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delay in the appellate process further exasperates the technological gap, as the Supreme Court just addressed the now outdated use of pagers in 2010 (*City of Ontario v. Quon*, 2010).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 is 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.

