related issues including evolving governmental interests, officers' reliance on alternative exceptions to the warrant requirement, and advancements in technology that would weaken the Court's support for its decision in *Riley*.

The *Riley* decision is important because it potentially impacts every person in the United States that owns a cell phone and keeps any type of personal information stored on such a device. Ninety-one percent of American adults own a cell phone of some sort,[2] with nearly two-thirds of Americans now owning a "smartphone"[3]—a cellular device with internet or cellular network accessing capabilities and an operating system capable of running downloaded applications.[4] Cell phones have become an integral part of society. Cell phones are no longer a rare convenience or commodity that some people have; on the contrary, society is trending towards a deeper

1. Riley v. California, 134 S. Ct. 2473, 2495 (2014) (The Court instructed that the "answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

2. Maeve Duggan, *Cell Phone Activities 2013*, PEW RESEARCH CENTER CTR. 2 (Sept. 16, 2013), http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_Cell%20Phone%20Activities%20May%202013.pdf.

3. Aaron Smith et al., *U.S. Smartphone Use in 2015*, PEW RESEARCH CTR. 2 (Apr. 1, 2015), http://www.pewinternet.org/files/2015/03/PI_Smartphones_0401151.pdf ("64% of American adults now own a smartphone of some kind, up from 35% in the spring of 2011.").

4. *Smartphone*, TECHOPEDIA.COM, https://www.techopedia.com/definition/2977/smartphone (last visited Feb. 18, 2017).

dependence on constant cell phone interaction.[5] Cell phones and smartphones alike are used for numerous functions, many of which are very private or personal in nature to the phone's owner.[6] Indeed, for many Americans, cell phones likely contain "the privacies of life."[7] With cell phone and smartphone ownership, use, and dependence on the rise, the Court's decision comes at a highly influential time.[8]

The Court's decision now gives guidance to arresting officers on what they can and cannot do in searching an arrestee's phone. However, the Court failed to address several issues that are likely to appear before lower courts. Due to the Court's failure to foresee or speak to these issues, the lower courts will likely struggle to reconcile the new issues with the Court's guidance that it is unlawful for officers to search an arrestee's cell phone incident to a lawful arrest. These issues include potential scenarios that the Court did not address in its decision that would bolster the government's interest in having access to an individual's cell phone. Likewise, alternative ex-

5. A recent survey showed that 47% of U.S. adults would not be able to last 24 hours without their cell phones. Smart phones only rank behind the internet and hygiene when ranked by importance in people's lives. Jessica Durando, *47% of Adults Couldn't Last a Day Without Smartphone, Survey Says*, USA TODAY (June 30, 2014, 2:56 PM), http://www.usatoday.com/story/news/nation-now/2014/06/30/consumers-cell-phones-americans/11780165/. Another survey showed that only 28% of people would be able to live without their cell phones, with more people being willing to live without caffeine, sex, or television before they would be willing to give up access to the internet. Allyssa Birth, *More Than 7 in 10 Americans Think Technology Has Become Too Distracting and Is Creating a Lazy Society*, THE HARRIS POLL (Nov. 4, 2015, 5:00 AM), http://www.theharrispoll.com/health-and-life/Technology-Too-Distracting-Lazy-Society.html.

6. *See* Smith et al., *supra* note 3, at 5 ("Smartphones are used for much more than calling, texting, or basic internet browsing. Users are turning to these mobile devices as they navigate a wide range of life events:

- 62% of smartphone owners have used their phone in the past year to *look up information about a health condition*.
- 57% have used their phone to do *online banking*.
- 44% have used their phone to look up *real estate listings* or other information about a place to live.
- 43% to look up *information about a job*.
- 40% to look up *government services or information*.
- 30% to *take a class or get educational content*.
- 18% to *submit a job application*.").

7. *See* Boyd v. United States, 116 U.S. 616, 630 (1886).

8. The Court sarcastically described the pervasive and insistent role cell phones have in society today by stating "the proverbial visitor from Mars might conclude [cell phones] were an important feature of human anatomy." Riley v. California, 134 S. Ct. 2473, 2484 (2014); *see also* Duggan, *supra* note 2 (showing that there is a high likelihood that most individuals lawfully arrested will be in possession of a cell phone).

ceptions to the warrant requirement may be relied upon or abused by officers in an attempt to gain access to the cell phone data without first acquiring a warrant. Furthermore, changes in technology in the upcoming years may cause lower courts substantial difficulties as they attempt to reconcile the Court's decision with new technological advancements.

Part I will provide background for the Article, first describing the history of the search incident to arrest doctrine and explaining the cases that led to the Supreme Court's review of this issue. Next, Part II will detail and examine the Court's decision and analysis in *Riley v. California*. Lastly, Part III will describe the positive results of the Court's decision, followed by a critique of the potential difficulties that the Court's decision may cause, as well as the impact of these unintended results in future cases.

I. THE HISTORY OF THE SEARCH INCIDENT TO ARREST EXCEPTION

This Part will explain the background for the debate in *Riley v. California*. First, this Part will give a brief description of the Fourth Amendment and its scope. Next, it will describe the search incident to arrest doctrine with an analysis of the cases that have defined this exception to the Fourth Amendment's warrant requirement. Lastly, it will provide an outline of the decisions of *Riley v. California* and *United States v. Wurie* to help to show the contrast between the lower courts' differing opinions, ultimately leading to the Supreme Court's involvement in resolving the issue.

A. The Fourth Amendment

A warrant is typically required in order for law enforcement officials to search a person or their property. The Fourth Amendment states:

> 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.[9]

The Fourth Amendment prescribes that a specific warrant, based

9. U.S. CONST. amend. IV.

upon probable cause, must be issued before a person's "houses, papers, and effects" can be searched or seized.

The Framers developed this Amendment in response to the intrusive search and seizure practices of the British prior to the American Revolution, specifically to counter the British's use of writs of assistance.[10] Writs of assistance gave custom officers the authority to search homes, shops, cellars, warehouses, and other places for illegally smuggled goods.[11] Defiant actions taken by the Framers and early Americans ultimately led to the adoption of the Fourth Amendment, implemented in order to protect colonists' privacy and property against the unlimited—and often unsubstantiated—discretion of government officials to which they had previously been subjected.[12]

The Fourth Amendment also requires that warrants particularly describe the things to be seized, thus making general searches under the Amendment impossible. It is the Supreme Court's role to interpret the Fourth Amendment and define its boundaries.[13] The Court explained that in relation to the Fourth Amendment warrant requirement, "nothing is left to the discretion of the officer executing the warrant."[14] Congress has been mindful of this in enacting the laws governing the issue and execution of search warrants, limiting seizures to things particularly described.[15] In sum, "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment[.]"[16]

10. M. Blain Michael, *Reading the Fourth Amendment: Guidance from the Mischief that Gave It Birth*, 85 N.Y.U. L. REV. 905, 907–08 (2010); *see also* United States v. Wurie, 728 F.3d 1, 3 (1st Cir. 2013).

11. Michael, *supra* note 10.

12. *Id.*; *see also* Johnson v. United States, 333 U.S. 10, 14 (1948) ("[The Fourth Amendment's] protection consists in requiring that . . . inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime."); McDonald v. United States, 335 U.S. 451, 455 (1948) ("Absent some grave emergency, the Fourth Amendment has interposed a magistrate between the citizen and the police. This was done not to shield criminals nor to make the home a safe haven for illegal activities. It was done so that an objective mind might weigh the need to invade that privacy in order to enforce the law.").

13. *See* CHARLES H. WHITEBREAD & CHRISTOPHER SLOBOGIN, CRIMINAL PROCEDURE: AN ANALYSIS OF CASES AND CONCEPTS 18 (5th ed. 2008).

14. Marron v. United States, 275 U.S. 192, 196 (1927).

15. *Id.*; FED. R. CRIM. P. 41(e)(2)(A) ("[T]he warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned.").

16. Arizona v. Gant, 556 U.S. 332, 338 (2009) (quoting Katz v. United States, 389 U.S. 347, 357 (1967) (footnote omitted)).

B. Search Incident to Arrest Exception

While warrantless searches are presumptively unlawful, "the ultimate touchstone of the Fourth Amendment is reasonableness."[17] Thus, "the warrant requirement is subject to certain exceptions."[18] Although the Fourth Amendment rule of obtaining a warrant before searching a person's property applies in most situations, the Court accepted "a few specifically established and well-delineated exceptions[]" as exemptions to this rule.[19] One such allowance is the search incident to arrest exception.

The search incident to arrest exception allows the police, during a lawful arrest, to search "the arrestee's person and the area within his immediate control[.]"[20] The traditional basis for the search incident to arrest exception is that it is presumed reasonable for an arresting officer to search for weapons, instruments of escape, and evidence of a crime during the course of the arrest in order to protect the officer's safety and prohibit the destruction of relevant evidence.[21]

This exception to the warrant requirement has long been recognized under American law,[22] with its first true application happening in 1927. In *Marron v. United States*,[23] officials charged the petitioner with conspiracy to commit various offenses against the National Prohibition Act.[24] Petitioner insisted that a ledger and certain bills were obtained illegally through a search and seizure that violated his Fourth and Fifth Amendment rights because the items seized were

17. Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (internal quotation omitted); *see also* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) ("Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant.").

18. *Brigham City*, 547 U.S. at 403.

19. *Gant*, 556 U.S. at 338.

20. *Id.* at 339 (quoting Chimel v. California, 395 U.S. 752, 763 (1969) (internal quotation omitted)).

21. *See, e.g.*, *Chimel*, 395 U.S. at 753; United States v. Edwards, 415 U.S. 800, 802–03 (1974).

22. *See* Weeks v. United States, 232 U.S. 383, 392 (1914) (stating that officers can "search the person of the accused when legally arrested, to discover and seize the fruits or evidences of crime."). The Court in *Riley* stated that this exception to the warrant requirement has been "well accepted" and that the label of "exception" is "something of a misnomer" due to warrantless searches incident to arrest occurring much more often than searches conducted pursuant to a warrant. *See Riley*, 134 S. Ct. at 2482 (citing 3 W. LaFave, Search and Seizure § 5.2(b) p.132, n.15 (5th ed. 2012)).

23. Marron v. United States, 275 U.S. 192, 192 (1927).

24. *Id.* at 193.

not with him on his person during the arrest.[25] Holding for the Government, the Supreme Court stated that the bills and ledgers were lawfully seized as an incident to arrest, providing the officers with "a right *without a warrant* contemporaneously to search the place in order to find and seize the things used to carry on the criminal enterprise."[26] The Court continued to establish the exception by narrowing and expanding the doctrine in a variety of cases,[27] ultimately preparing the way for *Chimel v. California*,[28] the case that established the search incident to arrest doctrine as we understand it today.[29]

In *Chimel*, the Supreme Court held that a warrantless search of a defendant's entire house was not justified based solely on the fact that it occurred as part of his valid arrest. Officers suspected Chimel of burglarizing a coin shop.[30] Despite the lack of consent, officers searched Chimel's entire house finding coins and other evidence that supported the burglary conviction.[31] The Court explained that a search incident to arrest would be reasonable in two scenarios, namely to maintain officer safety[32] and to preserve evidence of the crime.[33] The Court also explained that justification existed to search not only the arrestee's person, but also the area "within his immediate control," further defining that phrase as "the area from within which [the arrestee] might gain possession of a weapon or destructible evi-

25. *Id.* at 193–94.

26. *Id.* at 199 (emphasis added).

27. *Compare* Go-Bart Importing Co. v. United States, 282 U.S. 344, 358 (1931) (limiting the doctrine by disallowing officers to search through an arrestee's office), *and* Trupiano v. United States, 334 U.S. 699, 708 (1948) (narrowing the doctrine yet again by holding an incident search of a distillery following the manager's arrest violated his Fourth Amendment rights), *with* Harris v. United States 331 U.S. 145, 153 (1947) (expanding the scope of the doctrine to allow officers to search arrestee's entire house), *and* United States v. Rabinowitz, 339 U.S. 56, 65–66 (1950) (following the analysis in *Harris* to allow the incidental search of an arrestee's office in order to gather evidence).

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

29. Riley v. California, 134 S. Ct. 2473, 2483 (2014) ("*Chimel* . . . laid the groundwork for most of the existing search incident to arrest doctrine."); United States v. Wurie, 728 F.3d 1, 3–4 (1st Cir. 2013) *cert. granted*, 134 S. Ct. 999 (2014), *aff'd sub nom. Riley*, 134 S. Ct. at 2473 ("The modern search-incident-to-arrest doctrine emerged from *Chimel v. California*[.]").

30. *Chimel*, 395 U.S. at 753.

31. *Id.* at 753–54.

32. *Id.* at 763 ("[I]t is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated.").

33. *Id.* ([I]t is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.").

dence."[34] The officer's search in Chimel's home was not motivated by either officer safety or the preservation of evidence, and thus was held unconstitutional.[35]

Decisions since *Chimel* have further developed and refined our understanding of the search incident to arrest doctrine. In *United States v. Robinson*,[36] the Court addressed how the search incident to arrest exception applied to searches of a person.[37] Upon the arrest in *Robinson*, the arresting officer felt an object he could not identify in Robinson's coat pocket during a pat down.[38] He removed the object to discover it was a cigarette package containing what the officer believed to be something other than cigarettes.[39] The officer opened the package and found fourteen capsules of heroin concealed therein.[40] The Court held that the search was valid, stating that it is within a police officer's authority to conduct "a full search of [a] person" incident to a lawful arrest.[41] Because the officer found the package of cigarettes containing the heroin capsules during a pat down of Robinson following a lawful arrest for driving with a revoked license, the Court held the warrantless search was constitutional.[42] The Court further clarified:

> The 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. It is the fact of the lawful arrest which establishes the authority to search, and we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a "'reasonable'" search under that Amend-

34. *Id.* (internal citation omitted).
35. *Id.* at 768.
36. United States v. Robinson, 414 U.S. 218, 218 (1973).
37. *Id.* at 220.
38. *Id.* at 222–23.
39. *Id.* at 223.
40. *Id.*
41. *Id.* at 235.
42. *Id.* at 236.

ment.[43]

The following year, the Court decided *United States v. Edwards*.[44] Edwards was lawfully arrested and charged with attempting to break into the city's post office and taken to the local jail.[45] Upon discovering that entry to the post office had been made through a wooden window frame, the police seized Edwards' pants and shirt in the hopes of matching paint chip samples from the window frame with paint chips that were on his clothes.[46] The Court held such actions valid under the Fourth Amendment, affirming the Court of Appeal's reversal of the trial court's decision.[47] In its decision, the Court stated:

> The police were . . . entitled to take from Edwards any evidence of the crime in his immediate possession, including his clothing . . . . . . When it became apparent that the articles of clothing were evidence of the crime for which Edwards was being held, the police were entitled to take, examine, and preserve them for use as evidence, just as they are normally permitted to seize evidence of crime when it is lawfully encountered.[48]

The Court again addressed the search incident to arrest exception in *United States v. Chadwick*.[49] In *Chadwick*, officers made a lawful arrest of three individuals suspected of transporting a footlocker full of drugs.[50] The officers made the arrest once the arrestees loaded the footlocker into the trunk of a car, but before they closed the trunk lid or turned the vehicle on.[51] The arrestees and the footlocker were taken to the Federal Building, where officials searched the footlocker an hour and a half later and found marijuana inside.[52] The Court found this search impermissible as the officials conducted it more than an hour after the federal agents put the arrestees into custody and gained "exclusive control of the footlocker."[53] The Court supported

43. *Id.* at 235.

44. United States v. Edwards, 415 U.S. 800 (1974).

45. *Id.* at 801.

46. *Id.* at 801–02.

47. *Id.* at 802.

48. *Id.* at 804–05.

49. United States v. Chadwick, 433 U.S. 1, 1 (1977), *abrogated on other grounds by* California v. Acevedo, 500 U.S. 565, 565 (1991).

50. *Id.* at 3–4.

51. *Id.* at 4.

52. *Id.* at 4–5.

53. *Id.* at 15.

its decision by explaining that the agents were not in any danger since the arrestees could no longer access the property to seize a weapon or destroy relevant evidence.[54]

The Court continued to clarify the *Chimel* rationales in *New York v. Belton*.[55] In *Belton*, a police officer stopped a vehicle in which Belton was a passenger for exceeding the speed limit.[56] The officer approached the vehicle and noticed a strong smell of marijuana, as well as an envelope on the vehicle's floor, which the officer suspected contained marijuana.[57] The officer arrested the occupants of the car for unlawful possession of marijuana.[58] After searching each of the occupants, the officer searched the passenger compartment of the car, found a jacket belonging to Belton, unzipped one of the pockets, and discovered cocaine.[59] Belton was also indicted for possession of a controlled substance.[60] The Court held the search of Belton's jacket did not violate the Fourth Amendment as it was a search incident to a lawful arrest.[61] Because the jacket was located in the passenger compartment of the car, the Court held it was "within the arrestee's immediate control," as explained in *Chimel*.[62] The Court found the police could permissibly search the passenger compartment of the car as well as the contents of any containers[63] found in the passenger compartment.[64]

Only a few years ago, the Court again addressed the search incident to arrest exception in *Arizona v. Gant*.[65] Officers arrested Gant

54. *Id.* ("Once law enforcement officers have reduced luggage or other personal property not immediately associated with the person of the arrestee to their exclusive control, and there is no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident of the arrest.").

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

56. *Id.* at 455.

57. *Id.* at 455–56.

58. *Id.* at 456.

59. *Id.*

60. *Id.*

61. *Id.* at 462–63.

62. *Id.* at 462; *see* Chimel v. California, 395 U.S. 752, 763 (1969).

63. "Container" is defined as "any object capable of holding another object." *Belton,* 453 U.S. at 460 n.4.

64. *Id.* at 461 ("Such a container may, of course, be searched whether it is open or closed, since the justification for the search is not that the arrestee has no privacy interest in the container, but that the lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have.").

65. Arizona v. Gant, 556 U.S. 332, 332 (2009). The Court in *Gant* distinguished its decision in *Belton* by rejecting a broad interpretation of *Belton* and allowing the search of a vehicle once the arrestee has been secured. *Id.* at 343.

for driving on a suspended license, handcuffed him, and locked him in a patrol car before they searched his car and found cocaine in a jacket pocket.[66] Relying on the twin rationales listed in *Chimel*, the Court found that a search of an arrestee's vehicle incident to arrest is lawful in certain circumstances.[67] According to the Court, "Police may search a vehicle incident to a recent occupant's arrest only if the arrestee is within reaching distance of the passenger compartment at the time of the search or it is reasonable to believe the vehicle contains evidence of the offense of arrest."[68]

C. Disagreement Among Lower Courts

While the Supreme Court has addressed the search incident to arrest exception in numerous cases, lower courts have struggled and disagreed for years about how to best apply the Supreme Court's jurisprudence to the search of data on a cell phone seized during a lawful arrest. Circuit and state courts were divided on the issue until the Court's decision in *Riley*. Even among those that agreed, the rationales used to allow or prohibit a warrantless search of a cell phone differed from court to court.

1. Circuit splits

A large number of circuit courts and state courts approved or partially approved warrantless searches of an arrestee's cell phone data.[69] Those courts that fully approved a warrantless search relied on a variety of approaches in order to justify the search. For example, in *People v. Diaz*,[70] the Supreme Court of California relied on *Robinson* and *Edwards* to support the conclusion that an officer can freely search a cell phone when incident to a lawful arrest with no justification beyond the fact of the arrest itself.[71] Other courts have relied on other justifications to allow a warrantless search of a cell phone, including the need to preserve evidence.[72] When it comes to personal

66. *Id.* at 335.

67. *Id.* at 339–40.

68. *Id.* at 351.

69. *See* United States v. Wurie, 728 F.3d 1, 5 (1st Cir. 2013); *see also* H. Rick Yelton, *Riley v. California: Setting the Stage for the Future of Privacy by Distinguishing Between Digital and Physical Data*, 60 LOY. L. REV. 997, 1011–12 (2014).

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

71. *Id.* at 504–05.

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

items found on an individual during an arrest, courts have placed significant weight on law enforcement's need to protect against the destruction or tampering of evidence in justifying the warrantless search of personal items incident to arrest.[73]

Several courts have partially approved the warrantless search of an arrestee's phone, allowing the search of only specific data files incident to a lawful arrest. For example, the Seventh Circuit held that an officer's search of a phone to find the number of that particular phone was allowable as it was minimally invasive and justified by the rationale stated in *Chimel*.[74] Several state courts have also found sufficient justification in this same purpose to allow a limited search of a cell phone.[75] Despite the majority of courts supporting the warrantless search of a cell phone incident to a lawful arrest, a number of courts have held oppositely for a variety of reasons. For example, the Supreme Court of Ohio held that cell phones are distinguishable from closed containers in that the individual carrying the phone has a high expectation of privacy in the contents of his or her phone.[76] Similarly, in *United States v. Park*,[77] the court concluded that a cell phone is a possession within an arrestee's immediate control, to be governed by the *Chadwick* standard as opposed to the *Robinson* or *Edwards* standards.[78] Under these standards, such an item cannot be searched once it is in the exclusive control of the police, unless exi-

point that the need to preserve evidence justifies the warrantless search of a phone); United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007) ("[Police officers] may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial.").

73. United States v. Robinson, 414 U.S. 218, 225 (1973); *see also* United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996) (holding preservation of evidence supported search of electronic pager).

74. United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012). Note also that the Seventh Circuit suggested other justifications could be imagined for a more extensive search. *Id.* at 810.

75. Hawkins v. State, 723 S.E.2d 924, 925–26 (Ga. 2012) (affirming the lower court's decision that a cell phone, for purposes of a search incident to arrest, could be treated in the same manner as a traditional physical container); Commonwealth v. Phifer, 979 N.E.2d 210, 215–16 (Mass. 2012) (allowing the search of the phone's call log because the officers here had probable cause to believe the telephone's recent call list would contain evidence relating to the crime for which he was arrested).

76. State v. Smith, 920 N.E.2d 949, 954–56 (Ohio 2009).

77. United States v. Park, No. CR 05-375SI, 2007 WL 1521573, at *12 (N.D. Cal. May 23, 2007).

78. *Id.* at *1 ("[A] modern cellular phone, which is capable of storing immense amounts of highly personal information, is properly considered a 'possession within an arrestee's immediate control' rather than as an element of the person.").

gent circumstances exist. Most recently, the Supreme Court of Florida held that, under *Gant*, police officers are prohibited from searching an arrestee's cell phone removed from his person.[79] According to that court, such removal creates a situation where the phone can no longer be used as a weapon against the arresting officer, and the arrestee cannot destroy any evidence contained on the phone.[80]

The differences in application and understanding of the search incident to arrest doctrine again appeared when the California Court of Appeals addressed the issue in *Riley v. California*, and when the First Circuit took on the case of *United States v. Wurie*.

2. Riley v. California

Riley was involved in a shooting where he and several other gang members shot at a rival gang member as they drove by in his vehicle.[81] Officers later stopped Riley for driving with expired registration tags, and once the officers established his connection to the shooting, they arrested him and seized his phone.[82] Later, information the officials obtained from the phone linked Riley to the shooting and resulted in his conviction on counts of firing at an occupied vehicle, assault with a semi-automatic firearm, and attempted murder.[83]

The California Court of Appeals affirmed the trial court's rejection of Riley's argument that the warrantless search violated his Fourth Amendment rights.[84] The court relied on *Diaz*, a California Supreme Court case permitting a warrantless search of cell phone data incident to arrest, so long as the cell phone was immediately asso-

79. Smallwood v. State, 113 So. 3d 724, 734–35 (Fla. 2013).

80. *Id.* at 735 ("*Gant* demonstrates that while the search-incident-to-arrest warrant exception is still clearly valid, once an arrestee is physically separated from an item or thing, and thereby separated from any possible weapon or destructible evidence, the dual rationales for this search exception no longer apply.").

81. People v. Riley, No. D059840, 2013 WL 475242, at *1 (Cal. Ct. App. Feb. 8, 2013), cert. granted in part sub nom. Riley v. California, 134 S. Ct. 999 (2014) and rev'd and remanded sub nom. Riley v. California, 134 S. Ct. 2473, 2473 (2014).

82. *Riley*, No. D059840, 2013 WL 475242, at *1–2.

83. *Id.* at *3. The information found on Riley's phone connected him to gang activity. For example, officers noticed that some words in the phone were preceded by the letters "CK"—a label that the officers believed stood for "Crip Killers," a slang term for members of the Bloods gang. Detectives also found on the phone videos of young men sparring while someone yelled "Blood" as encouragement to keep fighting. Police also found photographs of Riley standing in front of a car they suspected had been involved in the shooting a few weeks earlier. *See Riley*, 134 S. Ct. at 2480–81.

84. *Riley*, No. D059840, 2013 WL 475242, at *6.

ciated with the arrestee's person.[85] The court found Riley's cell phone was immediately associated with his person when he was arrested, and therefore the search of the cell phone was lawful despite the lack of an exigency existing.[86] The California Supreme Court denied Riley's petition for review.[87]

3. United States v. Wurie

After observing Wurie perform a drug transaction with a man in the parking lot of a convenience store, an officer arrested him.[88] Upon his arrest, the officer took Wurie's phone and other personal belongings from him.[89] While at the station, officers noticed via the phone's external caller ID screen that one of Wurie's cell phones repeatedly received phone calls from a contact listed as "my house."[90] The officers opened the phone, noticing a picture on the background of a young woman holding a baby set as the wallpaper.[91] The officers navigated to the call log where they were able to locate the number associated with the caller ID.[92] Using this number, the officers pulled up the address associated with the phone number using an online white pages directory.[93] This information led to the officers obtaining a search warrant for Wurie's home; upon execution of the warrant, the officers found drugs, drug paraphernalia, and a firearm.[94] The officers then charged Wurie with possession with intent to distribute and distributing cocaine, as well as being a felon in possession of a firearm. The district court found Wurie guilty on all three counts after it denied Wurie's motion to suppress the evidence obtained through the search of his phone.[95]

The First Circuit reversed the district court's decision. In its analysis, the First Circuit first expressed its support of a bright-line

85. *Id.*; *see* People v. Diaz, 244 P.3d 501, 505 (Cal. 2011).

86. *Riley*, No. D059840, 2013 WL 475242, at *6.

87. *Riley*, 134 S. Ct. at 2481.

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

89. *Id.* at 2.

90. *Id.* The officers were able to see the caller ID, and the "my house" label, in plain view.

91. *Id.*

92. *Id.* Note that in locating the number, the officers only pressed two buttons on Wurie's phone.

93. *Id.*

94. *Id.*

95. *Id.*

rule as opposed to a subjective, fact-specific rule.[96] In denying the Government's arguments to apply the reasoning of *Edwards* and *Robinson*,[97] the First Circuit explained that the Government would only prevail by demonstrating that the warrantless search of Wurie's cell phone was valid based on the *Chimel* standards.[98] The court was "unconvinced" by the Government's argument that either of the *Chimel* rationales applied, holding that "warrantless cell phone data searches are categorically unlawful under the search-incident-to-arrest exception[.]"[99] It further reasoned that the data stored on phones is "highly personal" and such an intrusion into a person's privacy should not be violated flippantly.[100] The First Circuit's decision in *Wurie* created an official split in authorities, paving the way for the Supreme Court's involvement in resolving the discrepancy between the circuits and among the lower courts.

II. RILEY V. CALIFORNIA

The Supreme Court granted certiorari in both *Riley v. California* and *United States v. Wurie*, combining them into a single decision. The issue before the Court, present in both *Riley* and *Wurie*, was whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been lawfully arrested.[101] The justices unanimously agreed in a 9-0 decision that a warrant is generally required, absent exigent circumstances, to search an arrestee's cell phone data.[102] The Court reached the final decision after weighing the legitimate governmental interests on one hand and an individual's privacy on the other.

This Part will first describe the Court's analysis of the first consideration, namely the Government's interest in searching a cell

96. *Id.* at 6; *see also* Thornton v. United States, 541 U.S. 615, 623 (2004).

97. The First Circuit stated, "[T]here are categories of searches undertaken following an arrest that are inherently unreasonable because they are never justified by one of the *Chimel* rationales." *Wurie*, 728 F.3d at 7.

98. *Id.*

99. *Id.* at 12.

100. *Id.* at 8. The First Circuit found efficient police work an unpersuasive argument. *See id.* at 13 ("[W]arrantless cell phone data searches strike us as a convenient way for the police to obtain information related to a defendant's crime of arrest . . . without having to secure a warrant."); *see also* Mincey v. Arizona, 437 U.S. 385, 393 (1978) ("The mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment.").

101. Riley v. California, 134 S. Ct. 2473, 2480 (2014).

102. *Id.* at 2485.

phone without a warrant. Second, this Part will analyze the second consideration, which is a person's privacy as it relates to the content on a cell phone. Third, it will provide a description of the Court's analysis of the Government's arguments and the decision's foreseeable impacts, including a mention of the opinion's concurrence by Justice Alito.

A. Governmental Interests

The Court's analysis opened with a brief overview of the two cases to be decided,[103] followed by a description of the cases that have helped define what is permissible within the search incident to arrest exception.[104]

The Court's analysis centered on its weighing of an individual's privacy against the promotion of legitimate governmental interests.[105] Such a balancing test is generally the method used by the Court to determine whether a given type of search is exempt from the warrant requirement. The Court has traditionally weighed the degree to which a search intrudes on a person's privacy against the degree to which the search is needed to promote legitimate governmental interests.[106]

The governmental interests recognized by the Court in allowing the warrantless search of a cell phone were focused on the two risks identified in *Chimel*: the potential danger to an officer's safety and the possible destruction of evidence.[107] While the Court has extended these governmental interests to the context of physical objects in the past,[108] it deviated from this course in *Riley*, holding that digital data on a phone "bears little resemblance to the type of brief physical search considered in *Robinson*."[109] Although *Robinson* made searches incident to arrest reasonable regardless of "the probability in a particular arrest situation that weapons or evidence would in fact be found,"[110] the Court ultimately decided that a warrantless search of

103. *Id.* at 2480. For the facts and summaries of these cases, see *supra* Sections I.C.2 & 3.

104. The Court focused on its decisions in *Chimel*, *Robinson*, and *Gant*. For a description of each of these cases, as well as other cases relating to the search incident to arrest doctrine, see *supra* Section I.B.

105. *Riley*, 134 S. Ct. at 2484.

106. *See, e.g.*, Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

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

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

109. *Riley*, 134 S. Ct. at 2485.

110. *Robinson*, 414 U.S. at 235.

cell phones was disconnected to the justification underlying the *Chimel* exception.[111]

1. Officer safety

The Court determined that the concern of officer safety was not sufficiently present to justify the search of a cell phone without a warrant.[112] While the actual physical cell phone could potentially be used as a weapon, the digital data stored on a cell phone posses no legitimate threat to officer safety, nor can it assist an arrestee's escape. The Court determined that the physical aspects of a phone could be searched to determine whether it could be used as a weapon.[113] However, because the data on a phone could not threaten the officer once the phone was seized, it could not be searched.

The Court determined that the search of a cell phone did not rise to the level of uncertainty that "unknown physical objects . . . always pose," such as the cigarette pack in *Robinson*.[114] The difference recognized by the Court between physical objects and digital data on cell phones is that officers do not know what they will find in physical objects—such as in *Robinson* where the arresting officer did not know what the hard objects in the cigarette pack were or whether it posed a risk to his safety—but they do know what they will find when they search a cell phone, namely data, which does not pose a threat to officers' safety. The Court rejected the United States and California arguments that a search may ensure officer safety in an indirect way, such as alerting officers that the arrestee's comrades may be traveling to the site of arrest to assist in the arrestee's escape. While the Court recognized that this and other circumstances are possible, they do "not justify dispensing with the warrant requirement across the board."[115]

111. *Riley*, 134 S. Ct. at 2485; *see also* Knowles v. Iowa, 525 U.S. 113, 119 (1998) (declining to extend *Robinson* to the issuance of citations due to the *Chimel* justifications not being present in that situation; officer safety was only a minor threat, and destruction of evidence was not present at all).

112. *Riley*, 134 S. Ct. at 2485–86.

113. For example, the Court suggested that an officer could examine the physical aspects of a phone to ensure that a razor blade was not hidden between the phone and its case. *Id.* at 2485.

114. *Id.*

115. *Id.* at 2486.

2. Preservation of evidence

The Court focused a considerable amount of its opinion on the second *Chimel* rationale—"preventing the destruction of evidence"—before deciding that the governmental interests were too low to justify a warrantless search exception to cell phones.[116] The risk of destruction of evidence by the arrestee is almost completely eliminated once he or she is placed under arrest. By doing such, the officer removes any risk or possibility of the arrestee deleting incriminating data that may be on the phone.

The United States and California suggested two situations where digital evidence on a phone could nonetheless be subject to potential destruction: remote wiping and data encryption. The Court first rejected these arguments by pointing out that the *Chimel* justification focuses on the arrestee's ability to conceal or destroy evidence, not the ability of third parties to do so. As mentioned before, once an arrestee has been placed under arrest, his or her own ability to destroy or conceal evidence contained on his or her cell phone is eliminated. Furthermore, the Court stated that it had "little reason to believe that either problem is prevalent."[117] According to the Court, officers can easily protect against remote wiping by either turning the phone off, or placing the phone into an enclosure that isolates the phone from radio waves. As in the case of officer safety, if an officer feels that circumstances suggest that the arrestee's phone will be remotely wiped or irreversibly encrypted, the officer can always rely on the exigent circumstance exception "to search the phone immediately."[118]

According to the Court, the *Chimel* concerns are not salient in warrantless cell phone search cases. Thus, the Court determined that the government's interest in not obtaining a warrant before searching an arrestee's phone incident to arrest was very low.

B. Individual's Privacy

The second part of the weighing test that the Court conducted was considering the privacy interest of those being taken into police custody. The Court first explained the diminished privacy interests

116. *Id.* at 2486–88.

117. *Id.* at 2486.

118. *Id.* at 2487. Officers that find a phone in an "unlocked" state may also reasonably disable the phone's automatic locking feature in order to preserve evidence while a warrant is obtained. *Id.* at 2488.

that an arrestee has. While a search of a person is justified, in part by a reduced expectation of privacy caused by the arrest, "[n]ot every search is acceptable solely because a person is in custody."[119] When privacy interests are significant enough, a search will require a warrant, despite the diminished expectation of privacy of the arrestee.[120] Through this understanding, the Court ultimately determined that the privacy concerns involved with modern cell phones are categorically different from any other search approved by the lower courts under the *Robinson* and *Chimel* standards.[121] Therefore, the Court analyzed the privacy implications involved in searching an arrestee's cell phone on its own grounds.

1. Quantitative and qualitative differences

The Court first analyzed the quantitative and qualitative differences between cell phones and other physical objects.[122] Cell phone capacity has drastically evolved and changed over recent years; the term "'cell phone'" is arguably inappropriate since phones now have many of the same capabilities that a computer has.[123] Perhaps the most significant evolution in cell phone technology is the amount of storage capacity available on phones. For a person to carry a physical copy of every piece of information that is available to them on their cell phone would be impracticable—if not impossible—to say the least.

The Court recognized several "interrelated consequences" of cell phone searches due to their huge storage capacity. First, cell phones have many different types of information all conveniently located in one place.[124] This information, as a combined whole, reveals much more about the phone's owner than each single piece of information

119. *Id.* at 2488 (quoting Maryland v. King, 133 S. Ct. 1958, 1979 (2013)); *see also* United States v. Chadwick, 433 U.S. 1, 16 n.10 (1977).

120. *Riley*, 134 S. Ct., at 2488. A good example of this principle can be seen in the facts of *Chimel*: in that case, the search of the defendant's entire house was not justified due to the intrusive nature of the search, despite the arrestee's expectation of privacy being diminished due to the arrest. 395 U.S. at 768.

121. *Riley*, 134 S. Ct., at 2488–89 (2014).

122. *Id.* at 2489–91.

123. The Court recognizes that cell phones have the ability to function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Id.* at 2489. Some of the more personal features on a phone would include photos, videos, financial statements, medical information, personal messages such as text messages, emails, and social media messages, browsing history, and contacts. *See id.*

124. *Id.* at 2489.

independently. Second, due to the amount of data that can, and normally is, stored on a phone, a single type of information can be more intrusive than a physical counterpart would.[125] Third, the data on a phone can be stored much longer than physical information.[126] Lastly, because nearly every person the police encounter will be carrying a cell phone on which personal and sensitive information is likely stored,[127] the likelihood of invading an individual's privacy is much higher than in the past when such information was not regularly carried by an individual at all times of the day.

Additionally, the Court recognized how the information on a cell phone is qualitatively distinguishable from physical records.[128] The information that can be acquired by searching an individual's phone can give a unique perspective into that person's private thoughts, interests, or concerns. Location services can also pinpoint where that person has been recently. Likewise, many phones now have the ability to run application software ("apps"), which gives even more insight into the owner's life based on the apps that they have downloaded and the information that they have accessed or stored on those apps.

2. Cloud computing

The Court also considered the ability of modern cell phones to store information in the cloud.[129] Such an ability adds another complicated level to the search principles since information found on a cell phone often times is not actually "stored" on the actual device itself. This ability overcomes any *Belton* argument that a cell phone should be treated as a container whose contents may be searched incident to an arrest.[130] Because accessing information through cloud computing capacity is indistinguishable from accessing information stored on the actual phone itself, it is difficult to know whether the particular information being accessed is stored on the device or in the

125. *See id.* The example used by the Court is how the life of a cell phone owner could be essentially "reconstructed" based on the thousand of pictures on his or her phone, many of which would also have date and time stamps, location markings, and descriptions. This would not be possible to do with the few pictures that are found in an arrestee's wallet.

126. *Id.* For example, call records are often stored on a phone for set amount of times (typically several months) or until newer calls erase past calls at the bottom of the list.

127. *See supra* notes 2 and 6; *see also Riley*, 134 S. Ct. at 2490–91.

128. *Riley*, 134 S. Ct. at 2490–91.

129. *Id.* at 2491.

130. *See supra* notes 55–64; *see also Riley*, 134 S. Ct. at 2491.

cloud.

The cloud computing aspect of cell phones added additional weight to the privacy concern involved in searching an individual's phone without a warrant. The Court concluded that based on its analysis of the lack of government's interests versus the high likelihood of intrusive privacy invasion, an individual's privacy interests dwarf any legitimate concern expressed by the government.

C. Government's Arguments and Foreseeable Impacts of the Riley Decision

The United States and California introduced various reasons for permitting warrantless cell phone searches.[131] The Court disagreed with each of these proposals and found the reasoning to be either flawed or contrary to the Court's general preference to provide clear guidance to law enforcement through categorical rules.

The United States proposed "that the *Gant* standard be imported from the vehicle context . . . ."[132] However, as the Court noted, the *Gant* standard is unique to the vehicle context to allow a search for the sole "purpose of gathering evidence." The *Gant* standard would not be appropriate to apply to cell phones because the standard was based on the "unique circumstances" in the vehicle context of a "reduced expectation of privacy" and "heightened law enforcement needs."[133] As was explained by the Court earlier in its decision, there is not a reduced expectation of privacy or a heightened need by law enforcement that would justify a warrantless search of a cell phone.

The Court also rejected the Government's argument that officers should be allowed to search certain areas of the phone based on their reasonable belief that relevant information is contained therein. The Court found that such an approach would "impose few meaningful constraints on officers" since it is not always possible to discern where information will be stored on a phone.[134] Similarly, officers are not able to search a phone's call log, as was at issue specifically in the *Wurie* case. However, searching a phone's call log will involve searching more than just numbers such as contact information, pho-

131. *Riley*, 134 S. Ct. at 2491.

132. *Id.* at 2492.

133. *Id.* (citing Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring)); Arizona v. Gant, 556 U.S. 332, 343 (2009)*; see also* Wyoming v. Houghton, 526 U.S. 295, 303–04 (1999).

134. *Riley*, 134 S. Ct. at 2492.

tos, and other labels.[135]

Finally, the Court rejected the argument that officers should be able to search cell phone data if the same information could be obtained from another medium.[136] The Court reasoned that even if it may be reasonable to search a wallet, which may contain a few family photos, it is unreasonable to then justify the search of thousands of pictures on an arrestee's cell phone. If such a standard were applied, then officers would be able to search through information on one's phone not normally carried with an individual in physical form on a daily basis, such as bank statements, video tapes, or photo albums.[137]

The Court recognized that its decision would come at a potentially high cost and would possibly adversely impact the ability of law enforcement to combat crime.[138] However, it also noted that "the warrant requirement is an important working part of our machinery of government, not merely an inconvenience to be somehow 'weighed' against the claims of police efficiency."[139] The Court submitted that this adverse impact could be mitigated by other case-specific exceptions that may apply in justifying a warrantless search of a phone, such as the exigent circumstances exception.[140] The decision concluded with a reaffirmation of the importance and scope of the Fourth Amendment. The Supreme Court reversed the judgment of the California Court of Appeal, and affirmed the judgment of the First Circuit, providing a simple summary of the decision in its final statement: "Our answer to the question of what police must do before searching a cell phone seized incident to a arrest is accordingly simple—get a warrant."[141]

135. *Id.* at 2492–93. Such was the case in *Wurie* where the arrestee had labeled the phone number as "my house." 728 F.3d 1, 2 (1st Cir. 2013).

136. *Riley*, 134 S. Ct. at 2493.

137. *Id.* ("[I]t is implausible that [Riley] would have strolled around with video tapes, photo albums, and an address book all crammed into his pockets.").

138. *Id.*

139. *Id.* (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

140. *See infra* note 190.

141. *Riley*, 134 S. Ct. at 2495. Justice Alito concurred in part and concurred in the final judgment. He wrote to address two points separately. First, the reasoning for the search incident to arrest doctrine used by the Court is flawed; the reasoning of *Chimel* related to the lawfulness of a search of the scene of an arrest, not the person of an arrestee. Furthermore, the basis for the rule has long been the need to obtain probative evidence, not officer safety and evidence preservation. Notwithstanding this point, Justice Alito agrees that it is the only workable alternative to have a categorical ban on warrantless searches of cell phones. Justice Alito's second point in the concurrence questions whether this issue should be governed by statute rather than decisions by the judicial system. Justice Alito wrote, "[I]t would be very unfortunate

III. IMPACT OF *RILEY V. CALIFORNIA*

The guidance of the *Riley* decision appears to be clear: warrantless searches of cell phones are unlawful, unless a valid exception applies. The impact of this decision will be influential and far-reaching. The effect of the *Riley* decision will be a positive step in protecting an individual's privacy against unlawful intrusion by police officers. However, the Supreme Court failed to consider several implications of their decision, which lower courts will have to grapple with in the future. The first portion of this Part will detail the positive results of the *Riley* decision. The following portion will detail some of the potential shortcomings of the *Riley* decision, as well as the possible issues that lower courts will likely need to address due to the Supreme Court's lack of guidance on those subjects.

A. Positive Results

The Supreme Court's decision finally provides clarity to lower courts and the legal community about the appropriate standard for warrantless searches of cell phones. Though this Article draws attention to some of the complications the *Riley* decision will invoke, the positive impacts of the Court's decision should not be overlooked. The successes, as described below, include the Court providing a clear, categorical rule as opposed to a case-by-case determination, the Court providing guidance as to how cellular devices differ from other physical objects, and the Court protecting privacy rights of individuals from having their cell phones searched indecently. These successes will positively affect the legal system and privacy rights of arrestees moving forward.

1. Clear categorical rule

The decision in *Riley* is as clear as one would expect from the nation's highest court. With its unanimous decision, the Supreme Court sent a clear message that officers are not allowed to search an individual's phone upon arrest without a warrant. Such unanimity among the justices makes following the Court's guidance easier for

if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future." *Id.* at 2495–98; *see infra* note 172.

lower courts when faced with similar cases. The Supreme Court prefers to provide clear guidance to law enforcement through categorical rules.[142] "[I]f police are to have workable rules, the balancing of the competing interests . . . 'must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.'"[143] Such categorical rules provide clarity in an often-confusing and ever-changing area of the law.

The clear rule makes training officers much easier.[144] Officers now know and can teach other officers that, absent circumstances that cause the officer to fear for his or her safety or reasonably suspect that the evidence on the phone is under immediate risk of being destroyed, officers are not allowed to search the phone of an arrestee. This bright-line rule will reduce the number of cases where officers are searching an arrestee's phone, eliminating the need to look at each situation on a case-by-case basis and ultimately reducing the amount of litigation related to this particular issue.

The decision will have the positive impact of reducing the amount of cases that courts have to review. In a court system that is already bogged down and backlogged with too many cases,[145] a reduction in caseloads is an absolute success. Any case that does involve an officer searching an arrestee's cell phone without a warrant will

142. While I agree that in this case a clear categorical rule is the best option, note that the Court recently also held that a judgment-based test was the best option to be applied to a similar Fourth Amendment issue. *See* Missouri v. McNeely, 133 S. Ct. 1552, 1564 (2013). In *McNeely*, the Supreme Court concluded that in some drunk-driving investigations where an officer wants to do a blood test on the driver of a stopped vehicle, certain circumstances may give rise to the drawing of blood without the driver's consent and without a warrant. 133 S. Ct. at 1557–63. The Court rejected a bright line rule, instead looking at a "totality of the circumstances" to determine whether warrantless blood tests performed on drunk drivers were appropriate. *Id.* at 1564. Such a rule goes against the Court's "general preference" of categorical rules. *Riley*, 134 S. Ct. at 2491. This goes to show that certain issues may be best resolved by a clear categorical rule—such as in warrantless searches of cell phones—but such a rule is by no means necessary or required. *See* United States v. Wurie, 728 F.3d 1, 17 (1st Cir. 2013) (Howard, J., dissenting).

143. Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981) (quoting Dunaway v. New York, 442 U.S. 200, 219–20 (1979) (White, J., concurring)); *see also* Harold Laidlaw, *Shouting Down the Well: Human Observation As A Necessary Condition of Privacy Breach, and Why Warrants Should Attach to Data Access, Not Data Gathering*, 70 N.Y.U. ANN. SURV. AM. L. 323, 343–44 (2015) (arguing that because "privacy" is an undefined term by the Court, a categorical rule is better equipped to protect against the infringement of people's privacy rights than on a case-by-case basis).

144. Not to mention the life of a law student studying for a criminal procedure final.

145. *See Wheels of Justice Slow at Overloaded Federal Courts*, S. CAL. PUB. RADIO (Sept. 27, 2015), http://www.scpr.org/news/2015/09/27/54669/wheels-of-justice-slow-at-overloaded-federal-court/.

likely not make its way through the court system thanks to the clear guidance provided by the Court in its decision; both sides will be able to analyze the strength of their position based on *Riley* and reach a settlement rather than have to take the matter before a judge.

Furthermore, the Court was not blind to the possibility of circumstances arising that might require an officer to search the arrestee's phone without a warrant. Despite a clear ban on such a search, the Court's decision still allows officers to use discretion in maintaining their safety, ensuring that the arrestee does not escape, and preserving evidence against tampering or destruction if it appears that the only way to protect against each of these risks is to search the phone without first obtaining a warrant. Officers still retain some flexibility and discretion in how to best serve and protect the public.

2. Physical objects vs. digital data

The Court recognized that there were quantitative and qualitative differences between digital data and physical items.[146] With constant changes and advancements in technology, it was appropriate for the Court to acknowledge these differences. The Court identified the key difference between cell phones and other physical items, which is the cell phone's ability to store significant amounts of personal data.[147] Comparing a cell phone to any other type of container would have been disproportionate and inappropriate. Modern cell phones are essentially computers[148] and contain many of the same features and functions that can be found on desktop computers or laptops.

146. *See supra* Section II.B.1.

147. Modern cell phones can come with up to 256 gigabytes of storage. *See Compare iPhone Models*, APPLE, http://www.apple.com/iphone/compare/ (last visited Apr. 8, 2017). This is the same—and even more—storage capacity as some laptop computers, *see Tech Specs: MacBook Air*, APPLE, http://www.apple.com/macbook-air/specs.html (last visited Apr. 8, 2017), and even half this amount of storage space is enough to hold 5,699 software applications, 18,639 songs, and 56,988 photos. John Brownlee, *This is How Many Apps, Songs, Videos, Photos and Games You Can Fit on a 128GB iPad*, CULT OF MAC (Jan. 29, 2013, 9:53 AM), http://www.cultofmac.com/213073/this-is-how-many-apps-songs-videos-photos-games-you-can-fit-on-a-128gb-ipad/.

148. *See* United States v. Flores-Lopez, 670 F.3d 803, 805 (7th Cir. 2012) (quoting United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011)) ("Analogizing computers to other physical objects when applying Fourth Amendment law is not an exact fit because computers hold so much personal and sensitive information touching on many private aspects of life . . . There is a far greater potential for the 'inter-mingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer."); *see also* United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001); United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999).

Smart phones have the capability of storing photographs, videos, written and audio messages (i.e. text messages, emails, and voicemail), personal contacts, calendar appointments, web search and browsing history, purchases, financial and medical records, and many other types of personal data. Such functions take a cell phone out of the traditional "container" arena, and move it into a category more comparable to a computer or home. The potential invasion of privacy in a search of a cell phone is greater than in a search of a "container" in the conventional sense.

The Court wisely recognized this important distinction. Had the Court ruled narrowly on just cell phones, the holding might not have extended so easily to future technology-related privacy issues.[149] Because the Court had the foresight to look not only at the current state of technology, but also the high likelihood of technology continuing to become more pervasive, its decision will continue to be applicable for many years. The reach of the decision is foreseeably applicable to future cases involving other 'computer-like devices,' such as laptop computers, tablets, smart watches, and other devices that store large amounts of personal data.

A similar success was the Court's categorical rule for all cell phones, regardless of their make, model, or storage and processing capabilities. The two phones seized and searched in *Wurie* and *Riley* were very different.[150] The Court decided that rather than making a distinction and drawing a line between phones that could and could not be searched, it would instead create a clear ban on the warrantless search of any cellular phone. Drawing a distinction between different types of phones would have been unwise considering that "[e]ven the dumbest of modern cell phones gives the user access to large stores of information," and private data could still be stored on the crudest of cell phones.[151] Additionally, a rule forcing officers to differentiate between phones based on their storage and processing capabilities would have been unworkable and unreasonable.[152] It would also require officers to learn and memorize the capabilities of constantly

149. *See Yelton*, *supra* note 69, at 1029–30.

150. Riley's phone was a "smartphone" with a broad range of functions, large storage capacity, and internet connectivity features, while Wurie's phone was a traditional "flip-phone" capable of a smaller range of features compared to a smartphone. Riley v. California, 134 S. Ct. 2473, 2480–81 (2014).

151. *Flores-Lopez*, 670 F.3d at 806.

152. *See* Thornton v. United States, 541 U.S. 615, 623 (2004).

changing electronic devices.[153]

Furthermore, as part of its analysis, the Court mentioned the possibility of officers accessing information not actually stored on the device itself, but rather in the cloud. It is becoming increasingly common that mobile devices store personal user data in the cloud as opposed to on the actual device itself.[154] This ability to store information in the cloud takes the arguments from *Belton*—that a cell phone is a container—and throws them out the window. A cell phone could no longer be characterized as a "container" when the information that is being accessed on it is not actually held on the phone, but rather in the cloud through the assistance of an off-site storage facility.[155] The general trend is for individuals to store more information in the cloud than on the actual device.[156] As the First Circuit stated in *Wurie* regarding data stored in the cloud, "[W]e believe that it may soon be impossible for an officer to avoid accessing such information during the search of a cell phone or other electronic device."[157] A positive result of the Court addressing this issue in its decision is to set a precedent for future cases related to data stored in the cloud.

3. Protection of privacy rights

The Court's decision is a huge success for the protection of U.S. citizen's privacy rights. The Fourth Amendment serves as a protection to an individual's subjective expectation of privacy if that expectation is both reasonable and justifiable.[158] Due to cell phones' ability to hold large amounts of private information, the Court correctly determined that they should be held to a higher standard of privacy as compared to other physical items. Individuals today store more personal information on their cell phones than could ever fit in a wallet, pocket, purse, briefcase, backpack, or any other traditional container that an individual may usually carry on their person, and that previ-

153. Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012).

154. *See* James E. Cabral et al., *Using Technology to Enhance Access to Justice*, 26 HARV. J.L. & TECH. 241, 268 (2012).

155. *See* New York v. Belton, 453 U.S. 454, 460 (1981).

156. *See* Drew Henry, *5 Storage Trends to Transform Mobile*, EE TIMES (July 20, 2015, 1:32 PM), http://www.eetimes.com/author.asp?section_id=36&doc_id=1327172; Christina Bonnington, *In Less Than Two Years, a Smartphone Could be Your Only Computer*, WIRED (Feb. 8, 2015, 3:42 AM), http://www.wired.com/2015/02/smartphone-only-computer/.

157. United States v. Wurie, 728 F.3d 1, 8 n.8 (1st Cir. 2013).

158. *See* Katz v. United States, 389 U.S. 347, 361 (1967).

ous courts had allowed officers to search incident to arrest.[159] Even if we consider containers that individuals would not normally carry with them on a day-to-day basis—storage lockers, suitcases, filing cabinets, etc.—such containers still do not have the same storage capacities or capabilities that a modern smartphone has. This implicates an individual's privacy rights on an entirely different level.

The type of sensitive information that individuals store on their phones now would be akin to the personal information and possessions stored in the home. After the *Riley* decision, the information on a cell phone could be considered the most private and protection-worthy data possible.[160] Regardless of the hierarchy, the Court's comparison adds strength to the type of protection that cell phones are to be allotted. The Fourth Amendment protects an individual's privacy in his or her home more than any other situation; as the Supreme Court put it, "When it comes to the Fourth Amendment, the home is first among equals."[161] The Court strongly protects an individual's privacy rights in his or her home, and now this same protection has been extended to an individual's cell phone as well.[162] And rightly so; as the Court noted, an individual arguably carries around in his or her pocket now more sensitive information than could be acquired by looking through all of his or her personal effects in his or her home.[163]

Furthermore, the *Riley* decision is a success because the rule pro-

159. *Cf.* United States v. Molinaro, 877 F.2d 1341, 1344 (7th Cir. 1989) (searching wallet and papers); United States v. Gonzalez-Perez, 426 F.2d 1283, 1285–87 (5th Cir. 1970) (searching papers contained in pockets, wallets, and purses); United States v. Frankenberry 387 F.2d 337, 339 (2d Cir. 1967) (searching diary); Grillo v. United States, 336 F.2d 211, 213 (1st Cir. 1964) (searching papers in wallet); *see also* Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012) (searching defendant's digital camera and all of its pictures without a warrant).

160. Riley v. California, 134 S. Ct. 2473, 2490–91 (2014) ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.").

161. Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013).

162. *See* Silverman v. United States, 365 U.S. 505, 511–12 (1961). The Court stated that at the "very core" of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." *Id.* at 511.

163. *Riley*, 134 S. Ct. 2490–91. The First Circuit also recognized a situation where a cell phone could also provide direct access into an individual's home. United States v. Wurie 728 F.3d 1, 8–9 (1st Cir. 2013). Through the use of an app, phones can connect their owners directly to a home computer's webcam so that users can monitor the inside of their homes remotely. While such a possibility is tenuous at best, it is nonetheless a possibility, and one that should be guarded against.

tects arrestees involved in low-level crimes from having their privacy disproportionately infringed upon. While officers are trained on appropriate searches and seizures,[164] it is not difficult to conjure up a situation where an arrest for a minor crime leads to an officer indecently violating an individual's privacy. For example, in *Newhard v. Borders*,[165] the officer arrested the defendant for driving while intoxicated.[166] In the course of a routine search incident to arrest, the arresting officer retrieved the defendant's cell phone from his pocket, conducted a warrantless search of the phone's contents, and viewed multiple photos of the defendant and his girlfriend nude and in "sexually compromising positions."[167] These images found by the arresting officer were wholly unrelated to the defendant's drunk driving arrest.[168] As if such an intrusion was not already invasive enough, the seizing officer showed these images to several other officers and stationhouse employees, and also alerted members of the public "that the private pictures were available for their viewing and enjoyment."[169] Due to this ensuing scandal, the defendant lost his job as a public school teacher and had long lasting ramifications on the defendant's working career and personal life.[170] Although this is an extreme example, the Court's ruling protects against such cases becoming commonplace. The Court made it clear with its decision, as well as other recent decisions,[171] that it intends to strictly protect privacy rights as technology continues to become more entrenched in Americans' lives.

Cell phones place vast quantities of personal information literally in the hands of individuals. Denying the Court's sound reasoning of

164. *See* Search and Seizure Field Guide, *Search Incident to Arrest* 21–22, https://www.aclu.org/files/FilesPDFs/ALPR/oregon/Washington%20County%20Sheriff's%20Office/30012-30050%20Search%20and%20Seizure%20Field%20Guide.pdf (last visited Mar. 30, 2017).

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

166. *Id.* at 443–44.

167. *Id.* at 444.

168. *Id.*

169. *Id.*

170. *Id.*

171. United States v. Jones, 132 S. Ct. 945, 946–47 (2012) (holding that attachment of Global–Positioning–System (GPS) tracking device to a vehicle, and subsequent use of that device to monitor vehicle's movements on public streets, was a search within the meaning of the Fourth Amendment); *see also* Laidlaw, *supra* note 143, at 327 ("[R]ecent Supreme Court cases, most notably *United States v. Jones* and *Riley v. California*, have signaled a willingness by the Court to adopt a new jurisprudence sensitive to the capacity of technological advance to compromise privacy.").

the threat of excessive privacy intrusion would be absurd; as stated above, there are many successes created by the Court's decision. However, the Court failed to consider several potential impacts of its decision that could stand as future obstacles for arresting officers and lower courts applying the *Riley* decision.

B. Negative Results

Despite some of the positive aspects of the Court's decision, many negative implications are likely to follow in the future as well. Several potential shortcomings may plague lower courts, serving them the difficult task of applying the Court's guidance in likely-to-arise cases. Some of these negative effects are the result of the Court's failure to give weight to any other governmental interests outside the *Chimel* rationales, the possibility of officers relying on other exceptions in order to search phones without a warrant, and further-removed technological devices that do not lend themselves to exact comparison to a phone or computer. Lower courts will have to wrestle with these issues, potentially forcing the Supreme Court to enter again to clarify some of the discrepancies.

1. Alternative governmental interests

The Court weighed two specific governmental interests—officer safety and evidence preservation—in reaching the conclusion that governmental interest in searching an arrestee's phone without a warrant is low. However, the Court failed to consider other pertinent governmental interests that are also implicated during the arrest of an individual. These governmental interests, when considered along with the other twin rationales discussed by the Court, strengthen the government's argument in favor of searching phones without a warrant.[172]

One such governmental interest is efficient police work.[173] The Court recognized that its decision would "have an impact on the abil-

172. One such governmental interest is the need to obtain probative evidence. This interest was pointed out in Justice Alito's concurrence in *Riley v. California*, 134 S. Ct. 2473, 2495 (2014) (Alito J., concurring). While not explained in depth here, it is worth noting that Justice Alito was "not convinced . . . that the ancient rule on searches incident to arrest is based exclusively (or even primarily) on the need to protect the safety of arresting officers and the need to prevent the destruction of evidence." *Id.* Instead, Justice Alito believed the basis for the search incident to arrest rule was the "need to obtain probative evidence." *Id.*

173. The Court gave this interest mere lip service in its decision. *See id.* at 2493.

ity of law enforcement to combat crime."[174] It also recognized that cell phones are tools used by criminal enterprises to coordinate and communicate among its members. The information that officials can acquire from cell phones would be highly valuable in keeping potentially dangerous criminals off the streets.[175] Setting aside the privacy implications, safety to the public by removing criminals off of the streets is an ever-present interest that should be considered. The debate between privacy and protection is a hotly disputed issue, with many individuals being comfortable with some invasion into their privacy in order to maintain societal and national security.[176] One might argue that if you have nothing to hide, then there is no reason to be concerned about someone looking through your phone.[177] Indeed, being able to do so would likely lead to uncovering other wrongdoings by criminals during their arrest.[178] However, the Court found privacy more important than protection while also recognizing that its decision would adversely impact police work. Indeed, the Court stated, "[p]rivacy comes at a cost."[179]

The Court reconciles this "cost" by relying on the increased availability afforded to officers to easily request and receive warrants. The Court mentioned that changes in technology have provided officers easier and quicker access to warrants if they suspect that there is incriminating information on an arrestee's phone.[180] Indeed, such procedures allow swifter warrant issuance to the arresting officer.[181]

174. *Id.*

175. *Id.*

176. *See* Sophia Rosenbaum, *Privacy vs. protection: Public wrestles with what's most important*, NBC NEWS (June 6, 2013), http://usnews.nbcnews.com/_news/2013/06/06/18802435-privacy-vs-protection-public-wrestles-with-whats-most-important?lite (quoting several U.S. citizens, stating that they are not opposed to governmental oversight and intrusion into their personal data in order to protect against potential threats).

177. *Id.*

178. This issue is what both *Riley* and *Wurie* debated. Both were arrested, and the information on their phones led to them being charged of further, more severe crimes.

179. *Riley*, 134 S. Ct. at 2493.

180. *See* Missouri v. McNeely, 133 S. Ct. 1552, 1572–73 (2013) ("[P]olice can often request warrants rather quickly these days. At least 30 States provide for electronic warrant applications."). In many states, officers can receive a warrant by calling a judge and giving him or her the necessary information. The judge can then authorize the officer to affix the judge's signature to the warrant and proceed with the search. *See*, *e.g.*, ALA. R. CRIM. PROC. 3.8(B) (2012–2013); ALASKA STAT. § 12.35.015 (2012); IDAHO CODE §§ 19–4404, 19–4406 (2004); MINN. R. CRIM. PROC. 36.01–36.08. (2010 AND SUPP. 2013); MONT. CODE ANN. § 46–5–222 (2012). Note, however, that 40% of states do not have an electronic warrant system in place. For officers of these states, the traditional method of receiving a warrant must be followed.

181. For example, *see* Utah, e-Warrants: Cross Boundary Collaboration 1 (2008) (de-

However, due to the ban on warrantless searches of an individual's phone upon arrest, the amount of requested warrants from the magistrate judge will increase. This will increase the delay in receiving a warrant. Similarly, with such easy and regular access, obtaining a warrant simply becomes a hoop officers must jump through rather than acting as a protection against unlawful intrusion into an individual's privacy. Such easy and quick access may also create instances where officers request a warrant expecting to receive one, and before receiving it, begin to search an arrestee's phone, implicating the possibility of officer's reliance on the inevitable discovery doctrine in order to begin the search without the warrant.[182] Likewise, courts and judges now will be burdened with an increase in warrant granting, rather than focusing on the other cases they have on their dockets. The categorical rule was implemented in order to decrease litigation; by forcing officers to get a warrant to search an arrestee's phone, court involvement will actually increase, creating heavier workloads for lower courts.

In addition to the governmental interests not mentioned by the Court, there may have also been situations that the Court failed to consider in its analysis of the Government's interest in preserving evidence. The Court mentioned the possibility of remote wiping as a potential threat to the preservation of evidence. Along with this very real threat,[183] it is not difficult to think of additional situations where cautious criminals may be alerted that their partner in crime has been detained, and thus will either transport or destroy valuable evidence.

scribing Utah's "e-warrant" procedure where officers, through the use of the online system, can electronically receive a warrant). This system has led to officers receiving warrants in as little as five minutes. *See* Jason Bergreen, *Utah Cops Praise Electronic Warrant System*, SALT LAKE TRIB., Dec. 26, 2008, at B1; *see also* Gregory T. Benefiel, *DUI Search Warrants: Prosecuting DUI Refusals*, 9 KAN. PROSECUTOR 17, 18 (Spring 2012), http://www.kcdaa.org/Resources/Documents/KSProsecutor-Spring12.pdf ("From the time the officer begins completing the search warrant affidavit form to the time the judge returns the signed search warrant is now about 15 minutes.").

182. *See* Nix v. Williams, 467 U.S. 431, 440–41 (1984) (holding that evidence obtained in violation of the defendant's constitutional rights is admissible in court if it can be established that normal police investigation would have inevitably led to the discovery of the evidence); *see also* Brian S. Conneely & Edmond P. Murphy, *Inevitable Discovery: The Hypothetical Independent Source Exception to the Exclusionary Rule*, 5 HOFSTRA L. REV. 137, 154–64 (1976).

183. Eight percent of individuals have installed software on their phone that would enable them to remotely wipe their phones. *Smart phone thefts rose to 3.1 million in 2013*, CONSUMERREPORTS.ORG (May 28, 2014, 4:00 PM), http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm. Likewise, 7% of smartphone owners use some other form of encryption on their devices other than the lock screen. *Id.*

For example, one individual that is about to participate in a crime may instruct a friend that his or her failure to answer a phone call after a certain amount of call attempts should trigger the friend to move, conceal, or destroy other damning evidence of past or future crimes. While not every instance of a person's failure to answer a phone call three or four times in a row will lead to the destruction of evidence, it is a possibility not addressed by the Court. Even without an agreement, a co-conspirator may be tipped off that their accomplice has been detained when the accomplice does not answer their phone calls or text messages after several attempts.[184] An officer's inability to now look at incoming phone calls or messages may potentially lead to the loss of valuable evidence.

Similarly, some applications on a phone may alert an arrestee's accomplices of their detention. Certain applications now allow you to monitor where another user of the application is located by tracking the phone's location.[185] An app can alert accomplices in a crime when one of their comrades is in custody if they observe the phone's location is at the police station. One might argue that such a situation could easily be prevented by officers placing the phone into a bag that blocks the signal, by powering off the device, or by turning off location services. However, the app can alert an accomplice who is monitoring his or her partner's activities that some problem has occurred if he or she is no longer able to track the other's location. Furthermore, if an officer fails to do one of these preventive measures, taking the phone to the police station will alert the accomplice of the detention, giving them time to either conceal or destroy evidence of other crimes.[186]

In addition to some of these "distress calls," some of the preventative measures—turning off the phone, taking out the battery, disabling location services—may still involve officers observing information on an arrestee's phone. For example, if an officer turns off an

184. The dissent in *Wurie* brings this point up as well. Judge Howard points out that Wurie's "failure to answer these phone calls could have alerted Wurie's confederates to his arrest, prompting them to destroy further evidence of his crimes." United States v. Wurie, 728 F.3d 1, 17 (1st Cir. 2013). Judge Howard further asserts that this provided an objective basis for enhanced concern that evidence may be destroyed if the officers did not search the phone. *Id.*

185. *See, e.g.*, *About Find my Friends*, APPLE, https://support.apple.com/en-us/HT201493; *Find My Lost Phone!*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.fsp.android.phonetracker&hl=en (last visited Mar. 30, 2017).

186. This situation could be easily prevented through the use of a signal-blocking bag, but it is unclear how often police officers actually use or have access to such items.

arrestee's phone, he or she will often times illuminate the screen by pressing and holding the button that shuts down the device. In cases of older generation phones, such as the one in *Wurie*, an officer must actually open the phone in order to access the off button located on the inside of the phone. Opening the phone will automatically illuminate the screen, enabling the officer to see the main screen as he or she inspects the phone to make sure it has been powered off. Likewise, a smartphone that has a case that covers the front screen could only be turned off after opening the front flap and manually sliding or clicking on the screen to power the device down. In the course of both of these situations, the officer may observe the contents of a message that has been unread or a phone call that has been missed.[187] While such an alternative might be better than allowing officers to search the entire phone, these situations may result in officers relying on other exceptions to the warrant requirement based on their observations while turning the phone off.

Another difficult situation that lower courts may confront is whether officers can search an arrestee's phone without a warrant when that person was arrested while on the phone. What if the arrestee was speaking to another person when the officers recognized that a crime had occurred? What if the person is texting as the officers arrest him or her and the officers suspect the information sent could lead to the destruction of evidence? One might contend that such a situation would then fall under the exigent circumstances exception, but this exception could lead to other issues for the lower courts.[188]

While these government interests do not detract from the privacy implications discussed by the Court, they nonetheless make the governmental interest argument stronger in weighing it against privacy interests of individuals.

187. Most phones provide a service to users where the first portion of a text message, email, or alert appears on the phone screen, notifying the user of some of the content of the received message. *See Use Notifications on iPhone, iPad, and iPod Touch*, APPLE, https://support.apple.com/en-us/HT201925. These alerts may contain information that is viewed by the officer as he is taking preventative measures to preserve evidence. Such a situation may fall under the plain view exception, or the "freezing" of the scene while a warrant is obtained; however, this is something that lower courts will have to analyze in the future.

188. *See infra* Section III.B.2.a.

2. Alternative exceptions

The Court's decision has created a situation where officers may potentially rely on other exceptions to the warrant requirement in order to search an arrestee's phone. The *Riley* decision does not make information on a cell phone immune from any type of search. Rather, officers can still acquire a warrant in order to search a phone. In addition to this, other exceptions may give officers the right to search an arrestee's phone without a warrant. As the Court stated, "[E]ven though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone."[189]The exceptions that may prove difficult for officers and lower courts to apply are (a) the exigent circumstances exception and (b) arrestees' consent to search their cell phone's data.

a. Exigent circumstances. The Court specifically noted that the exigent circumstances exception could still apply in cases involving searches incident to arrest of cell phones.[190] Whenever one of the rationales from *Chimel*—officer safety or evidence preservation—is present, the Court felt it would be "better addressed through consideration of case-specific exceptions to the warrant requirement, such as the one for exigent circumstances."[191] Thus, when exigent circumstances appear, there is no need for an officer to obtain a warrant before conducting a search because the need for a warrant is overcome by a compelling need of law enforcement.[192] Common compelling needs of law enforcement are potential destruction of evidence, potential escape of suspects, and possible danger to the investigating officers or to citizens in the area where the search is to take place.[193] If an officer's life or the lives of others is in danger, that officer can con-

189. Riley v. California, 134 S. Ct. 2473, 2494 (2014).

190. *Id.*; *see also* United States v. Wurie, 728 F.3d 1, 13 (1st Cir. 2013) ("There are, however, other exceptions to the warrant requirement that the government has not invoked here but that might justify a warrantless search of cell phone data under the right conditions. Most importantly, we assume that the 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, as well as a compelling need to act quickly that makes it impracticable for them to obtain a warrant[.]").

191. *Riley*, 134 S. Ct. at 2486.

192. *See* Mincey v. Arizona, 437 U.S. 385, 394 (1978); Kentucky v. King, 131 S. Ct. 1849, 1856–57 (2011); *see also* Topic: Exigent Circumstances, CRIMPRO.COM, https://crimprocasebook.files.wordpress.com/2011/06/ladder3c1.pdf (last visited Apr. 8, 2017).

193. MARC L. MILLER & RONALD F. WRIGHT, CRIMINAL PROCEDURES: THE POLICE 182 (4th ed. 2011).

tinue with the investigation in order to prevent the danger he or she fears is imminent.[194]

For the exigent circumstances exception to apply, there must be an emergency situation justifying warrantless activity and there must be probable cause.[195] The Court has clarified the requirements for exigent circumstances as dependent on the severity of the crime committed and the extent of the privacy intrusion to be instigated by the warrantless search.[196] Exigent circumstances vary with the seriousness of the crime; the showing becomes more difficult as the crime under investigation becomes less serious.[197] Because "courts tend to demand greater justifications for warrantless searches of a house,"[198] the same demand likely will be required for warrantless searches of cell phones as well, especially when considering the weighty import the Court has put on the personal nature of cell phone data. While the Court generally has been reluctant to find exigent circumstances,[199] the Court has allowed exigent circumstances in the past,[200] creating a potential avenue for officers to abuse. If allowed to go unchecked, the exigent circumstances exception will swallow the warrant rule, thus making the Court's decision potentially obsolete. Officers may also begin to game the system by abusing the exception for the sake of efficient police work. While this Article does not intend to suggest that the nation's police force is corrupt, situations could arise where officers manipulate an investigation in order to apply the exigent circum-

194. *See, e.g.*, Warden Md. Penitentiary v. Hayden, 387 U.S. 294, 298–99 (1967) ("The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others."); *see also* STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE 363 (8th ed. 2007) ("The exigent circumstances exception excuses the officer from having to obtain a magistrate's determination that probable cause exists; it does not permit a search in the absence of probable cause. Besides needing probable cause to search, the officer must have probable cause to believe that the persons or items to be searched or seized might be gone, or that some other danger would arise, before a warrant could be obtained.").

195. ERWIN CHEMERINSKY & LAURIE L. LEVENSON, CRIMINAL PROCEDURE 219 (1st ed. 2008).

196. Welsh v. Wisconsin, 466 U.S. 740, 753 (1984).

197. *See id.* ("[A]pplication of the exigent-circumstances exception in the context of a home entry should rarely be sanctioned when there is probable cause to believe that only a minor offense . . . has been committed.").

198. MILLER & WRIGHT, *supra* note 193, at 183.

199. *See generally* Mincey v. Arizona, 437 U.S. 385 (1978) (rejecting a claim that there should be a blanket exception to the warrant requirement for all murder scenes).

200. *See, e.g.*, Brigham City v. Stuart, 126 S. Ct. 1943 (2006) (allowing police to act without a warrant if there is an emergency and the police believe that entering a premise will provide protection).

stances exception as opposed to obtaining a warrant.

The Court's decision in *Riley* may have also created a situation where officers are more likely to apply the exigent circumstance exception. While no such threat has actually occurred yet,[201] it is conceivable that a criminal may create a cell phone bomb undetectable on a cursory examination of the phone.[202] Officers can inspect the exterior of a phone, but now that they are unable to check the functionality of the phone, officers will be unaware that the phone is actually a weapon or an explosive instead of a normal functioning device. If even one such "phone bomb" injured or killed a law enforcement official, then officers could objectively argue that they feared that they were in imminent danger any time they seized a cell phone, thus justifying a search of the phone in order to determine that it is a normal functioning phone instead of a weapon.[203] Additionally, terrorists and radicals now have an opportunity available to them to get a bomb inside of a police vehicle, headquarters, or compound because they know that the phone will likely not be inspected as a supposed weapon.[204]

The judiciary must analyze and review the use of the exigent circumstances exception on a case-by-case basis to determine whether the circumstances indeed required a search without a warrant.[205] If

201. Hollywood has recognized the possibility of cell phones (and other less conspicuous items) to be used as weapons against officers and other government officials. *See* LAW ABIDING CITIZEN (Overture Films 2009) (judge's cell phone used as a bomb, detonating when the judge answers a phone call); THE DARK KNIGHT (Warner Bros. 2008) (cell phone bomb smuggled into police station and detonated by a call from another phone killing officers and prisoners within the holding cell area); *Breaking Bad: Negro y Azul* (AMC Network Entertainment LLC. Apr. 19, 2009) (explosives stuffed inside a tortoise and detonated to kill DEA agents).

202. Erik Schechter, *Could Terrorists Build a Bomb That Looks Like a Working Phone?*, POPULAR MECHANICS (July 10, 2014), http://www.popularmechanics.com/flight/a10935/could-terrorists-build-a-bomb-that-looks-like-a-working-phone-16972003/. Furthermore, although the argument may be improbable, the courts arguing in favor of the categorical rule likewise used events unlikely to occur in order to bolster their positions. *See, e.g.*, United States v. Wurie, 728 F.3d 1, 8 (1st Cir. 2013) (describing how a phone could be used to essentially search a person's home through the use of a webcam).

203. Powering on the phone may not be sufficient. Experts have determined that a clever enough terrorist might be able to build a bomb that passes as a working phone. Schechter, *supra* note 202. Thus, officers would potentially need to search the phone further to determine its risk of danger.

204. If officers suspect that a phone could be used as a bomb, or that it contains "some immediately dangerous instrumentality, such as explosives, it would be foolhardy to transport it to the station house" without first opening the container, or in this case, the phone, checking for potential dangers, and disarming the weapon. *See* United States v. Chadwick, 433 U.S. 1, 24 (1977); *see also* United States v. Johnson, 467 F.2d 630, 639 (2d Cir. 1972).

205. Riley v. California, 134 S. Ct. 2473, 2494 (2014) ("The critical point is that, unlike

officers use this exception, it requires a court to examine whether an emergency justified a warrantless search in each particular case. This will lead to an increase in litigation, thus countering one of the intentions of the Supreme Court in creating a bright-line rule. The practical result of officers finding convenient exceptions to the warrant requirement will potentially be worse than if the Court had allowed searches in the general case.

As technology continues to advance, lower courts will face more and more difficult questions regarding this exception. For example, what if the only personal item an arrestee has on his person is a cell phone containing all relevant information about him or herself? Will officers be able to rely on this exception when an arrestee is not cooperating and all of the arrestee's information is on the phone, including his or her identification or other items typically held in a wallet or purse? Individuals now use phones as keys to homes and vehicles as well.[206] Will the court allow an officer to access the phone if entering the home or vehicle is supported by exigent circumstances and probable cause? The *Riley* decision tends to suggest that the warrant requirement applies due to the individual's privacy being implicated. However, there may be some types of information that cannot be acquired in any other way, and in order to proceed, the officer needs that information held on the phone. If these things are eventually held exclusively on an individual's phone, the lower courts will have to decide whether such a situation fits within the exigent circumstances exception.

b. Consent. Another exception to the warrant requirement that may be problematic as a result of the *Riley* decision is consent. Officers may now try to convince arrestees to allow them to look at their phones—while avoiding undue influence or other negations of consent—so as to circumvent the warrant requirement. Officers can conduct a full search without a warrant and without probable cause if the target of the search consents.[207]A search to which an individual consents meets Fourth Amendment requirements.[208] The need to rely on consent or a warrant appears to be the Court's intention in the *Riley*

the search incident to arrest exception, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case.").

206. Todd Haselton, *Audi Mobile Key Hands-On–This Android App Turns Your Phone Into Car Keys*, TECHNOBUFFALO (Jan. 11, 2015), http://www.technobuffalo.com/videos/audi-mobile-key-hands-on-this-android-app-turns-your-phone-into-car-keys/.

207. MILLER & WRIGHT, *supra* note 193, at 214.

208. Zap v. United States, 328 U.S. 624, 630 (1946).

decision. Indeed, it is far more common for officers to conduct searches based on consent than those allowed by a search warrant.[209]

However, relying on consent can create additional problems for lower courts. Officers may try to use inappropriate means to coerce consent.[210] For example, what if an officer asks for consent from the arrestee to search his or her phone, but also informs them that if they do not consent, the officer will simply just get a warrant to search the phone?[211] While such attempts may or may not be ethical or legal, questionable attempts will give rise to an increase in litigation as individuals feel that they did not give voluntary or valid consent to search their phones. In addition to this point, almost all state courts agree that a totality of the circumstances determines whether a person consented to a search.[212] This will again cause more cases to be brought before the courts, requiring their judgment on the issues. The increase in litigation again goes against the reasoning for having a categorical rule in place, which is to reduce the amount of cases that come before the courts on that particular issue because the rule is clear on its face.

Furthermore, research shows that most people, even those that have incriminating evidence, will consent to a search if asked by an officer.[213] These studies show that many people—even those with evidence to hide—unreflectively defer to the wishes of authority figures.[214] Because *Riley* creates a situation where officers rely on consent of individuals to search their phones, the categorical rule may actually lead to an increase in phone searches because officers will be asking to search more often, and arrestees are likely to allow it, even if they have incriminating information on their phones.

Another related issue is that individuals are choosing to make their personal lives more public through social media. Could the po-

209. MILLER & WRIGHT, *supra* note 193, at 214.

210. *See* WHITEBREAD & SLOBOGIN, *supra* note 13, at 299–307 (explaining the various circumstances affecting the analysis of voluntary consent as knowledge of the right, custody, force, show of force and threats, and personal characteristics).

211. Similar situations have occurred in past cases. *See* Bumper v. North Carolina, 391 U.S. 543, 546 (1968) (describing situation where an officer informed a homeowner that he had a warrant, and then relied on the individual's consent to search the house); *see also* State v. Brown, 783 P.2d 1278, 1280–82 (Kan. 1989) (describing situation where officer stated he would seek a warrant if the person did not consent to a search).

212. *See* Schneckloth v. Bustamonte, 412 U.S. 218, 226 (1973).

213. *See* Steven L. Chanenson, *Get the Facts, Jack! Empirical Research and the Changing Constitutional Landscape of Consent Searches*, 71 TENN. L. REV. 399, 447–55 (2004).

214. *Id.*

lice not gather as much information on this individual by looking at his or her online profiles made available to the public on the internet? Similarly, could officers argue that if there is not a passcode on the phone, that there is implied consent to search the arrestee's phone? Other people would have access to the phone's content if no passcode were on the phone and the phone's owner were to leave it somewhere.[215] Are failures to password-protect a cell phone essentially implied consent for others to look at that phone?[216] In some states, officers that approach a home for the sole purpose of obtaining consent to search the home must inform the resident that he or she does not have to consent.[217]Because cell phones are compared to homes as far as privacy concerns go, are officers under the same obligation to inform cell phone owners that they are not required to consent to the search? Is it possible for third parties to consent to the search of an arrestee's phone to which the third party also has access?[218] There are no clear answers to these questions. Such issues may likely arise in future cases before the lower courts, creating difficult judgment calls for judges to make.

3. Other technological devices and advancements in technology

While the Supreme Court's decision will likely apply to other "computer-like" devices, the line between which devices are computer-like and which devices are not is unclear. Cell phones now have a

215. Most people do not take any steps to secure their phone in the case that it is stolen, lost, or taken from them. *See* Herb Weisbaum, *Most Americans Don't Secure Their Smartphones*, CNBC (Apr. 26, 2014), http://www.cnbc.com/2014/04/26/most-americans-dont-secure-their-smartphones.html (stating that 34% of all smartphone owners do absolutely nothing, including not creating a simple code to lock the screen, in order to protect their phones); *cf.* BOARD OF GOVERNORS OF THE FED. RES. SYS., CONSUMERS AND MOBILE FINANCIAL SERVICES 6 (March 2015), http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf ("Consumers appear to be more cognizant of the need to protect the personal information stored on their phones, as they are increasingly using passwords to protect their smartphones. The share of smartphone owners who password protect their phone increased to 69 percent in 2014, from 61 percent in 2013 and 54 percent in 2012.").

216. This argument likely holds little weight in court because it would be similar to saying that because a person leaves the front door of their home open or unlocked that police officers could then assume they had consent to search it. While this is not a strong argument, it is still a situation that could arise and that would lead to more litigation in the lower courts.

217. *See, e.g.*, State v. Brown, 156 S.W.3d 722, 731 (Ark. 2004).

218. *See* Georgia v. Randolph, 547 U.S. 103, 106 (2006) (explaining that a third party has actual authority to consent to a warrantless search of a home, and thus presumptively also a cell phone, by the police when the third party shares common authority over the home, or as applied to our scenario, a cell phone).

clear rule in that they cannot be searched. However, it is less clear when it comes to other computer-like devices such as laptops, tablets, palm pilots, or other computing devices with storage capacity and processing capabilities. It is very likely that such devices will follow the same rule since they have many of the same storage capabilities and processing functionalities that a modern cell phone does and would likely implicate the same privacy concerns that the Court acknowledge in *Riley*.

However, the line is blurred when it comes to devices that lack significant storage capacities or functioning capabilities. For example, a variety of digital devices—such as the Apple Watch, Google Glasses, Fitbit, or other wearable Bluetooth accessories for a phone[219]—provide individuals access to an assortment of features that the typical phone has. These devices, however, are limited in their storage capacity and do not mirror all of the functioning capabilities that a cell phone has. Would these items be searchable incident to a lawful arrest? It is unclear how the lower courts trying to reconcile these devices with the Court's ruling in *Riley* would rule on such an issue.[220]

Similarly, it remains unclear how courts will deal with situations involving hard drives, USB drives, or thumb drives found on an arrestee's person. These devices have huge amounts of storage capacity, but they do not possess the computing functionalities that a phone does. Furthermore, it is unlikely that such items contain data that is private in nature. The courts will have to deal with these cases in the likely not-so-distant future and determine whether they are covered under *Riley*, or if officers are allowed to search such items under the search incident to arrest doctrine.

With the digitalization of everything, it is more likely than not that the Court's decision will need to be revisited again soon. Expo-

219. How lower courts will handle devices that track the owner's location and movement is unclear. Examples of such devices are Garmin watches, Fitbit, or Nike Fit technology. Such technology will track the user's location, physical activity, heart rate, pace, and even certain phone notifications. Will such technology also be protected under the *Riley* decision? Likely so, but lower courts will have to grapple with these issues. As technology continues to advance and becomes more engrained in each item a person wears or carries with him or her on a daily basis, arresting officers will be faced with difficult decisions and challenges as to what items are under *Riley's* protection. Courts will have establish precedent, and it is likely that the changes in technology to come will force the Supreme Court or legislature to become involved in resolving the matter.

220. It is conceivable to picture lower courts viewing such devices as either a gateway to access the personal information on the phone, or as stand alone devices that do not possess nearly as much personal information that the cell phone does.

nential growth of technology over time will make it increasingly difficult to stay atop the ever-changing technological advancements.[221] Such changes will continue to occur at an accelerated rate.[222] Similarly, changes in technology may change many of the justifications that the Court relied so heavily on in reaching its decision. For example, with the rise of voice-activated technology, an arrestee may still have access to his or her phone despite it not being in his or her possession. The Court rejected the argument of the need to preserve evidence by pointing out that the *Chimel* justification focuses on the arrestee's ability to conceal or destroy evidence, not the ability of third parties to do so. The Court reasoned that once an officer places an arrestee under arrest, the arrestee's own ability to destroy or conceal evidence contained on his or her cell phone is eliminated. However, the Court failed to consider the possibility of an arrestee's ability to access functions or data on the phone without having to have physical access to the phone. Voice-command technology has now adapted to only respond to one user, and such technology could potentially allow an owner to erase incriminating data held on the phone through use of his or her voice. This technology would threaten the preservation of evidence, undermining one of the Court's justifications for not allowing warrantless searches of cell phones.[223] Similarly, some Bluetooth technology allows users to control phone functions from wearable devices.[224] Massive technological changes and shifts will likely create entirely new problems the Court did not consider, and that lower courts will be forced to face and reconcile.

CONCLUSION

How each of these possible issues evolves with time and how the lower courts will deal with each of these potential conflicts remains

221. Michael G. Daigneault, *A Matter of Foresight*, CUES (July 2013), http://www.cues.org/article/view/id/A-Matter-of-Foresight.

222. *Emerging Technology Overview*, TRACE CTR. (Feb. 16, 2007), http://trace.wisc.edu/tech-overview/indexe9e5.html?attachment_id=256.

223. Although the phone could be removed from the owner and taken outside of voice range, the possibility of a voice-command data wipe is a realistic threat, and one that will continue to grow in plausibility considering the amount of voice-activated technology devices out on the market. *See* Johnny Crowder, *Have You Met Alexa, Amazon's Siri Competitor Yet?*, THE AMERICAN GENIUS (Jan. 25, 2015), http://theamericangenius.com/tech-news/met-alexa-amazons-siri-competitor-yet/ (describing Amazon's attempt to create a voice-activated device to compete with Apple's Siri and Google Now).

224. For example, an arrestee could use a smart watch to send or delete text messages despite being physically separated from the phone, but still within Bluetooth connectivity range.

undetermined. In the mean time, the successes of the Court's decision will provide clear guidance to lower courts in regards to cell phones being seized and searched during a search incident to a lawful arrest. The bright-line rule established by the Supreme Court's decision is a solid victory for privacy protection. However, as circumstances change and technology continues to evolve and advance, the Court's decision in *Riley* may lead to many other unintended and unanticipated consequences, burdening the lower courts with cases that are not exactly congruent to a cell phone search. The lower courts will either have to analyze the case within the standard set out in *Riley*, or to differentiate it as outside the *Riley* boundaries. Either way, lower courts will have a difficult time adjusting without further guidance from the legislature or the Court.

Parker Jenkins∗

∗ J.D., April 2017, J. Reuben Clark Law School, Brigham Young University.