September - October 2014 Volume 19.5

Police Law Bulletin

City Attorneys' Office Toni M. Smith, Senior Assistant City Attorney

In this issue:

UNITED STATES SUPREME COURT

Police Generally May Not, Without a Warrant, Search Digital Information on a Cell Phone Incident To An Arrest

***Riley v California*, No. 13-132, 25 June 2014.**

This decision arose out of a pair of cases in which both defendants were arrested and their cell phones seized and searched incident to arrest.

In one case before the Court, petitioner Riley was stopped for driving with expired registration tags. In the course of the stop, the officer learned that Riley's license had been suspended. The officer impounded Riley's car and another officer conducted an inventory search of the car. Riley was arrested for possession of concealed and loaded firearms when that search turned up two handguns under the car's hood. An officer searched Riley incident to arrest and found items associated with the "bloods" street gang. The officer also seized a cell phone from Riley's pants' pocket. The officer accessed information on the phone and noticed the repeated use of a term associated with a street gang. At the police station two hours later, a detective specializing in gangs further examined the contents of the phone. Based in part on photographs and videos that the detective found, the State charged Riley in connection with a shooting that had occurred a few weeks earlier and sought an enhanced sentence based on Riley's gang membership. Riley moved to suppress all evidence that the police had obtained from his cell phone. He contended that the searches of his phone violated the Fourth Amendment because they had been performed without a warrant and were not otherwise justified by exigent circumstances. The trial court denied the motion, and Riley was convicted. The California Court of Appeal affirmed. The California Supreme Court declined review.

In the other case before the Court, respondent Wurie was arrested after police observed him participate in an apparent drug sale. At the police station, the officers seized a cell phone from Wurie's person and noticed that the phone was receiving multiple calls from a source identified as "my house" on its external screen. The officers opened the phone, accessed its call log, determined the number associated with the "my house" label, and traced that number to what they suspected was Wurie's apartment. They secured a

search warrant and found drugs, a firearm and ammunition, and cash in the ensuing search. Wurie was then charged with drug and firearm offenses. He moved to suppress the evidence obtained from the search of the apartment, arguing that it was the fruit of an unconstitutional search of his cell phone. The District Court denied the motion, and Wurie was convicted. The First Circuit reversed the denial of the motion to suppress and vacated the convictions. The court held that cell phones are distinct from other physical possessions that may be searched incident to arrest without a warrant because of the amount of personal data cell phones contain and the negligible threat they pose to law enforcement interests.

The United States Supreme Court agreed to hear both cases on appeal and unanimously issued the following opinion:

The police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.

The Court reasoned as follows:

(a) The ultimate touchstone of the Fourth Amendment is "reasonableness." Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, reasonableness generally requires that a warrant first be obtained.
(b) In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement. The well-established exception at issue here applies when a warrantless search is conducted incident to a lawful arrest.

Although the existence of the exception for such searches has been recognized for a century, its scope has been debated for nearly as long. Three related precedents govern the extent to which officers may search property found on or near an arrestee. The first, *Chimel* v. *California*, 395 U. S. 752, requires that a search incident to arrest be limited to the area within the arrestee's immediate control, where it is justified by the interests in officer safety and in preventing evidence destruction. Four years later, in *United States* v. *Robinson*, 414 U. S. 218, the Court applied the *Chimel* analysis to a search of a cigarette pack found on the arrestee's person. It held that the risks identified in *Chimel* are present in all custodial arrests, 414 U. S., at 235, even when there is no specific concern about the loss of evidence or the threat to officers in a particular case, *id.,* at 236. The trilogy concludes with *Arizona* v. *Gant*, 556 U. S. 332, which permits searches of a car where the arrestee is unsecured and within reaching distance of the passenger compartment, or where it is reasonable to believe that evidence of the crime of arrest might be found in the vehicle, *id.,* at 343.

(b) The Court declined to extend *Robinson*'s categorical rule to searches of data stored on cell phones. Absent more precise guidance from the founding era, the Court generally determines whether to exempt a given type of search from the warrant requirement by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests. That balance of interests supported the search incident to arrest exception in *Robinson*. But a search of digital information on a cell phone does not further the government interests identified in *Chimel*, and implicates substantially greater individual privacy interests than a brief physical search.

(1) The digital data stored on cell phones does not present either *Chimel* risk.

(i) Digital 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. Officers may examine the phone's physical aspects

to ensure that it will not be used as a weapon, but the data on the phone can endanger no one. To the extent that a search of cell phone data might warn officers of an impending danger, *e.g.,* that the arrestee's confederates are headed to the scene, such a concern is better addressed through consideration of case-specific exceptions to the warrant requirement, such as exigent circumstances.

(ii) The United States and California raised concerns about the destruction of evidence, arguing that, even if the cell phone is physically secure, information on the cell phone remains vulnerable to remote wiping and data encryption. As an initial matter, those broad concerns are distinct from *Chimel*'s focus on a defendant who responds to arrest by trying to conceal or destroy evidence within his reach. In addition, there was little indication that either problem is prevalent or that the opportunity to perform a search incident to arrest would be an effective solution. And, at least as to remote wiping, law enforcement currently has some technologies of its own for combatting the loss of evidence, such as turning the phone off or removing its battery. If there is a concern about encryption or other potential problems, a phone can be left on and placed in an enclosure that isolates the phone from radio waves, such as a Faraday bag. To the extent law enforcement still has specific concerns about the potential loss of evidence in a particular case, there remain more targeted ways to address those concerns. If the police are truly confronted with a "now or never situation," for example, circumstances specifically suggest that a defendant's phone will be the target of a remote wipe attempt, they may be able to rely on exigent circumstances to search the phone immediately. See *Missouri* v. *McNeely*, 569 U. S. ___, ___ (2013). Or, if officers happen to seize a phone in an unlocked state, they may be able to disable the phone's automatic-lock feature in order to secure the scene. See *Illinois* v. *McArthur*, 531 U. S. 326, 331–333.

(2) A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but more substantial privacy interests are at stake when digital data is involved.

(i) Cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person. Notably, modern cell phones have an immense storage capacity. Before cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy. But cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences. First, a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video - that reveal much more in combination than any isolated record. Second, the phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, data on the phone can date back for years. A person might carry in his pocket a slip pf paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months. In addition, an element of pervasiveness characterizes cell phones but not physical records. A decade ago officers might have occasionally stumbled across a highly personal item such as a diary, but today many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives.

(ii) The scope of the privacy interests at stake is further complicated by the fact that the data viewed on many modern cell phones may in fact be stored on a remote server. Thus, a search may extend well beyond papers and effects in the physical proximity of an arrestee, a concern that the United States recognizes but cannot definitively foreclose.

(c) The Court recognized that this decision will have some impact on the ability of law enforcement to combat crime. But the Court did not hold that the information on a cell phone is immune from search; but rather that a warrant is generally required before a search. The warrant requirement is an important component of the Court's Fourth Amendment jurisprudence, and warrants may be obtained with increasing efficiency. In addition, although the search incident to arrest exception does not apply to cell phones, the continued availability of the exigent circumstances exception may give law enforcement a justification for a warrantless search in particular cases.

High-lights and Take-aways:

- Law enforcement officers generally may *not* make a warrantless search of a cell phone incident to arrest; this includes looking for any data contained in the phone, even recent calls or texts.
- Officers should not seize a cell phone incident to arrest and make a warrantless download of its contents. Extracting data from a phone would likely be considered a search. Thus, officers should not make a warrantless download even if the intention is to obtain a warrant prior to reading the content of the downloaded data.
- If officers want to search a cell phone, they should seize it and apply for a search warrant. This includes all cell phones regardless of their technological advancement. The phone at issue in one of the cases reviewed by the Supreme Court was a flip phone (the other was a smart phone). The Court's ruling would also apply to searching similar electronic storage devices incident to arrest, such as tablets and laptops.
- A cell phone may still be searched with consent. Note though that while asking a person if he/she "minds if [you] look through their cell phone," may provide valid consent for a manual search of the phone, if officers want to download the phone's contents, they should clearly explain this to the consenting party to help ensure that the consent is informed and therefore, valid.