Search a Cell Phone Incident to Lawful Arrest? Get a Warrant!

In its decision issued just yesterday, the United States Supreme Court delivered the ruling that, barring any exigent circumstances, officers must obtain a warrant to search a cell phone seized in a search incident to a lawful arrest. For the past year or two, we have been very vocal in law enforcement training when addressing the issue of searching cell phones incident to arrest, and have cautioned and instructed officers to apply for a search warrant prior to conducting the search. Our concern has mirrored that expressed through the holding in this Supreme Court case, that considering a cell phone's functionality, the information it contains, and its intrinsic link to an individual's personal life, there exists a high expectation of privacy in the device. In addition, as the Court expressed, there is great concern that giving officers the ability to "rummage" through a cell phone, and the vast amount of information contained therein, will invade the privacy rights of the owner.

The Supreme Court consolidated two cases, *Riley v. California*[1] and *United States v. Wurie*[2] as they raised a common question: "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."

Factual Background

In the first case, a police officer stopped David Riley for driving with expired vehicle registration tags, and discovered that Riley's license had been suspended. The officer impounded Riley's car and, pursuant to department policy, conducted an inventory search, which revealed two handguns under the car's hood. Riley was arrested for possession of concealed and loaded firearms. While conducting a search of Riley incident to the arrest, the officer found items associated with the "Bloods" street gang and seized a cell phone located in Riley's pants pocket. Riley's cell phone was a "smart phone" model with a broad range of functions, large storage capacity, and Internet connectivity. When the officer accessed information on the cell phone, he noted that some words were preceded by the letters "CK," which he believed to stand for "Crip Killers" – a slang term for members of the Bloods gang. Two hours following the arrest, a detective specializing in gangs further examined the contents of the cell phone to search for evidence of gang activity. The detective discovered a video with young men fighting while someone yelled "Blood," and also found photographs of Riley standing in front of a vehicle suspected to have been involved in a shooting a few weeks prior.

Riley was ultimately charged, in connection with the earlier shooting, with firing at an occupied vehicle, assault with a firearm, and attempted murder. The State alleged that Riley committed these crimes to benefit his gang. Such activity is considered an aggravating factor and carries an enhanced sentence. At trial, Riley filed a motion to suppress the evidence obtained from the search of his cell phone on the basis that it violated his Fourth Amendment rights against unreasonable search and seizures because the police conducted a warrantless search that was not otherwise justified by exigent circumstances. The trial court rejected this argument and, at trial, police officers testified about the information found on the cell phone, and some of the photographs from the cell were admitted into evidence. The California Court of Appeals affirmed. The U.S. Supreme Court granted certiorari.

In the second case, police officers arrested Brima Wurie for making an apparent drug sale from his vehicle while under surveillance. At the police station, officers seized two cell phones from Wurie's person. One of the cell phones was a "flip phone," which generally has fewer features than a "smart phone." Five or ten minutes after Wurie arrived at the police station, officers noted that the phone was repeatedly receiving calls from a number identified on the screen as "my house." Officers then opened the phone and saw that the wallpaper picture was a woman holding a baby. Officers

pressed one button on the phone to access the call log to determine the actual number associated with "my house." The number was traced to an apartment building utilizing an online phone directory. When officers arrived at the apartment building, they noted Wurie's name on a mailbox and observed through a window the woman shown in the cell phone's wallpaper. Officers secured the apartment while they obtained a search warrant. Upon execution of the warrant, officers located drugs, firearms, ammunition, and cash.

Wurie was charged with various drug charges and being a felon in possession of a firearm and ammunition. Wurie moved to suppress the evidence obtained from the apartment, claiming that it was the fruit of an unconstitutional search of his cell phone. The district court denied Wurie's motion to suppress and he was convicted. The First Circuit Court of Appeals reversed the denial of the motion to suppress and vacated the conviction. The U.S. Supreme Court granted certiorari.

Supreme Court Analysis

The United States Supreme Court began its analysis of this issue with a review of the Fourth Amendment right against unreasonable search and seizure. The Court stated that the "ultimate touchstone of the Fourth Amendment is 'reasonableness' . . . and reasonableness generally requires the obtaining of a judicial warrant." In the absence of a search warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement. The Court noted that in the present two cases, the issue is the reasonableness of a warrantless search of the cell phones incident to a lawful arrest. The Court stated that "it has been well accepted that such a search constitutes an exception to the warrant requirement." The debate over these searches, however, focuses on the extent to which officers may search property found on or near the arrestee.

The Supreme Court discussed three related precedents that set forth the rules governing search of this nature. In *Chimel v. California*,[3] police officers arrested Chimel in his home and proceeded to search his entire three-bedroom home, including the attic and garage. Officers also search through drawers in some of the rooms as well. The resulting rule from the *Chimel* case to assess the reasonableness of a search incident arrest is that officers may search the person arrested to remove any weapons that may endanger the safety of officers or to effect an escape. Officers may also search for and seize any evidence on the arrestee's person to prevent its concealment or destruction. The *Chimel* court held that "there is ample justification, therefore, for a search of the arrestee's person and the area 'within his immediate control' – construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence."

In *United States v. Robinson*,[4] the court concluded that a "custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification." The court concluded that officer's search of the cigarette package was reasonable even though there was no concern about loss of evidence or that Robinson might be armed.

In *Arizona v. Gant*,[5] the Court analyzed the search of an arrestee's vehicle, concluding that officers are authorized to search a vehicle "on when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search." The *Gant* Court added, however, an independent exception for a warrantless search of a passenger compartment "when it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle."

The Court discussed, however, that while *Robinson* concluded that the risks presented in *Chimel* – harm to officers and destruction of evidence – were present in all custodial arrests, these risks are not necessarily present when the search is of digital data. The Court further discussed that cell phones "place vast quantities of personal information literally in the hands of individuals. A search of information on a cell phone bears little resemblance to the type of brief physical

search considered in *Robinson.* The Supreme Court declined to extend *Robinson* searches to include the search of data on cell phones, and held that "officers must generally secure a warrant before conducting such a search."

In reaching its conclusion, the court considered the concerns raised in *Chimel.* The Court noted that digital data stored on a cell phone cannot be used as a weapon against officers, and cannot be used to assist in an escape. The Court stated, however, that officers are free to examine the physical aspects of a cell phone to ensure that it will not be used as a weapon – e.g. the placement of a razor blade between the phone and the case.

The Court also examined the issue regarding the potential for destruction of evidence. The Court noted that both Riley and Wurie conceded that officers could have seized and secured their cell phones while obtaining a search warrant to protect against the destruction of evidence. The Court stated that once officers have a cell phone in custody, there is no longer any risk that an arrestee will delete or destroy incriminating evidence from the phone.

To counter this rationale, however, the United States and California argued that data on a cell phone may be destroyed by two methods unique to digital data – remote wiping and data encryption. The court explained that remote wiping occurs when a third party sends a remote signal or a when a phone is preprogrammed to delete data upon entering or leaving a specific geographic area. Encryption is a security feature that, when the cell phone locks, protects it through sophisticated encryption that is unbreakable without a password.

The Court noted, however, that remote wiping does not appear to be a prevalent problem and, in fact, the briefing revealed only a few anecdotal examples of remote wiping. Further, an officer's ability to search a password-protected cell phone before data becomes encrypted is limited as most cell phones default to locked position after a short time. The Court pointed out that remote wiping can be avoided by disconnecting a cell phone from the network. The Court noted two methods of disconnecting the cell phone – by turning it off or removing the battery, and by utilizing a "Faraday bag," which isolates the phone from radio waves.

The Court discussed the added issue of information that is not stored directly on the device, but rather remotely accessed or stored in the cloud. Even the United States conceded that "the search incident to arrest exception may not be stretched to cover a search of files accessed remotely." The Court equated this type of search as finding a key in a suspect's pocket and being able to unlock and search a house. The issue is further complicated because often times officers do not know whether they are accessing data stored directly on the device or in the cloud.

The Court rejected the United States and California's suggested "fallback options" for permitting warrantless searches under certain circumstances – such as allowing warrantless searches of an arrestee's cell phone when it is believed that the phone contains evidence of the crime of arrest or restricting the scope of the search to those areas of the phone where an officer reasonably believes that information relevant to the crime, suspect's identify, or officer safety will be discovered. The Court stated that "each of the proposals is flawed and contravenes our general preference to provide clear guidelines to law enforcement through categorical rules." The Court reasoned that it would be a "particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a phone" or, when restricting the scope, officers would not be able to "discern in advance what information would be found where."

The Court also rejected the United States claim in their brief that "all data stored on a cell phone is 'materially indistinguishable' from searches of various personal items carried by an arrestee – e.g. the search of a zipper bag found on arrestee, wallet, billfold, address book. The Court reasoned that this analogy is "<u>like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together</u>."

When examining the characteristics of a cell phone, the Court stated that "modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." It reasoned that "cell phones differ in both quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." The Court described the cell phone as "minicomputers," and discussed the immense storage capacity of the cell phone and the wide variety of material that is stored on the devices. The Court stated that even the most basic phones have the capacity to hold "photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on." The Court stated that "it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep in their person a digital record of nearly every aspect of their lives – from the mundane to the intimate. . . . Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case." The use of cell phones Internet browsing, for example, can reveal an individual's private interests or concerns – e.g. health issues – and location information can reveal an individual's location over a period of time, even down to the minute. Mobile application downloads allow a person to manage detailed information about every aspect of a person's life.

The Court acknowledged that its decision "will have an impact on the ability of law enforcement to combat crime" as "cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals." The Court stressed, however, that its holding does not render information on cell phones immune from searches; **"it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest**. Moreover, the Court found that even though the search incident to a lawful arrest exception does not apply to cell phones, "other case-specific exceptions may still justify a warrantless search of a particular phone." These exigent circumstances could include "the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, or to assist persons who are seriously injured or are threatened with imminent injury." The Court, however, did not provide guidance beyond presenting the possibility that an exigent circumstances exception could exist in a case-by-case basis. **The United States Supreme Court concluded its holding by stating: "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant."**

Conclusion

It is recommend that all police departments first educate their officers on the importance of this holding, and provide instruction that while securing the cell phone or electronic device is allowed, it should be preserved and a warrant obtained. While officers like to push the envelope on search and seizure application, the concern still stands that electronics, such as cell phones, need to be treated conservatively. While we do not believe this holding requires policy revision, it does require department-wide training on its application. Departments should also provide each officer with "Faraday bags" to avoid any potential for destruction of evidence, as well as provide them the opportunity to be scrupulous in the process in between the seizure of the cell phone and the actual search.

[1] 2013 WL 4752428 (Feb. 8, 2013)
[2] 728 F.3d 1 (May 17, 2013)
[3] 395 U.S. 752 (1969)
[4] 414 U.S. 218 (1973) (patdown search of Robinson revealed a crushed cigarette package in his coat pocket. Upon opening the package, police discovered 14 capsules of heroin)
[5] 556 U.S. 332 (2009)