CRIMINAL PROCEDURE—More Protection for Digital Information? The Supreme Court Holds Warrantless Cell Phone Searches do not Fall Under the Search Incident to Arrest Exception; Riley v. California, 134 S. Ct. 2473 (2014)

James B. Peters

Follow this and additional works at: http://repository.uwyo.edu/wlr

Part of the Law Commons

Recommended Citation

Case Note

CRIMINAL PROCEDURE—More Protection for Digital Information? The Supreme Court Holds Warrantless Cell Phone Searches do not Fall Under the Search Incident to Arrest Exception;

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

James B. Peters*

INTRODUCTION

As technology advances, the balance between the governmental and individual privacy interests fluctuates.¹ For example, advances in cell phone technology have changed the way people communicate and store private information.² Originally, cell phones were primarily used for verbal communication. The “smart phone,” however, has vastly expanded cell phone capabilities.³ Smart phones are used for a wide array of functions including storing financial data, photographs, e-mails, and personal calendars.⁴ Because cell phones have the capability to store large quantities of data, courts face the issue of whether information stored on a cell phone is protected from warrantless searches under the Fourth Amendment.⁵ In

* J.D. candidate, University of Wyoming College of Law, Class of 2016. I would like to thank the 2014–2015 Wyoming Law Review Editorial Board for their insightful comments and patience throughout the writing process. I would also like to thank Professor Darrell Jackson and Professor Jerry Parkinson for taking the time to provide me with valuable feedback and guidance. Finally, I would like to thank my family, friends, and Ms. Jasmine Fathalla for their continued support and encouragement.

¹ See e.g., Riley v. California, 134 S. Ct. 2473 (2014); United States v. Finley, 477 F.3d 250, 258 (2007).


³ See id. A 2013 study conducted by the Pew Research Center found that more than ninety-one percent of all Americans use cell phones. Lee Ranie, Cell Phone Ownership Hits 91% of Adults, PEW RESEARCH CENTER (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/. This case note uses the term “cell phone” to encompass both smart phones with internet and advanced computing capabilities as well as traditional cell phones with only the capability to make and receive phone calls and send/receive text messages. A smart phone is a cellular phone with a broad range of functions based on advanced computing capability, large storage capacity, and Internet connectivity. Riley v. California, 134 S. Ct. 2473, 2479 (2014).

⁴ See Riley v. California, 134 S. Ct. 2473, 2489 (2014). Smart phones today not only have the ability to record data on incoming and outgoing calls and text messages, but also information about how often an individual accesses the Internet, what websites were browsed, and the individual’s location. Fact Sheet 2b: Privacy in the Age of the Smartphone, PRIVACY RIGHTS CLEARINGHOUSE, (Feb. 2, 2015), available at https://www.privacyrights.org/smartphone-cell%20phone-privacy#smartphonedata.

⁵ See Riley, 134 S. Ct. at 2479.
Riley v. California, the United States Supreme Court addressed this issue and held that warrantless cell phone searches are not permissible during a search incident to lawful arrest (SILA).6 This case note examines Riley and argues that, although the holding is supported by public policy, it improperly protects digital information to a greater degree than it does tangible documents under the Fourth Amendment, leading to unintended consequences.7

The first part of this case note discusses the history of the Fourth Amendment, the prohibition against unreasonable search and seizures, and the legal precedent regarding searches incident to lawful arrest.8 The second part outlines the facts and the majority and concurring opinions of Riley.9 The third part argues that while the holding of Riley is consistent with public policy, unintended consequences may result which will require the Court to reevaluate the treatment of tangible items during a SILA in the future.10

BACKGROUND

The Fourth Amendment

The Fourth Amendment of the United States Constitution is a vital safeguard of the right to individual privacy. Specifically, it provides: “The right of the people to be secure in their persons, houses, papers, and effects . . . [.].”11 More generally, the Fourth Amendment requires adherence to judicial processes to obtain a warrant.12 The judicial process for obtaining a warrant requires a magistrate or judge to authorize and issue a search or arrest warrant based upon a sufficient showing of probable cause.13 Searches conducted outside the judicial process, without prior approval by a judge or magistrate, are held to be per se unreasonable.14 However, as the U.S. Supreme Court held in Johnson v. United States, “[t]here are exceptional circumstances . . . [under which] a magistrate’s

6 Id. at 2493.
7 Id. at 2480.
8 See infra notes 11–82 and accompanying text.
9 See infra notes 83–154 and accompanying text.
10 See infra notes 155–200 and accompanying text.
11 U.S. CONST. amend. IV.
13 FED. R. CRIM. P. 41(b). The Fourth Amendment requires that a warrant be supported with probable cause and that it particularly describes the person or place to be searched or seized. U.S. CONST. amend. IV.
warrant for a search may be dispensed with. 15 One exception to the warrant requirement of the Fourth Amendment is a SILA. 16

Search Incident to Lawful Arrest

A SILA is a valid search of an arrestee conducted without a warrant in order to remove weapons and seize evidence on an arrestee’s person. 17 In Agnello v. United States, the U.S. Supreme Court stated:

The right without a search warrant contemporaneously to search persons lawfully arrested while committing crime and to search the place where the arrest is made in order to find and seize things connected with the crime as its fruits or as the means by which it was committed, as well as weapons and other things to effect an escape from custody, is not to be doubted. 18

SILAs are justified as an exception to the warrant requirement for two reasons: to protect and maintain officer safety during an arrest, and to preserve evidence after making an arrest. 19 During a SILA, police officers are authorized to search the person, purses, wallets, and other objects found on the arrestee’s person. 20 The SILA exception is only available at the time of an arrest. 21 Under this exception, the government’s interest in preserving evidence and officer safety outweighs individual privacy rights, thus justifying the search. 22

In the late 1940s and early 1950s, the U.S. Supreme Court established the broad scope of a SILA exception in Harris v. United States and United States v.

---

15 Johnson v. United States, 333 U.S. 10, 14–15 (1948) (holding that if the need for effective law enforcement outweighs the right of privacy, the warrant requirement may be dispensed with). Exceptions to the general rule requiring search warrants include: exigent circumstances, searches incident to lawful arrests, searches of cars and containers therein, the plain view doctrine, inventory searches, and consent. See 1 Joshua Dressler & Alan C. Michaels, Understanding Criminal Procedure: Investigation 179–259 (6th ed. 2013).

16 William W. Greenhalgh, The Fourth Amendment Handbook, 16 (2010). Other recognized exceptions to the warrant requirement include: The Carroll Doctrine, the suitcase or container exception, exigent or emergency circumstances, stop and frisk, the plain view doctrine, and consent by the party to be searched. See Joshua Dressler & Alan C. Michaels, supra note 15.


20 See Joshua Dressler & Alan C. Michaels, supra note 15 at 191.


In *Harris*, the defendant was arrested pursuant to a valid warrant at his apartment for mail fraud and intent to defraud a bank. After the arrest, agents searched each room of the apartment and all furniture, ultimately discovering in a closed bedroom drawer incriminating documents in an envelope marked “George Harris, personal papers.” The Court addressed whether the search was a valid SILA and held that because the evidence was obtained without violating the defendant’s constitutional rights, the search was valid. Moreover, the Court recognized that “a search incident to arrest may . . . extend beyond the person [of the arrest] to include the premises under his immediate control.” Because the defendant in *Harris* was in exclusive possession of the entire apartment, his control extended to all of the rooms, not just the room in which he was arrested.

A few years after *Harris*, the Court decided the issue of whether a search of an arrestee’s entire office fell under the scope of a valid SILA in *Rabinowitz*.

In *Rabinowitz*, the defendant was arrested at his place of business for possessing and concealing forged government postage stamps. After Rabinowitz’s arrest, police officers searched the desk, safe, and file cabinets in his office and seized 573 stamps. The Court held the search valid as incident to a legal arrest. Writing for the majority, Justice Minton reasoned that a SILA includes the premises under the control of the person arrested and the area in which the crime was committed.

Twenty years later, the foundational case of *Chimel v. California*—which discussed the boundaries of the SILA exception—called into question the holdings in *Harris* and *Rabinowitz*. After Defendant was convicted of burglary, he appealed through the California state court system claiming the police obtained evidence during an unconstitutional search of his home. Upon review, the Supreme Court of California determined that a warrantless search of an arrestee’s home is

---

24 *Harris*, 331 U.S. at 148.
25 *Id.* at 149. The agents discovered incriminating evidence which was presented at trial, leading to the defendant’s conviction. *Id.*
26 *Id.* at 155.
27 *Id.* at 151.
28 *Id.* at 152.
30 *Rabinowitz*, 339 U.S. at 58.
31 *Id.* at 59.
32 *Id.* at 60.
33 *Id.* at 61.
justified if the search was conducted incident to a valid arrest inside the home.\(^{35}\)

Thereafter, the United States Supreme Court granted certiorari, and overruled both *Harris* and *Rabinowitz*, holding that the search of a home is unjustified under the SILA exception because, by going beyond the arrestee’s person and the area within his immediate control, the search’s scope was exceeded.\(^{36}\) In *Chimel*, the Court stated that a warrantless SILA is reasonable only when executed to seize weapons that could be used to assault an officer or to preserve evidentiary items from possible destruction.\(^{37}\) Furthermore, the Court held a valid SILA only includes the arrestee’s person and the area *within his immediate control*.\(^{38}\) Although *Chimel* provided guidance on the boundaries of a SILA, the Court did not address whether arresting officers may search containers found in the area within an arrestee’s immediate control. This issue stood open for debate until 1973, when the Court decided *United States v. Robinson*.\(^{39}\)

**SILAs and Containers**

In *Robinson*, the Court attempted to create a bright-line rule regarding whether law enforcement officers may search containers during a SILA.\(^{40}\) In doing so, the Court revisited the scope of a SILA and addressed the issue of whether a police officer may search tangible items found on an arrestee’s person during an arrest.\(^{41}\) The defendant in *Robinson* was stopped by a police officer and arrested for operating a vehicle under a revoked driver’s license.\(^{42}\) In accordance with standard police procedures, the officer searched the defendant and felt an object in the left breast pocket of defendant’s coat, but could not readily identify the object.\(^{43}\) To ensure the item was not a weapon, the officer reached into the defendant’s pocket and pulled out the object: a “crumpled-up cigarette package.”\(^{44}\) As the officer

---

\(^{35}\) *Id.* at 753–55. In *Chimel*, three police officers arrested Defendant inside his own home for the burglary of a coin shop. The officers asked for permission to look around Defendant’s home, and Defendant denied their request. The officers subsequently searched the entire house, and directed Defendant’s wife to open drawers in some rooms. The officers seized numerous items that were admitted into evidence during trial for burglary charges. Chimel argued that the items were unconstitutionally seized. His argument was rejected and he was ultimately convicted. *Id.*

\(^{36}\) *Id.* at 768.

\(^{37}\) *Id.* at 764.

\(^{38}\) *Id.* at 763 (emphasis added). The Court defined the area within one’s immediate control as the area from within which the arrestee might gain possession of a weapon or destructible evidence. *Id.*


\(^{40}\) JOHN WESLEY HALL, JR., SEARCH AND SEIZURE 22–2 (5th ed. 2013).

\(^{41}\) *Robinson*, 414 U.S. at 218.

\(^{42}\) *Id.* at 220.

\(^{43}\) *Id.* at 223.

\(^{44}\) *Id.*
felt the package, he believed the package did not contain cigarettes. Therefore, the officer opened the package and found capsules of white powder, which later proved to be heroin. The capsules were seized and admitted into evidence at the defendant’s trial.

The Court began its analysis by reiterating the rationales underlying a SILA: protection of arresting officers and preservation of evidence. The Court stated that the purpose of a SILA applies to all arrests, and explained that the likelihood of an arrestee possessing a dangerous weapon does not depend on the type of crime committed. Based on the SILA justifications, the Court held that all custodial arrests provide the officer with the ability to search the arrestee to evaluate the potential presence of weapons, and to ensure preservation of evidence. Justice Rehnquist added that, although an object is removed from the defendant’s person, the officer is entitled to inspect the object and seize fruits probative of criminal conduct.

In 2009, expanding on Robinson, the Court addressed the issue of whether police officers are permitted to search a vehicle incident to an arrest in the seminal case Arizona v. Gant. In Gant, the defendant was arrested for driving under a suspended license. After his arrest, the defendant was placed in the back of a patrol car and his vehicle was searched. The Court held the SILA exception did not apply in this situation because the defendant did not have the ability to retrieve weapons or destroy evidence at the time of the search. In arriving at this decision, the Court extended the Chimel standard to the search of vehicles. The Court stated that police officers are authorized to search a vehicle incident to an arrest only when the arrestee is “unsecured and within reaching distance of the passenger compartment at the time of the search.” In addition, the Court held

---

45 Id.
46 Id.
47 Id. at 234.
48 Id.
49 Id.
50 Id. at 236. (citing Harris v. United States, 331 U.S. 145, 154–55 (1947); Warden v. Hayden, 387 U.S. 294, 299, 307 (1967); Adams v. Williams, 407 U.S. 143, 149 (1972)).
52 Id at 332.
53 Id.
54 Id at 333.
55 See id. at 343.
56 See Gant, 556 U.S. at 343. Although a search is reasonable in these circumstances, Justice Stevens stated that it is a rare situation because police officers are trained and equipped to ensure a safe arrest of the occupants of a vehicle. Id. at 340 n.5.
an officer is permitted to search an arrestee’s entire vehicle if the officer reasonably believes he will discover evidence relevant to the crime of the arrest.57

*Gant*, *Robinson*, and *Chimel* all provide foundational information and boundaries for delineating when application of the SILA exception to the warrant requirement is justified.58 However, these cases do not address the SILA exception as applied to digital storage devices.59 Because *Gant*, *Robinson*, and *Chimel* did not address digital devices, courts are being forced to reexamine the SILA exception in its entirety as digital storage technology continues to advance.60

**SILA and Cell Phones**

When faced with the issue of whether warrantless cell phone searches and other digital devices are permitted during a SILA, many courts have answered affirmatively.61 For instance, in *United States v. Finley*, the Fifth Circuit addressed whether the SILA exception applied to cell phone searches generally.62 *Finley* held warrantless searches of call records and text messages contained on an arrestee’s cell phone are permissible during a SILA.63 Applying the holding from *Robinson*, the court held the search of the cell phone was both reasonable and lawful.64 Moreover, *Finley* stated “[p]olice officers . . . may look for evidence of the arrestee’s crime on his person in order to preserve it for use at trial.”65 The court

57 *Id.* at 335.

58 See supra notes 35–57 and accompanying text.


60 See infra notes 61–76 and accompanying text.


63 *Id.* at 253–59. In *Finley*, Defendant was arrested for aiding and abetting possession with intent to distribute methamphetamine. Upon arrest and questioning, a Drug Enforcement Agency (DEA) Special Agent searched through call records and text messages contained within Defendant’s cell phone. The agent discovered text messages on the cell phone that appeared to be related to narcotics use and trafficking. Defendant contended that the text messages and other information obtained from the search of his cell phone should not have been allowed as evidence during his trial. *Id.*

64 *Id.* at 259.

65 *Id.* (citing *United States v. Robinson*, 414 U.S. 218 223–24 (1973)). In *Finley*, the defendant was arrested for possession with intent to distribute methamphetamine. The defendant’s cell phone was searched for evidence of narcotics use and trafficking. *Id.* at 255.
also noted that the permissible scope of a SILA extends to any container found on an arrestee’s person.\textsuperscript{66} Relying on Robinson and Chimel, Finley concluded the warrantless search was lawful as a SILA, and therefore the officer was permitted to search the defendant’s phone pursuant to his arrest.\textsuperscript{67}

Similarly, in\textit{ People v. Diaz}, the court upheld a warrantless search of a cell phone incident to an arrest.\textsuperscript{68} In\textit{ Diaz}, the defendant was arrested for co-conspiring in the sale of ecstasy.\textsuperscript{69} A detective seized the defendant’s cell phone and a sheriff conducted a warrantless search of text messages contained on the cell phone at the sheriff’s station and found evidence of an illegal drug transaction.\textsuperscript{70} The defendant moved to suppress the incriminating evidence contained in the text messages, but was unsuccessful.\textsuperscript{71} The California Supreme Court held that based on the United States Supreme Court’s binding precedent, “the warrantless search of defendant’s cell phone was valid.”\textsuperscript{72} Given the cell phone was within the area of the defendant’s immediate control, the court applied the rationale from Robinson and determined the arresting officer was entitled to inspect the phone’s contents without a warrant.\textsuperscript{73} The defendant argued that based on the quantity of personal information cell phones store, it should not be treated as a container.\textsuperscript{74} The court rejected this argument stating that “the [Supreme Court] has expressly rejected the view that the validity of a warrantless search depends on the character of the searched item.”\textsuperscript{75} Before Riley, the Court did not address whether digital information is equivalent to tangible information for the purposes of a SILA. However, in other aspects of the law, the Court has treated digital information as equivalent to its tangible counterpart.\textsuperscript{76}

\textbf{Digital Information}

One example where Congress held digital information to be equivalent to its pre-digital counterpart is provided by the Federal Rules of Evidence (FRE).\textsuperscript{77}

---

\textsuperscript{66} Id. at 259 (citing United States v. Johnson, 846 F.2d 279, 282 (5th Cir. 1988)).
\textsuperscript{67} Finley, 477 F.3d at 260.
\textsuperscript{69} Id. at 503.
\textsuperscript{70} Id. at 502–03.
\textsuperscript{71} Id. at 503.
\textsuperscript{72} Id. at 511.
\textsuperscript{73} Id. at 506.
\textsuperscript{74} Id.
\textsuperscript{75} Id. at 507 (citing United States v. Ross, 456 U.S. 798, 825 (1982)).
\textsuperscript{76} See e.g. \textit{Fed. R. Evid.} 1001.
\textsuperscript{77} \textit{Fed. R. Evid.} 1001. The Federal Rules of Evidence were adopted by order of the Supreme Court in 1972. \textit{Federal Rules of Evidence, Legal Information Institute}, http://www.law.cornell.edu/rules/fre (last visited Feb. 28, 2015). The purpose of the FRE was to provide uniform rules to govern
Rule 1001, in the FRE, provides definitions for the contents of writings, recordings and photographs.\(^7^8\) The Rule states: “[w]ritings and recordings consist of letters, words, or numbers, or their equivalent, set down by handwriting, typing, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.”\(^7^9\) Congress specifically enacted Rule 1001 with the intent to treat tangible and digital information equal for the purposes of evidentiary matters.\(^8^0\) The United States Supreme Court adopted these rules with the understanding that, in evidentiary inquiries, digital documents would be equivalent to their pre-digital counterparts.\(^8^1\) Interestingly, in Riley v. California, the Court departed from its previous treatment of digital information, as equivalent to tangible documents, and held that warrantless searches of cell phones violate the Fourth Amendment.\(^8^2\)

**Principal Case**

**Factual Background**

In Riley v. California, defendant David Riley was stopped by a police officer while driving a motor vehicle with expired registration tags under a suspended driver’s license.\(^8^3\) Riley’s car was subsequently impounded and a standard inventory search of the vehicle was conducted.\(^8^4\) The search revealed two handguns under the hood of Riley’s car.\(^8^5\) After this discovery, Riley was arrested for possession of concealed and loaded firearms and the arresting officer searched Riley incident to arrest.\(^8^6\) The officer confiscated and explored Riley’s cell phone, resulting in the

---

\(^7^8\) Fed. R. Evid. 1001.

\(^7^9\) Fed. R. Evid. 1001(a)–(e).

\(^8^0\) Fed. R. Evid. 1001 advisory committee’s note. “Present day techniques have expanded methods of storing data, yet the essential form which the information ultimately assumes for usable purposes is words and figures.” Id.

\(^8^1\) See supra notes 77–79 and accompanying text.

\(^8^2\) Riley v. California, 134 S. Ct. 2473, 2493 (2014).

\(^8^3\) Id. at 2480.

\(^8^4\) Id. After lawfully taking custody of vehicles or other property, police officers may conduct a warrantless search of property in police custody. Courts have held inventory searches of vehicles to be lawful including searches of passenger compartments, glove compartments, trunk, engine compartments, and any containers in the vehicle. Article: I. Investigations and Police Practices, 37 Geo. L. J. Ann. Rev. Crim. Proc. 3.

\(^8^5\) Riley, 134 S. Ct. at 2480.

\(^8^6\) Id. The arresting officer found items associated with the “Bloods” street gang. The “Bloods” are a national street gang, and one of the most violent criminal organizations in the United States. Gang activities include murder, assault, robbery, and narcotics distribution. COMMONWEALTH OF VA. DEPT’’ OF STATE POLICE VA, FUSION CT’R, BLOODS STREET GANG INTELLIGENCE REPORT, (Nov. 2008), available at https://info.publicintelligence.net/BloodsStreetGangIntelligenceReport.pdf.
discovery of information consistent with members of the Bloods street gang. Two hours after Riley’s arrest, a gang detective analyzed the information stored on Riley’s phone and found incriminating photographs of Riley.

These photographs led to additional charges and ultimately, Riley was convicted of assault with a semiautomatic firearm, firing at an occupied vehicle, and attempted murder. The district court denied Riley’s motion to suppress and convicted him on all charges. The appellate court affirmed the district court’s holding, and the California Supreme Court denied Riley’s petition for review. However, the U.S. Supreme Court granted certiorari to determine whether the trial court erred in denying Riley’s motion to suppress the evidence obtained from his cell phone.

Majority Opinion

The Court addressed whether police officers can search digital information stored on a cell phone seized from an individual during a SILA without a warrant. Writing for the majority, Chief Justice Roberts stated that warrantless searches of digital information on cell phones conducted during a SILA violate the Fourth Amendment. The Court’s analysis began by examining whether such a search was reasonable. In doing so, the Court looked to Chimel for guidance.

As stated in Chimel, the first rationale for a SILA is to ensure officer safety. In Riley, the Court addressed whether digital data stored on a cell phone could be used as a weapon to endanger the arresting officer. The Court held that a cell phone could no longer be used as a weapon after the initial search for

---

87 Riley, 134 S. Ct. at 2480.
88 Id. The detective searched Riley’s phone to find other evidence, such as pictures or videos, which might link Riley to the Bloods street gang. The detective found photographs of Riley standing in front of a car thought to be involved in a gang shooting a few weeks earlier. Id. at 2481.
89 Id. at 2481.
90 Id.
91 Id.
92 Id.
93 Id. at 2480.
94 Id. at 2485.
95 Id. at 2482.
96 Id. at 2485 (holding that purpose of a SILA is to prevent the arrestee from obtaining a weapon to use against the officer or obtaining destructible evidence).
97 Id. at 2484.
98 Id.
physical weapons contained around or inside the cell phone occurred. Because no potential physical threats were present in Riley, the Court found the additional search of the data stored on the cell phone failed to satisfy the officer safety justification of Chimel.

Next, the Court examined the second rationale for a SILA as stated in Chimel. This analysis required the Court to determine if a search of the digital information on Riley’s cell phone prevented the destruction of evidence. Riley argued that once a cell phone is confiscated, an arrestee is no longer able to delete, alter, or destroy any incriminating evidence stored on the cell phone. Therefore, according to Riley, the preservation of evidence justification for the SILA exception did not apply. In comparison, the prosecution argued that both remote wiping and data encryption are methods used to destroy evidence after a cell phone is confiscated. Based on that contention, the prosecution maintained the warrantless search of the defendant’s cell phone was justified to preserve evidence.

In response to both arguments, the Court suggested alternative methods police officers could have implemented in order to prevent remote wiping and data encryption from occurring. First, Chief Justice Roberts explained that because

---

99 Id. While the data stored in the phone did not qualify as a weapon, the majority explained that police officers are free to search the area between the cell phone and a cell phone case. A search of these areas may be conducted to ensure that a physical weapon—such as a razor blade—that may pose harm to the arresting officer is not hidden in a phone. Id.

100 Id. The prosecution further argued that searching cell phone data may alert the arresting officer if the arrestee had notified other assailants who may come to the scene and potentially cause danger to the officer. The Court held the aforementioned interest in protecting an arresting officer did not justify a bright-line rule disposing of the warrant requirement to search the contents of a cell phone during a SILA. Id. at 2485–86.

101 Id.

102 Id.

103 Id.

104 Id. at 2486.

105 Id. Remote wiping occurs when a phone connected to a wireless network receives a signal which causes all data stored on the phone to be erased. Remote wiping can be triggered by the two following circumstances: activation by a third party, or automatic preprogramming of the phone to delete data under specific circumstances, such as leaving a certain geographic area. Data encryption is an additional security feature that some cell phones use to protect stored data in addition to a passcode protection. When a cell phone locks, the data become protected by a sophisticated encryption algorithm that is inaccessible unless the password is entered. Id.

All major cell phone manufacturers provide remote wiping capabilities and such capability may also be purchased from a mobile security company. United States v. Flores-Lopez, 670 F.3d 803, 807 (7th Cir. 2012).

106 Riley, 134 S. Ct. at 2486.

107 Id.
remote wiping occurs when a cell phone is connected to a wireless network, police officers could have simply removed the battery from the cell phone.108 Second, the majority suggested that the officers could have used a faraday bag to prevent data encryption.109 As a result, the Court concluded that the possibility of remote wiping and data encryption did not justify a warrantless search of the arrestee’s cell phone during the SILA.110 Chief Justice Roberts also reasoned that it was not clear whether a warrantless search would prevent occurrence remote wiping.111 Based on this reasoning, the Court held that the evidence preservation rationale under Chimel did not justify the warrantless search of Riley’s cell phone.112

Even though the Court held the SILA exception in Riley was unsupported under Chimel, the prosecution argued in the alternative, stating that the search was reasonable under the Fourth Amendment because the defendant’s privacy interests were minimal.113 The government asserted that the search of Riley’s cell phone was equivalent to the search of physical items on Riley’s person.114 The Court rejected this argument because the Court found the quantity and quality of personal information cell phones store implicate a higher degree of intrusion when a search is conducted.115 The majority differentiated cell phones and non-electronic objects based on certain identifiable characteristics, including the type of information contained and the amount of information discoverable.116 Because cell phones store a significant amount of personal information, the Court detailed four privacy implications created by warrantless cell phone searches.117

First, cell phones store a wide array of information, such as videos, contact information, and personal notes. Thus, if police officers were permitted to search cell phones, they would have unfettered access to a variety of information that

---

108 Id. A cell phone that is powered off is unable to connect to a wireless network, thus preventing remote wiping from occurring. Id.
109 Id. A faraday bag is an enclosure that isolates a cell phone from radio waves while it is still powered on. Faraday bags are essentially bags made of aluminum foil that prevent the phone from receiving radio waves. Id.
110 Id. at 2486.
111 Id. at 2486. The majority continued by arguing in the alternative, stating that even if law enforcement officers had the ability to search the contents of a cell phone without first obtaining a valid warrant, it would be very unlikely that the cell phone would be in an unlocked state upon confiscation, and thus the information would be inaccessible regardless. Id. at 2487.
112 Id. at 2486. The Court noted that during an arrest, police officers have more pressing issues to attend to in order to ensure an effective and safe arrest than the search of data contained on a cell phone. Often the cell phone data may not even be able to be searched until hours after the arrest, which would not prevent remote wiping from occurring. Id. at 2487.
113 See id. at 2488.
114 Riley, 134 S. Ct. at 2488.
115 Id.
116 See id. at 2489 (distinguishing a cell phone from a cigarette package and other tangible objects).
117 Riley, 134 S. Ct. at 2489.
otherwise would be unavailable. Second, the immense storage capacity of a cell phone gives users the ability to store large quantities of private information unavailable in other forms. Third, cell phones have the ability to store information for long periods of time. Given the large storage capacity, individuals are able to store past and present information on a hand-held device. Finally, cell phones do not present a historical issue because they did not exist at the time of reference, when “physical records” documented personal information. In contrast, modern cell phones are exceedingly prevalent in society and capable of storing large amounts of personal information. In fact, more than seventy-five percent of all cell phone users indicated they kept their cell phones within five feet of themselves at almost all times. Based on the aforementioned privacy implications, the Court determined that warrantless searches of cell phones intrude on an individual’s privacy rights.

Riley also found that the quality, in addition to the quantity, of information stored on cell phones was a significant factor in the analysis. The Court explained that smart phones have the ability to browse the internet, store information on applications, and remember terms imputed into search engines. Thus, a cell phone search might reveal very personal information and significantly invade an individual’s privacy. The Court also dismissed the age-old maxim

\[ \text{Id.} \]

\[ \text{Id.} \]

\[ \text{Id.} \]

\[ \text{Riley, 134 S. Ct. at 2489. Other physical objects a person might carry around with him or herself would not record all of that individual’s acts for a long period of time, and therefore are not comparable. Id.} \]

\[ \text{Id. at 2490.} \]

\[ \text{See id.} \]

\[ \text{Riley, 134 S. Ct. at 2490 (citation omitted).} \]

\[ \text{Id. at 2493.} \]

\[ \text{Id. at 2490.} \]

\[ \text{Id.} \]

With the development of mobile application software, there is an application available for almost every aspect of an individual’s life, and such software can contain almost limitless information. As of June 2014, the iPhone App Store contains approximately 1,200,000 applications available to mobile devices. Sam Costello, \textit{How Many Apps Are in the iPhone App Store? About Technology}, \url{http://ipod.about.com/od/iphonesoftwareterms/qt/apps-in-app-store.htm} (last visited Feb. 28, 2015).

Depending on the operating system and capabilities of a particular smartphone, the number of applications it can hold ranges from 2,160 to 41,040. Sam Costello, \textit{How Many iPhone Apps and iPhone Folders Can I Have? About Technology}, \url{http://ipod.about.com/od/usingios4/qt/Iphone-Apps-Iphone-Folders.htm} (last visited Feb. 28, 2015).

\[ \text{Riley, 134 S. Ct. at 2490. An individual’s search history can contain personal information ranging from his or her health, mental state, interests, travel locations, fears, and shopping habits. Molly Wood, \textit{Sweeping Away a Search History}, New York Times (Apr. 2, 2014), \url{http://www.nytimes.com/2014/04/03/technology/personaltech/sweeping-away-a-search-history.html?_r=0}.} \]
that searching the contents of a man’s pocket is far different from the contents of his house.\textsuperscript{128} Today, a search of an individual’s pocket would likely reveal a smartphone, a device containing more information than an exhaustive search of an individual’s home would reveal.\textsuperscript{129}

In contrast, the prosecution in \textit{Riley} offered three arguments for allowing warrantless searches of cell phones upon arrest. First, the government argued the \textit{Gant} standard for vehicle searches should be extended to the warrantless search of cell phones.\textsuperscript{130} The Court rejected this argument because it requires the arresting officer to determine whether the phone contains evidence of a crime on a case-by-case basis, instead of creating a bright-line rule.\textsuperscript{131} Moreover, extending the \textit{Gant} standard to cell phone searches provides police officers with unfettered authority to search the contents of a cell phone.\textsuperscript{132}

Second, the government proposed to limit searches to the areas of a cell phone that an officer reasonably believes contain information regarding the crime committed.\textsuperscript{133} The Court rejected this proposal reasoning that these searches would likely discover information beyond the scope of the initial search.\textsuperscript{134}

Finally, the government offered a third argument that would allow a police officer to search cell phone data if information sought could have been obtained before cell phones were invented.\textsuperscript{135} In rejecting this proposition, the Court stated that a search for one specific piece of information does not justify the ability to rummage through all the other data contained on the phone.\textsuperscript{136} Further, the Court reasoned that it was implausible that Riley would have walked around with incriminating videotapes and photographs in his pockets before the invention of modern cell phones.\textsuperscript{137} Additionally, the government’s proposal was rejected because of the difficulty of comparing a modern phenomenon, such as an e-mail,

\textsuperscript{128} \textit{Riley}, 134 S. Ct. at 2490.
\textsuperscript{129} \textit{Id.}
\textsuperscript{130} \textit{Id.} at 2492. Extending the \textit{Gant} standard would allow a warrantless search of an arrestee’s cell phone whenever it is reasonable to believe it contains evidence of the crime. \textit{Id.}
\textsuperscript{131} \textit{Id.} This proposal was also rejected because the \textit{Gant} standard is based on the notion that individuals have a reduced expectation of privacy rights when motor vehicles are involved (quoting \textit{Thornton v. United States}, 541 U.S. 615, 631 (2001)).
\textsuperscript{132} \textit{Riley}, 134 S. Ct. at 2493.
\textsuperscript{133} \textit{Id.} at 2492. For example, if an arresting officer reasonably believed evidence of narcotics trafficking would be found in text messages to another individual, the officer would have the ability to search messages sent between the arrestee and the other individual.
\textsuperscript{134} \textit{Id.}.
\textsuperscript{135} \textit{Id.} at 2493.
\textsuperscript{136} \textit{Id.}
\textsuperscript{137} \textit{Id.}
to the pre-digital equivalent of that type of information, such as a letter, package, or video-tape.\textsuperscript{138}

After assessing all of the arguments, the Court held that an individual’s right to privacy outweighs the government’s interest in a warrantless search of a cell phone upon arrest.\textsuperscript{139} In analyzing cell phone searches in relation to the Fourth Amendment, Chief Justice Roberts said, “the fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.”\textsuperscript{140}

\textit{Justice Alito’s Concurrence}

Although Justice Alito agreed with the Court’s holding in \textit{Riley}, he argued the SILA exception serves a purpose more broad than ensuring officer safety and preserving evidence.\textsuperscript{141} Justice Alito contended that the basis for adoption of the SILA exception was to obtain probative evidence.\textsuperscript{142} He reasoned that after confiscation, there is no chance an item will be destroyed or used to harm the officer.\textsuperscript{143} He also argued the officer safety and evidence preservation rationales centered on the “search of the scene of the arrest and not the search of the arrestee.”\textsuperscript{144} Justice Alito reasoned that the justifications provided in \textit{Chimel} should not affect the search of the arrestee’s person incident to arrest.\textsuperscript{145}

Furthermore, Justice Alito explained that the bright-line rule established by the majority should not be applied mechanically.\textsuperscript{146} Instead, he suggested a balancing test be implemented, weighing the interests of law enforcement officers and individual’s privacy.\textsuperscript{147} Justice Alito viewed the Court’s opinion to be unjust because it provides more protection for digital information than physical information.\textsuperscript{148} Because digital information stored on a cell phone is not subject to a SILA, it is afforded greater protection than tangible items subject to the
SILA exception. Justice Alito explained if two separate individuals are arrested who possess the same information, but one has the information recorded on a piece of paper and the other has it stored on her cell phone, under the majority’s holding, the same rule does not apply to both individuals. Rather, the officer is authorized to examine the information on the paper without first obtaining the warrant, but a warrant is required to search the information contained on the other individual’s cell phone.

Finally, Justice Alito urged Congress to assess the needs of law enforcement and weigh them against the privacy interests of individuals. Based on the Court’s analysis of cell phones and the Fourth Amendment, Justice Alito suggested the issue regarding law enforcement’s ability to search digital information contained on an arrestee’s cell phone should be left for Congress to decide. Justice Alito stated modern cell phones have a wide array of capabilities including both lawful and unlawful functions and the Court is not in the best position to evaluate and weigh the government’s interest against an individual’s privacy interest.

Analysis

Although the holding is supported by public policy, Riley improperly provides heightened protection for digital information than tangible documents under the Fourth Amendment, leading to unintended consequences. First, the Court properly determined that warrantless searches of cell phones significantly intrude on an individual’s right to privacy for public policy reasons. Second, the holding improperly distinguished digital information from its tangible, pre-digital counterpart. Finally, the Court will need to reevaluate SILAs of tangible documents in the future to afford the same protection for information stored on different mediums to avoid unintended consequences.

Correct Outcome Based on Public Policy

When drafting the Constitution, the Framers did not consider how the Fourth Amendment would apply to modern technological advances because such topics

---

149 See id.
150 Riley, 134 S. Ct. at 2496 (Alito, J., concurring).
151 Id. at 2497.
152 Id.
153 Id. Justice Alito cited electronic surveillance as an example where the Court spoke on this issue first, based solely on Constitutional rights, and Congress enacted subsequent legislation and thus the issue of electronic surveillance was governed by the State and not the courts. Id.
154 Id.
155 See infra notes 158–68 and accompanying text.
156 See infra notes 169–93 and accompanying text.
157 See infra notes 194–200 and accompanying text.
were unforeseeable. In contrast, when Riley was decided, a majority of American citizens used cell phones daily as a means of communication, data storage, and entertainment. The prevalence of cell phones in society is significant because Riley advocates to protect individual privacy rights during an arrest.

The Fourth Amendment serves as a mechanism for balancing individual privacy interests against governmental interests. As Justice Harlan stated, “[an] individual’s sense of security must be balanced against the utility of the conduct as a technique of law enforcement.” In applying the Fourth Amendment balancing test, a warrantless search of a cell phone would be a significant intrusion on an individual’s right to privacy. Individual privacy rights outweigh the government’s interest in a search of a cell phone incident to arrest because warrants are generally available in a short period of time. Another factor supporting this conclusion is that law enforcement officers have other options available to preserve evidence. A bright-line rule prohibiting warrantless searches of cell phones incident to arrests prevents police officers from having the ability to access an arrestee’s personal information without a warrant. Although preventing an officer from searching an arrestee’s cell phone without a warrant may have an adverse effect on law enforcement’s ability to combat crime, Riley correctly determined that individual privacy interests outweigh the government’s interests. Additionally, if a judge or magistrate determines a search of a cell phone is reasonable and subsequently issues a warrant, the scope of the search will be narrowly defined to protect the individual from an unreasonable search.

158 Petition for a Writ of Certiorari at 26–27, Riley v. State, 134 S. Ct. 2473 (2014) (No. 13-132), 2013 WL 3934033. Even as little as thirty-five years ago, the Court could not have envisioned that the majority of arrestees would be carrying an item containing intangible evidence. Id.

159 See Lee Rainie, Cell Phone Ownership Hits 91% of Adults, PEW RESEARCH CENTER (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.


163 See infra notes 164–68 and accompanying text.

164 Petition for a Writ of Certiorari at 27, Riley v. State, 134 S. Ct. 2473 (2014) (No. 13-132). If it is necessary to search the contents of a cell phone, a warrant may be requested of a judge, signed, and e-mailed back to the officer in a short period of time. At least 30 states provide for electronic warrant applications. Missouri v. McNeely, 184 L. Ed. 2d, 696, 721 (2013). Utah is one state that uses an e-warrant procedure in which judges have been known to issue warrants in as little as five minutes. Jason Bergreen, Faster Warrant System Hailed, SALT LAKE TRIBUNE, Dec. 26, 2008 at B1.

165 See supra notes 107–09 and accompanying text.

166 See supra note 139 and accompanying text.


168 See Groh v. Ramirez, 540 U.S. 551, 557 (2004) (stating that the Fourth Amendment requires particularity in the warrant or the things to be seized).
**Digital Data Distinguished**

Although *Riley* is supported by public policy, the holding improperly provides heightened protection for digital information. Based on the Court’s treatment of digital information in other fields as well as previous SILA precedent, *Riley* improperly distinguishes digital data from its pre-digital counterpart. The holding also provides greater protection for digital information than for information contained on paper for the purposes of a SILA. As a result, *Riley* erroneously provides greater protection for information contained on an individual’s cell phone than for the same information was contained on a piece of paper in an arrestee’s pocket.

Under a Fourth Amendment analysis, the Court should have held the term “papers” to be synonymous with its digital equivalent. As Justice Alito correctly stated in his concurrence, the “Court’s broad holding favors information in digital form over information in hard-copy form.” If the same information is contained on a cell phone or a document, the Fourth Amendment should provide the same amount of protection to all “papers.” Instead, *Riley* provides police officers with a different rule to follow when searching digital information found on an arrestee. *Riley* also provides that the form in which an individual’s personal information is recorded determines the level of protection it receives, reflecting a preference for the greater protection of digital information.

Previously, the validity of a search did not depend on the character of the item being searched. However, because a custodial arrest gives police officers authority to conduct a SILA, the officer is entitled to inspect tangible objects

---

169 See supra notes 158–68 and accompanying text.
170 See infra notes 171–93 and accompanying text.
171 See *Riley*, 134 S. Ct. at 2497 (Alito, J., concurring).
172 See supra notes 148–51 and accompanying text.
173 See Brianne Gorod, The “papers and effects” on your cell phone may not be as private as you think, nat’l. CONSTITUTION CTR (August 30, 2013), http://blog.constitutioncenter.org/2013/08/the-papers-and-effects-on-your-cell-phone-may-not-be-as-private-as-you-think/; See supra note 11 and accompanying text.
177 See *Riley*, 134 S. Ct. at 2497 (Alito, J., concurring).
found on an arrestee’s person. The Court has consistently held in Gant, Robinson, and Chimel that the contents found on an arrestee may be examined without a warrant during a SILA and has “long accepted that written items found on the person of an arrestee may be examined and used at trial.” This same legal analysis should have been extended in Riley to digital data, which would allow the officer to examine the contents of an arrestee’s cell phone.

Cell Phone as a Container

In Riley, the majority distinguished a cell phone from other containers based on the quantity and quality of information stored. Yet, in Chimel, the Court overruled both Harris and Rabinowitz by stating that searches of entire homes were beyond the area within a defendant’s immediate control, but did not base its opinion on the quantity or quality of the information stored. In Rabinowitz, the officers searched the defendant’s desk, safe, and file cabinets. Those objects had the ability to store a significant quantity of personal information from the individual’s entire life. However, in Chimel, the sole basis for overruling Harris and Rabinowitz was the scope of the SILA, not the quality and quantity of information at stake. Therefore, it is reasonable to infer that if the information were stored in an area within the defendant’s immediate control, the SILA would have been valid even though the object of the search had an immense storage capacity.

In comparison to Rabinowitz, in Riley, the defendant’s cell phone was seized from his pocket incident to arrest. Based on the Chimel standard, the object of the search needed to be on the arrestee’s person or in the area within his immediate control. Because the cell phone was found on the defendant’s person in Riley, the search did not exceed the Chimel standard for the scope of a SILA. Although the Chimel standard was satisfied, the Court distinguished a cell phone from other tangible objects based on the quality and quantity of information

181 Riley, 134 S. Ct. at 2489–91.
182 Chimel, 395 U.S. at 768.
184 See Chimel, 395 U.S. at 768.
185 Id.
187 Chimel, 395 U.S. at 763.
188 See Riley, 134 S. Ct. at 2480.
stored. In distinguishing the character of the item searched, the Court ignored prior SILA precedent, which allowed the searches to be conducted regardless of the storage capacities. Akin to a cell phone, an individual’s desk, safe, and file cabinets have an immense storage capacity. The Court failed to recognize the similarities between the cell phone in Riley and the storage containers in Harris and Rabinowitz. In failing to do so, the Court misconstrued the purposes of both Harris and Rabinowitz. Based on the foregoing analysis, the Court improperly distinguished digital information from its tangible counterpart in the context of a SILA.

Future Implications

Cell phones have changed the way society stores information. For instance, individuals increasingly store private information on their cell phones rather than solely within the confines of their homes. However, providing greater protection for digital information may also have an adverse effect on society. For example, individuals may be encouraged to store information on their cell phones instead of carrying tangible documents, eliminating the possibility of exposure to a SILA. Since the information is not subject to a SILA, law enforcement’s ability to effectively combat crime is thereby hindered. Even if Riley does not directly encourage individuals to store data on their phones, it is very likely that cell phones will become society’s main source of storing information. While the holding exemplifies the Court’s emphasis on individual privacy interests, as cell phones and their technological capabilities continue to advance, the Court will need to reevaluate the government’s interest in searches of cell phone data.

If the Court continues to place a high value on individual privacy interests during a SILA, the Court may also need to reevaluate whether tangible documents

---

189 Riley, 134 S. Ct. at 2489–91.
193 See supra notes 181–92 and accompanying text.
197 See id.
198 See id. at 2493. (stating the holding will affect law enforcement’s ability to combat crime and that privacy comes at a cost).
found on an arrestee’s person can be searched without a warrant. In Riley, the Court stressed the importance of the Chimel rationales for a SILA, including officer safety and the preservation of evidence.\textsuperscript{199} However, if an officer seizes tangible documents from an individual during a SILA, the individual no longer has the ability to destroy the evidence or use the document to harm the officer. For example, if an officer seized a diary during a search incident to arrest, the diary can no longer be used as a weapon, nor does the arrestee have the ability to destroy the information contained within the diary. If it wishes to give weight to the rule, the Court should hold that warrantless searches of tangible documents are unjustified.\textsuperscript{200} Moreover, the Court should hold that searches of any information, tangible or digital, are prohibited during a SILA without a warrant, thereby affording equal protection to the same information stored on different mediums.

\textbf{Conclusion}

In Riley v. California, the United States Supreme Court held that the warrantless search of an arrestee’s cell phone was not justified by the SILA exception.\textsuperscript{201} The Court’s reasoning was based on balancing an individual’s right to privacy against the government’s interest in searching digital data contained on an arrestee’s cell phone.\textsuperscript{202} Riley is significant because the holding improperly distinguishes digital information from its pre-digital counterparts.\textsuperscript{203} As Justice Alito stated, “the Court’s broad holding favors information in digital form over information in hard-copy form.”\textsuperscript{204} The majority should have provided the same Fourth Amendment protections to both digital and non-digital content, regardless of the form of information at issue.\textsuperscript{205} Additionally, while the holding of Riley reflects public policy, it will lead to unintended consequences and may require the Court to reevaluate the degree of protection afforded to papers found on an arrestee’s person.\textsuperscript{206} Finally, Chief Justice Roberts stated “[t]he fact that technology now allows an individual to carry such information in his hand, does not make the information any less worthy of the protection for which the Founders fought.”\textsuperscript{207} However, the correct statement according to Riley is: The fact that technology now allows an individual to carry such information in his hand, makes the information more worthy of the protection for which the Founders fought.

\begin{footnotes}
\item[199] See id. at 2485–89.
\item[200] See id. at 2483 (citation omitted).
\item[201] See supra note 94 and accompanying text.
\item[202] See supra notes 95–140 and accompanying text.
\item[203] See supra notes 169–93 and accompanying text.
\item[205] See supra notes 169–93 and accompanying text.
\item[206] See supra notes 194–200 and accompanying text.
\item[207] Riley, 134 S. Ct. at 2495 (emphasis added).
\end{footnotes}