



THE JOURNAL OF
**DIGITAL FORENSICS,
SECURITY AND LAW**

**Journal of Digital Forensics,
Security and Law**

Volume 9 | Number 3

Article 2

2014


The Cost Of Privacy: Riley v. California's Impact on Cell Phone Searches

Jennifer L. Moore
DeSales University

Jonathan Langton
DeSales University

Joseph Pochron
DeSales University

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Recommended Citation

Moore, Jennifer L.; Langton, Jonathan; and Pochron, Joseph (2014) "The Cost Of Privacy: Riley v. California's Impact on Cell Phone Searches," *Journal of Digital Forensics, Security and Law*. Vol. 9 : No. 3 , Article 2.

DOI: <https://doi.org/10.15394/jdfsl.2014.1185>

Available at: <https://commons.erau.edu/jdfsl/vol9/iss3/2>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.



(c)ADFSL





This work is licensed under a Creative Commons Attribution 4.0 International License.

THE COST OF PRIVACY: *RILEY V. CALIFORNIA'S* IMPACT ON CELL PHONE SEARCHES

Jennifer L. Moore, Jonathan Langton, and Joseph Pochron
DeSales University
2755 Station Avenue, Center Valley, Pennsylvania 18034
jennifer.moore@desales.edu

ABSTRACT

Riley v. California is the United States Supreme Court's first attempt to regulate the searches of cell phones by law enforcement. The 2014 unanimous decision requires a warrant for all cell phone searches incident to arrest absent an emergency. This work summarizes the legal precedent and analyzes the limitations and practical implications of the ruling. General guidelines for members of the criminal justice system at all levels consistent with the Supreme Court's decision are provided.

Keywords: search incident to arrest, cell phone searches, U.S. Supreme Court

1. INTRODUCTION

The law notoriously lags behind advancements in technology. The initial explosion of cybercrimes in the 21st century left the American criminal justice system woefully unprepared. The courts struggled to confront the emerging crimes of computer hacking, Internet viruses and sexting with traditional criminal statutes. Forced to work within the confines of criminal laws already on the books, trespass, theft and child pornography statutes were stretched to new limits (Birkhold, 2013). While the federal and state governments eventually updated their laws, the technology gap remains.¹ The slow response time of state and federal legislatures perpetuates a legal system constantly trying

to “catch up” with innovation. In addition, a two hundred year old constitution is also asked to confront modern technological issues that the founding fathers never imagined. The long delay in the appellate process further exasperates the technological gap, as the Supreme Court just addressed the now outdated use of pagers in 2010 (*City of Ontario v. Quon*, 2010).

The search and seizure clause of the Fourth Amendment was recently evaluated in relation to cell phone privacy. Nearly 41 years after the development of the first mobile phone (“The first mobile”, 2013), the Supreme Court in *Riley v. California* issued its first major privacy ruling regarding the devices. In a unanimous decision, the justices emphatically ruled that the search of a suspect's cell phone incident to arrest requires a warrant. Conceding that *Riley* will now make the job of law enforcement more difficult, the Court emphasized the unique attributes of cell phones and the cost of maintaining personal privacy (*Riley v.*

¹ See The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2008); Pennsylvania enacted its sexting statute on October 25, 2012 in 18 PA.C.S. § 6312 (2014).

California, 2014). Local, state and federal law enforcement agencies must now confront the real-world impact of *Riley* in criminal investigations. This article will examine the legal aspects of the Supreme Court's opinion in *Riley* and highlight the limitations of the ruling. In addition, the practical effect of the decision on various parties in the criminal justice system will be evaluated in detail. Finally, a blueprint of acceptable digital forensic techniques after *Riley* will be explained.

2. THE SUPREME COURT'S UNANIMOUS VERDICT

The Supreme Court consolidated the cases of David Leon Riley and Brima Wurie in a groundbreaking case regarding the evolution of privacy in the digital age. In separate incidents, both men had their cell phones searched incident to arrest without a warrant. The information contained on their cell phones ultimately led to convictions for additional offenses. Riley was initially stopped in California for a traffic violation but eventually arrested after an inventory search revealed two loaded handguns under the hood of his car. During the search incident to arrest, Riley's cell phone was removed from the pocket of his pants and searched preliminarily by the police officer on scene. A review of texts messages and contacts indicated membership in the Bloods street gang. Two hours after the arrest, a detective further analyzed Riley's cell phone without a warrant at the police station. The detective discovered photographs of Riley standing near a car allegedly used in a drive by shooting. Riley was ultimately convicted for attempted murder, assault with a semiautomatic firearm, and firing at an occupied vehicle and sentenced to 15 years to life in prison for his involvement in the drive by shooting (*Riley v. California*, 2014, p. 2481).

Brima Wurie was arrested after purchasing drugs and two cell phones were seized from his person incident to arrest. At the police station, Burie's phone continued to receive calls from a contact noted as "my house." An officer opened the flip phone and accessed the call log to retrieve the incoming telephone number. A trace of the number was completed to obtain a physical address. After securing a search warrant, the police searched Burie's home and seized weapons, cash and large amounts of crack cocaine. Burie's convictions resulted in a sentence of 262 months in federal prison (*Riley v. California*, 2014, p. 2482). On appeal, both cases raised the question of whether a warrant is needed to search a cell phone incident to arrest.

Chief Justice Robert's opinion addressed the question presented within the framework provided by the leading search incident to arrest case, *Chimel v. California*. In 1969, *Chimel* declared that police officers could perform a warrantless search of a suspect and the area within the suspect's immediate control incident to an arrest. This exception to the warrant requirement was justified by the potential threat to officer safety and the possibility for the destruction of valuable evidence (*Chimel v. California*, 1969). The *Chimel* doctrine was extended to include a quick search of personal property "immediately associated with the person of the arrestee" (*U.S. v. Chadwick*, 1977, p. 15). In searching for relevant precedent applicable to the factual scenarios before the Court, Chief Justice Roberts focused on the 1973 decision of *United States v. Robinson*. The holding in *Robinson* permitted police officers to search a crumpled cigarette packet located in a suspect's coat pocket incident to arrest. A review of the contents of the cigarette packet revealed illegal drugs. The Supreme Court in *Riley* had to determine if a cell phone was analogous to that crumpled cigarette package or an entirely different category of property. Similar to most Fourth Amendment cases, the answer hinged on the balancing of government interests and individual privacy.

The unanimous decision spent a significant amount of time examining the unique characteristics of a cell phone. When compared to other physical objects, the Court emphasized the vast quantitative and qualitative differences of the modern phone. The immense storage capacity and variety of data contained on cell phones was emphasized, which Chief Justice Roberts noted could just “as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps or newspapers” (*Riley v. California*, 2014, p. 2489). Accordingly, a warrantless search of a cell phone implicates a substantially greater violation of privacy than reviewing the contents of a wallet or cigarette packet. The Court noted that 90 percent of adults in America essentially have “on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate” (*Riley v. California*, p. 2490). A detailed examination of a cell phone is analogous to an exhaustive search of an entire home.² Accordingly, cell phones were distinguished from other types of personal property and the precedent from *Robinson* was inapplicable.

The decision also reviewed each of the *Chimel* rationale as they applied to cell phones—officer safety and the imminent destruction of evidence. The Supreme Court quickly dismissed the concern for officer safety, noting that “[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee’s escape” (*Riley v. California*, 2014, p. 2485). While police officers remain free to examine the physical aspects of a cell phone for concealed risks, such as razor blades, the content of the phone remains protected. The Court also clarified that the

potential for “indirect” threats from third parties does not justify an automatic warrantless search of cell phone data incident to arrest. While data on a phone can potentially reveal to law enforcement that additional accomplices are en route to the scene, they are not covered by the rationale of *Chimel* and its progeny. *Chimel* applies only to threats from the arrestee, not third parties. In factually specific situations where a unique safety threat exists, the exigent circumstances exception remains available for law enforcement (*Riley v. California*, p. 2487).

In regards to the destruction of evidence rationale from *Chimel*, the Court focused on the potential for remote wiping or encryption of digital data. The federal government and the State of California argued that imminent threats to cell phone contents justified a warrantless search incident to arrest exception. Specifically, the contents of a phone can be completely erased if it remains connected to a wireless network and a third party sends the appropriate signal. In addition, after a phone locks the information stored can be encrypted with a special program to completely prevent access without the applicable encryption key. The Supreme Court quickly dismissed both ideas as justification for an automatic warrantless search, noting that little evidence was provided that these problems even exist in the field. The Court also reiterated that *Chimel* applies only to direct threats from the arrestee, and not to third parties wiping content or the normal functions of an encryption security feature. Police officers remain free to employ alternative methods to protect digital data at the scene of an arrest short of a search, such as removing the battery, turning the phone off or disabling an automatic-lock feature (*Riley v. California*, 2014).

The unanimous Court concluded by acknowledging the impact of their decision, noting “[w]e cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime” (*Riley v.*

² Chief Justice Roberts explained that, “a cell phone search would typically expose to the government to far more than the most exhaustive search of a house” (*Riley v. California*, 2014, p. 2491).

California, 2014, p. 2493). The decision in *Riley*, however, does not completely isolate a cell phone from a comprehensive search. It simply requires a warrant or an independent exception to the warrant requirement to justify the excessive privacy intrusion.

2.1 Justice Samuel Alito's Concurrence

While the Supreme Court was unanimous in requiring a warrant for cell phone searches incident to arrest, Justice Alito issued a concurrence to explain his legal reasoning. Specifically, the concurrence addressed the underlying *Chimel* rationale cited by the Court for conducting a search incident to arrest – officer safety and preventing the destruction of evidence. Alito argues that the practice of searching a suspect after an arrest has a strong historical foundation independent of the *Chimel* factors. Citing numerous historical examples of searches incident to arrest as routine practice for police officers, Alito concludes that “the rule is not closely linked to the need for officer safety and evidence preservation” (*Riley v. California*, 2014, p. 2496). In addition, Alito cites numerous court decisions that permitted officers to read written items found on suspects incident to arrest as evidence that safety and evidence destruction are not the only controlling factors. The concurrence clarifies that *Chimel* involved searching the scene of an arrest, not the search of a person. Accordingly, Alito would not “allow that reasoning to affect cases like these that concern the search of the person of the arrestees” (*Riley v. California*, p. 2496).

Alito also emphasizes the limits of the *Riley* decision and the need for state and federal legislatures to pass laws regarding digital evidence. Citing the passage of the Omnibus Crime Control Act after *Katz v. United States* restricted the warrantless monitoring of public pay phones, the concurrence emphasized the “better position” of legislatures to address changing technology. As written, Alito concedes that *Riley* gives

greater protection to digital evidence than physical evidence. An address on a slip of paper is searchable incident to arrest, but an address contained in a cell phone’s contacts list is not. Additionally, photographs in a wallet can be viewed by police officers, while those on a phone are protected. Alito concludes “it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment” (*Riley v. California*, 2014, p. 2497).

3. LIMITATIONS ON THE RULING

A single Supreme Court decision is never the “last word” on a specific legal issue. The opinion will inevitably be dissected by the lower courts, distinguished by different factual circumstances and interpreted differently. The *Riley* decision provides several notable limitations that can potentially impact police officers’ enforcement of the ruling. For example, the Roberts Court traditionally issues very limited decisions that apply specifically to the factual situations presented. *Riley* is no exception. Both consolidated cases resolved in *Riley* involved searches of cell phones incident to arrest. Consequently, the Court’s ruling appears to apply only in situations where the suspect is arrested. This leaves open the possibility for warrantless cell phone searches in other circumstances independent of arrest. For example, police may encounter a cell phone while performing a warrantless search under the automobile exception. Although the Supreme Court distinguished cell phones from other physical property, it did not completely eliminate the possibility that a brief content search might be appropriate in the automobile context due to the mobility of vehicles. In addition, the plain view exception could also arise and justify a cell phone search. If a police officer is lawfully in an apartment and sees a text message implicating criminal activity flash on the screen, they could be justified in searching

the phone. As long as the scenario does not involve a search incident to arrest, *Riley* is not completely controlling.

The opinion itself contains a limiting instruction to remind the audience that *Riley* is limited solely to search incident to arrest cases. In footnote 1, the Court notes that since both parties “agree that these cases involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances” (*Riley v. California*, 2014, p. 2489). Therefore, the collection of digital information by law enforcement using other means beyond cell phone examination incident to arrest remains an open legal issue.

Riley also fails to provide adequate guidance for limiting the scope of search warrants on cell phones. Mobile devices are currently searched and examined by practitioners with nuanced tools that contain forms of automated data extraction and parsing. While *Riley* calls for the acquisition of a search warrant, the Supreme Court did not specify which techniques could be used on mobile device. This issue has already surfaced in the lower courts. The U.S. District Court for the Central District of Illinois recently ruled in *U.S. v. Schlingloff* (2012) that a computer forensic practitioner may not utilize automated data filters to locate evidence that is extraneous to the basis of the probable cause articulated in the search warrant. In *Schlingloff*, a computer forensic practitioner utilized an automated filter within a forensic tool to search for files containing child pornography, resulting in the location of child pornography on the suspect’s computer. The warrant was explicitly based on probable cause pertaining to an identity theft investigation, and although the child pornography filter utilized to search the computer is commonly set as a default methodology within the forensic tool, the practitioner did have the ability to conduct an examination of the device without using the filter. Because the practitioner did not choose

to deactivate the child pornography filter, the District Court ruled that the utilization of the filter reached beyond the scope of the search, resulting in the suppression of the digital evidence. Although methodologies certainly differ between mobile device forensics and computer forensics, Chief Justice Roberts’ opinion in *Riley* draws clear analogies between modern cell phone technology and the capabilities that are typically associated with computers. Because of this commonality, *Schlingloff* may represent a glimpse into the future of legal issues concerning the examination of cell phones and the associated requirements for warrants and methodologies.

Although *Riley* largely neglected to delve into the intricacies of the scope of search warrants for digital devices, the Court acknowledged the complexities associated with the data capabilities of mobile devices. Just as Apple mobile devices support data storage through the iCloud service, modern cell phones consistently use data remotely stored on third-party servers. The Court explicitly referenced modern cell phones’ utilization of cloud computing, noting that “a cell phone is used to access data located elsewhere, at the tap of the screen” (*Riley v. California*, 2014, p. 2491). Although the majority opinion appears to recognize a necessity for Fourth Amendment protection of data stored through cloud-based technology, the Court hesitates to clearly delineate the important distinction between locally and remotely stored data. More importantly, *Riley* also fails to recognize the significance of such a distinction, stating that “cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference” (*Riley v. California*, p. 2491). While modern cell phone capabilities allow for the storage of data in a multitude of locations on the individual device and through cloud-based services, *Riley* fails to establish a framework for the legal and forensic interpretation of these differences. The Court’s opinion suggests that this distinction is irrelevant for the purpose of searching a device incident to arrest, and effectively paves

the way for further discussion and debate regarding the scope of warrants for the search of digital evidence.

Arguably, the *Riley* decision can also be read as applying only to cell phones as opposed to all types of electronic devices. While the type of information stored on a cell phone is analogous to that found on iPads or iPods, the justices did not directly make the comparison. As additional technological devices continue to emerge, such as Google glasses or the highly anticipated iWatch, courts will be forced to determine if they are similar enough to cell phones to apply *Riley*. An armband used by athletes to map their latest run or bike ride could provide indispensable GPS data. Since these devices lack the photographs, contacts, calendars and other personal information found on cell phones, they are potentially distinguishable from the *Riley* decision based on the level of privacy intrusion. The ultimate determination of what types of devices fall under *Riley's* control will fall on the lower courts.

The Supreme Court also expressly noted that the exigency exception to the warrant requirement is still applicable in appropriate factual circumstances to justify a search of cell phone data. Similar to other areas of Fourth Amendment jurisprudence, the warrant requirement is eliminated in situations where the safety of the police or public is in immediate danger or evidence is imminently being destroyed. The *Riley* opinion provides two factual examples in which a cell phone search may be justified due to exigent circumstances. First, law enforcement would be entitled to search the contents of a phone if the suspect is apparently texting an accomplice to detonate an explosive device. Second, the Court would seemingly allow the warrantless search of a phone believed to contain the location of a kidnapped child (*Riley v. California*, 2014, p. 2494). These examples simply highlight the potential for countless unique factual scenarios that justify cell phone searches

incident to arrest. As the lower courts begin to interpret and apply *Riley*, this exception possesses the greatest potential for expansion and abuse. At this time, however, the justices explicitly held that threats of remote wiping and/or data encryption do not constitute exigent circumstance.

4. PRACTICAL IMPACT OF *RILEY* ON LAW ENFORCEMENT

Riley appears to unequivocally require a warrant for any cell phone seized during an arrest that lacks exigent circumstances. In order to ascertain the practical impact of *Riley* on the law enforcement community, a few points must be clarified. First, the term “search” used in relation to a cell phone can actually describe a multitude of approaches utilized by law enforcement personnel with varying levels of digital forensics knowledge. In some jurisdictions, cell phone searches are limited to a simple scroll analysis (Ayers, Brothers, and Jansen, 2013, p. 16). A scroll analysis of a mobile device involves the manual manipulation of a cell phone, through which a law enforcement officer will “scroll” through a phone while photographing or similarly documenting the phone’s screen as it displays the relevant information. Scroll analyses, although recognized as an accepted practice in the digital forensics community, represent a cursory and rudimentary form of mobile device forensic analysis, requiring negligible training or experience on the part of the individual examining the device (Ayers, et al., p. 18).

Other jurisdictions utilize more advanced digital forensic tools designed specifically for the acquisition, extraction, decoding, and reporting of data residing within a mobile device (Ayers, Brothers, and Jansen, 2013, p. 17). These innovative tools require specialized training and certification, as well as acceptable forensic laboratories for proper utilization. The environmental requirement

remains a focal point of concern for law enforcement personnel. Digital forensics laboratories formerly focused almost exclusively on traditional computer analysis. These laboratories adapted in response to the exponential growth in the prevalence of mobile device use and the evolution of the technological capabilities of these mobile devices. As the prevalence and capabilities of cell phones have grown and developed, the law enforcement community has reacted by training personnel on mobile forensic tools and methodologies, as well as utilizing or establishing laboratory environments for the analysis of the devices (Malone, 2011).

Due to the differences in jurisdictional capabilities and practices, the practical implications of *Riley* on the law enforcement community are diverse and versatile. The opinion doesn't simply impose restrictions or regulations on a singular "police" presence, but on a number of law enforcement personnel working in different capacities. For the sake of brevity, the law enforcement personnel impacted by the *Riley* decision can be categorized into the following four groups: first responders, criminal investigators, prosecutors and forensic practitioners.

First responders and criminal investigators are the categorical groups of law enforcement personnel that will arguably be the most heavily impacted by *Riley*. As seen through the facts of both consolidated cases under the umbrella of *Riley*, police officers who are in the process of arresting an individual and conducting administrative or investigative searches of the arrestee's person or immediate surroundings will commonly locate a cell phone. The language of the *Riley* opinion very clearly establishes the necessity to procure a search warrant after the seizure of a cell phone incident to arrest. While Chief Justice Roberts identified exigency exceptions in the unanimous opinion, his emphasis on the acquisition of a search warrant before conducting an investigative search of a cell phone's contents has a sizeable impact on the actions of first responders and criminal

investigators immediately after an administrative seizure.

Previously, a police officer may have conducted a cursory scroll analysis of the phone in order to verify written or verbal statements made by the arrested party, to expedite traditional investigatory tactics, or to document information before a device or its contents can be remotely wiped, protected by password, or otherwise modified (Murphy, 2009, p. 2). Exigency exceptions aside, *Riley* very clearly disallows some of the aforementioned tactics that have been utilized by first responders and criminal investigators in order to expediently search the content of a cell phone. Rather than reacting intuitively or reflexively as investigators seeking actionable information, law enforcement personnel conducting searches incident to arrest must accept the challenge presented by *Riley* of protecting and preserving digital evidence.

Additionally, prosecutors will be impacted by the *Riley* opinion. While many prosecutors are currently procuring search warrants for digital evidence, they will undoubtedly be pressured to achieve a higher degree of awareness regarding mobile devices that require authority for search or forensic examination. The Department of Justice currently serves as an example of the reaction to *Riley* on the part of prosecutors, as it has publicly announced that it will strive to operate within the bounds of the unanimous opinion while seeking to clarify and utilize exigency exceptions (Myers, 2014). Prosecutors will need to provide guidance in order to ensure that first responders and criminal investigators are dealing with digital evidence from cell phones in a manner that is consistent with the *Riley* decision. More importantly, *Riley* represents the Supreme Court's first foray into the realm of mobile device forensics. As the rampant utilization of cell phones continues to permeate the lives of American citizens, the Court will inevitably need to make similarly impactful decisions in the future regarding warrant scope considerations and plain view technicalities as

they relate to the forensic analyses of cell phones. As these legal discussions evolve, prosecutors will face the unenviable task of representing the Government's interests, educating first responders, and learning the methodological nuances of mobile device forensics from competent practitioners.

Although the on-site methods utilized by first responders to expediently search the contents of a cell phone appear to have been largely invalidated by *Riley*, Chief Justice Robert's language seems less indicative of a dramatic change in policy for the part of the fourth categorical group of law enforcement personnel, the certified forensic practitioners. The vast majority of mobile device forensic practitioners currently require legal authority to examine a cell phone through a search warrant or written consent due to industry standards and individual agency operating procedures (U.S. Department of Justice, 2004, p. 7). While the language of *Riley* does little to hamper the current practices of mobile device forensic examiners, it may have a counterintuitive and decidedly positive impact on the discipline of mobile device forensics as whole. Rather than placing an emphasis on the ambiguously dangerous "cost" that privacy in the digital age may have, the *Riley* decision clearly communicates the nuances and protocols associated with mobile device forensics for the law enforcement community.

In order to do so, Chief Justice Roberts relied on the National Institute of Standards and Technology (NIST) Guidelines on Mobile Device Forensics (*Riley v. California*, 2014, p. 2486). Roberts used these guidelines to emphasize and respond to the government's arguments about remote data wiping, encryption, and similar concerns about the volatility of data residing on mobile devices. By utilizing industry standards and appropriate literature, the Supreme Court outlined a blueprint for acceptable law enforcement techniques utilized to secure and examine a cell phone.

5. THE BLUEPRINT: ACCEPTABLE TECHNIQUES FOR LAW ENFORCEMENT AFTER RILEY

First, the physical aspects of a phone may be inspected to determine if it could be used as a weapon. Although fairly straightforward and simplistic, the Supreme Court's allowance of a physical inspection of a cell phone serves to protect the law enforcement official, typically a responding officer or investigator, from immediate and obvious danger. Although Chief Justice Roberts' opinion clearly demonstrates the Court's prioritization of personal privacy over the government's concerns about the protection of digital evidence, the opinion also relays several acceptable practices for law enforcement to protect volatile digital evidence on mobile devices. Aside from a physical inspection of the device, the second allowable practice suggests that police officers concerned with the threat of remote wiping can remove a phone's battery or turn the phone off (*Riley v. California*, 2014, p. 2487). Although the removal of a cell phone's power source will ultimately prevent a phone from being remotely wiped through a command using wireless connectivity or cellular network services, the practice can create different problems for mobile device practitioners. Removing a cell phone's battery or effectively turning the phone off may activate authentication codes such as PIN's, passwords, or complex security codes unique to the device. While following this practice will maintain the integrity of the digital evidence, it may also compromise access to the device, effectively delaying or invalidating the search of the cell phone.

Additionally, law enforcement personnel can leave a seized cell phone turned on and place the phone in a Faraday bag to block radio waves (*Riley v. California*, 2014, p.

2487). Faraday bags are capable of blocking radio frequency (“RF”) waves from reaching the mobile device and denying wireless connectivity, preventing the remote wipe or encryption of a cell phone’s data. Although largely effective, the utilization of Faraday bags entails a certain level of risk. Faraday containers are not without limitations, as they do allow for the minute possibility that a contained cell phone could connect to a cell tower in the immediate area. Additionally, Faraday bags and similar vessels can be unsuccessfully sealed by a first responder, while cables connecting a contained phone to a forensic workstation may act as antennas, ultimately allowing access to cellular networks. Unfortunately, even the successful utilization of a Faraday bag has negative ramifications. Once a Faraday container isolates a cell phone from radio frequency, the device’s battery life will be significantly shortened as the cell phone raises its power consumption levels in an attempt to connect to a network that is being blocked by the Faraday bag. Finally, certain mobile device manufacturers and cellular service providers design and implement protocols that cause cell phones to reset or clear data if isolated from the network for an extended period of time (Ayers, Brothers, and Jansen, 2013, p. 30).

The final options presented by the Supreme Court allow first responders to disable the automatic-lock feature on a phone to prevent data encryption and protection through passcodes, or to put the device in airplane mode to disallow cellular and wireless network connectivity (Ayers, Brothers, and Jansen, 2013, p. 15). Although both of these methods have the potential to preserve the integrity of the digital evidence, they present a shared concern for law enforcement personnel. Disabling automatic-lock features and enabling airplane mode both require the direct manipulation of the device, as the first responder directly interacts with the cell phone. These methods technically necessitate a directly intrusive altering of the device’s data, resulting in a digital footprint, which

could prove problematic if the first responder is unfamiliar with the cell phone or the methodologies being used. The law enforcement community can mitigate these concerns by providing base levels of training, as well as ensuring that first responders who are tasked with disabling an automatic-lock feature or enabling airplane mode understand that they must document the actions taken in order to preserve the integrity of the evidence. While none of the techniques provided by the Supreme Court represent airtight solutions to the Government’s concerns regarding data vulnerability, they should succeed in establishing a crucial foundation for awareness throughout the law enforcement community regarding the quality and nature of evidentiary data within cell phones.

6. THE SUPREME COURT AND TECHNOLOGY

The Supreme Court in *Riley* acknowledged the prevalence of modern cell phones in American society, noting, “the proverbial visitor from Mars might conclude they were an important feature of human anatomy” (*Riley v. California*, 2014, p. 2484). Yet, the justices themselves seem to lack this familiarity with cell phones and other technology. The average age of the nine justices sitting on the Supreme Court today is 68 years old. As law and technology continue to intertwine, the lack of technical awareness of the Supreme Court justices is increasingly apparent. Justice Elena Kagan, the Supreme Court’s youngest justice at age 54, even identified the issue of age and technology. In regards to cell phones, she stated, “[t]hey’re computers. They have as much computing capacity as laptops did five years ago. And everybody under a certain age, let’s say under 40, has everything on them” (Serwer, 2014). The justices do not even use email to communicate with one another (Smith,

2013).³ They received substantial criticism for their comments during the oral arguments for *American Broadcasting Cos. v. Aereo, Inc.* (2014), a recent case regarding the retransmission for cable television over the Internet. Several justices were unable to understand how the technology at issue actually worked, with Justice Sonia Sotomayor admitting, “this is really hard for me” (*American Broadcasting Cos. v. Aereo, Inc.*, oral arguments, 2014; Rubin, 2014). Justice Stephen Breyer was similarly befuddled, proclaiming to counsel during oral argument that “what disturbs me on the other side is I don’t understand what the decision for you and against you when I write it is going to do to all kinds of other technologies. I’ve read the briefs fairly carefully, and I’m still uncertain that I understand it” (*American Broadcasting Cos. v. Aereo, Inc.*, oral arguments, 2014; Rubin, 2014). The technological confusion was also apparent in a 2010 case regarding the use of pagers by employees. In *City of Ontario v. Quon*, Justice Anthony Kennedy displayed his misunderstanding of texting. During oral argument, he inquired about what would happen if an individual both sends and receives a text message at the same time, “Does it say: ‘Your call is important to us, and we will get back to you’” (*City of Ontario v. Quon*, oral argument, 2010)? In the same case, Chief Justice Roberts had to ask counsel to explain the difference between a pager and e-mail.⁴

The justices not only need to understand how technology works, but also how the average American utilizes technology in their daily lives. During the oral argument for *Riley*, Chief Justice Roberts was surprised to

hear that individuals sometimes carry more than one cell phone. He specifically asked defense lawyer Judith Mizner in relation to Brima Wurie, “[w]hy would he have two cell phones?” When Ms. Mizner replied that it was a common occurrence, Chief Justice Roberts replied, “[w]hat is your authority for the statement that many people have multiple cell phones on their person” (*Riley v. California*, oral argument, 2014; Hurley, 2014)? The exchange during oral argument seemed to suggest that Roberts believed only a drug dealer involved in illegal activity would possess two cell phones. While the confusion did not appear to impact the ultimate decision in *Riley*, it raises concerns about future cases with continually advancing technology.

The degree to which Supreme Court justices truly need to understand technology before they issue a legal ruling is debatable. The Court continually confronts factually complex issues on a variety of subject. Patent cases, for example, are notoriously intricate and can involve any number of scientific or engineering disciplines. A justice does not need to be an expert in every field that is brought before the Supreme Court. However, they should seek outside assistance when addressing an advancing field to avoid the appearance of looking foolish and out-of-date. Perhaps the greatest threat to the Supreme Court in technologically related cases is the complete loss of public confidence. A controversial verdict is undoubtedly questioned when the leading Court in the country doesn’t know the correct name for the widely popular Netflix or that HBO is not a free television channel (Logiurato, 2014).⁵

While their understanding of technology is relatively limited, the justices appear to appreciate the impact digital devices potentially have on a citizen’s expectation of privacy. In 2012, the Supreme Court

³ Justice Elena Kagan announced that the justices do not use email as a means of communication during a speech at Brown University in August 2013.

⁴ Chief Justice Roberts asked, “Maybe -- maybe everybody else knows this, but what is the difference between the pager and the e-mail?”

⁵ Justice Sotomayor referred to Netflix as “Netflick” in the *Aereo* oral argument.

addressed the issue of monitoring a suspect through the use of modern global positioning systems or GPS. In *United States v. Jones*, a physical monitor was placed on a suspect's automobile without a valid warrant and his position was tracked for four weeks. The majority concluded that a search occurred due in part to the physical intrusion on Jones' automobile. GPS monitoring today, however, does not always require the attachment of a physical object, but can be accomplished remotely through a suspect's cell phone or other electronic device. In her concurrence, Justice Sotomayor recognized the challenges advancing technology poses to privacy interest protected by the Fourth Amendment. She specifically noted that "[a]wareness that the Government may be watching chills associational and expressive freedoms" (*U.S. v. Jones*, 2012, p. 956). Justice Sotomayor also suggests that the new digital age might require a reconsideration of the expectation of privacy for information voluntarily disclosed. Citizens typically disclose large amounts of personal information in order to complete routine tasks on their electronic devices, such as purchasing items online. In modern times, Justice Sotomayor explains that "secrecy" is not always a "prerequisite for privacy" (*U.S. v. Jones*, p. 957). Consequently, the entire foundation of the expectation of privacy in digital information is potentially up for reconsideration in future cases before the Supreme Court.

7. CONCLUSION

A Supreme Court decision's full impact cannot be measured until the lower courts begin to interpret and apply the ruling. For example, a broad reading of *Riley v. California* may result in the imposition of a warrant requirement in situations beyond searches incident to arrest. Alternatively, the courts may view the exigency exception as a broad loophole for law enforcement to review preliminary cell phone data that is connected to an ongoing crime or the imminent destruction of evidence. *Riley*, however, is

not the last word on searching digital information on cell phones and other devices. The justices left many areas open for interpretation and future Supreme Court decisions. Specifically, *Riley's* application to other electronic devices remains uncertain. Similarly, *Riley* deliberately fails to address cell phone searches in the context of other warrantless searches such as plain view or the automobile exception. For now, law enforcement must work within the confines of *Riley* and obtain warrants in most search incident to arrest situations. The small blueprint of acceptable techniques provided by the Supreme Court should be carefully followed as the legal wrangling continues. While seemingly straightforward, the *Riley* decision has provided the platform from which contentious debate will undoubtedly rise, as the intersection of technology and criminal procedure continues to impact the law enforcement community.

REFERENCES

- 18 PA.C.S. § 6312 (2014).
- 18 U.S.C. § 1030 (2008).
- American Broadcasting Cos. v. Aereo, Inc.*, 134 S.Ct. 2498 (2014).
- American Broadcasting Cos. v. Aereo, Inc.*, Oral Arguments, 134 S.Ct. 2498 (2014).
- Ayers, R., Brothers, S., & Jansen, W. (2013). Guidelines on mobile device forensics (draft). National Institute of Standards and Technology, Special Publication 800-101. Retrieved from <http://www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf>.
- Birkhold, M.H. (2013) Freud on the court: Re-interpreting sexting & child pornography laws. 23 *Fordham Intell. Prop. Media & Ent. L.J.* 897.
- Chimel v. California*, 395 U.S. 752 (1969).
- City of Ontario v. Quon*, 130 S.Ct. 2619 (2010).

- City of Ontario v. Quon, Oral Argument, 130 S.Ct. 2619 (2010).
- Hurley, L. (2014, May 9). In U.S., when high-tech meets high court, high jinks ensue. Reuters. Retrieved from <http://www.reuters.com/article/2014/05/09/us-usa-court-techidUSBREA480N420140509>.
- Logiurato, B. (2013, April 22). Justice Scalia did not know you can't get HBO for free. Business Insider. Retrieved from <http://www.businessinsider.com/scalia-hbo-aereo-case-supreme-court-2014-4>.
- Malone, JD. (2011, March 24). Digital forensics lab to aid lehigh county police in fight against crime. The Express-Times. Retrieved from http://www.lehighvalleylive.com/allentown/index.ssf/2011/03/digital_forensics_lab_to_aid_l.html.
- Murphy, C. A. (2009). Developing process for mobile device forensics. Retrieved from <http://www.mobileforensicscentral.com/mfc/documents/Mobile%20Device%20Forensic%20Process%20v3.0.pdf>.
- Myers, B. (2014, June 25). Supreme court: Police need warrant to search cell phones. CNN Justice. Retrieved from <http://www.cnn.com/2014/06/25/justice/supreme-court-cell-phones/>.
- Riley v. California, 134 S.Ct. 2473 (2014).
- Riley v. California, Oral Argument, 134 S.Ct. 2473 (2014).
- Rubin, J. (2014, April 23). Supreme court justices have their heads in the cloud(s). The Washington Post. Retrieved from <http://www.washingtonpost.com/blogs/right-turn/wp/2014/04/23/supreme-court-justices-have-their-heads-in-the-clouds/>.
- Serwer, A. (2014, April 29). Justices split on cops' right to search cell phones. MSNBC. Retrieved from <http://www.msnbc.com/msnbc/cops-may-soon-be-free-search-your-iphone>.
- Smith, M.R. (2013, August 20). Kagan: Court hasn't really 'gotten to' email. Associated Press. Retrieved from <http://bigstory.ap.org/article/kagan-justices-not-tech-savvy-send-paper-memos>.
- The first mobile phone call was placed 40 years ago today. (2013, April 3). FoxNews. Retrieved from <http://www.foxnews.com/tech/2013/04/03/first-mobile-phone-call-was-placed-40-years-ago-today/>.
- United States Department of Justice. (2004). Forensic examination of digital evidence: A guide for law enforcement (Publication Number NCJ 199408). Washington, DC. Retrieved from <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>.
- U.S. v. Chadwick, 433 U.S. 1, 15 (1977).
- U.S. v. Jones, 132 S.Ct. 945 (2012).
- U.S. v. Schlingloff, 901 F.Supp.2d 1101 (C.D. Ill. 2012).