wiley

NEWSLETTER

The Supreme Court's Landmark "Cell Phone" Privacy Decision

July 2014

The Supreme Court's June 25, 2014 decision in *Riley v. California* (No. 13-132) and *U.S. v. Wurie* (No. 13-212) (2014 U.S. Lexis 4497) decided "how the search incident to arrest doctrine applies to modern cell phones." The Court held that under the Fourth Amendment "a warrant is generally required for such a search, even when a cell phone is seized incident to arrest."

This decision likely will have future ramifications extending far beyond police practices in searching street criminals, for multiple reasons. First, all nine justices joined in the bottom line, so this is not a decision that will be undermined by the next Supreme Court appointments. Second, the decisional rationale is broad and forward looking. Third, although phased, and thus far publicized, in terms of "cell phones," the Court's focus was on computerized digital information, which will be seen as an invitation to seek privacy protection for such information in numerous other contexts, both from the courts and in the legislature.

Proceedings Below

The *Riley* case arose through the California state court system. Riley was stopped for "driving with expired registration tags." When it appeared his "license had been suspended," the police impounded and searched the car. They found guns and then arrested Riley. The police searched Riley incident to that arrest and "seized a cell phone from Riley's pocket." This was a "smart phone," which the Supreme Court characterized as a "cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity."

Authors

Bruce L. McDonald
Senior Counsel
202.719.7014
bmcdonald@wiley.law

The police interpreted certain entries on Riley's contact list and videos on the phone to indicate Riley had associations with the Bloods street gang. Stored photographs showed Riley standing in front of a car the police "suspected had been involved in a shooting a few weeks earlier." Riley was charged in connection with that earlier crime. His motion to suppress evidence was denied, and Riley was convicted. The conviction was affirmed by the California intermediate Court of Appeal on the strength of the California Supreme Court's decision in *People v. Diaz*, 244 P.3d 501 (2011), holding that the Fourth Amendment permitted a warrantless search of cell phone data where the phone was "immediately associated with the arrestee's person." After the California Supreme Court declined review, the U.S. Supreme Court granted *certiorari.*

The *Wurie* case proceeded through the federal court system. It began when a "police officer performing routine surveillance" observed Wurie "make an apparent drug sale from a car." Wurie was arrested and taken to the police station where a "flip phone," described as having a "smaller range of features than a smart phone," was "seized" from "Wurie's person." That phone began "repeatedly receiving calls from a source identified as 'my house' on the phone's external screen." The police then opened the phone and determined the "phone number associated with the 'my house' label." Then using an "online phone directory," they identified the location of Wurie's apartment. They obtained and executed a search warrant and found in the apartment crack cocaine, other drugs, a firearm, and ammunition. On that basis, Wurie was charged with crack cocaine distribution and being a felon in possession of a firearm and ammunition. His motion to suppress the evidence as the fruit of an unlawful cell phone search was denied, and Wurie was convicted. On appeal, a divided panel of the First Circuit reversed the denial of Wurie's motion to suppress. The Supreme Court then granted *certiorari.*

Supreme Court Proceedings

By combining these two cases for review, the Supreme Court perhaps signaled that it intended to consider issues broader than presented by these two specific searches. In any event, the briefing attracted a score of *amici*, who tended to broaden the issues before the Court.

Two years ago, when he announced the Administration's Consumer Privacy Bill of Rights, President Obama declared that, "Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones." Accordingly, "applying our timeless privacy values to the new technologies and circumstances of our times" was said to justify the business community's paying the substantial price needed to implement and maintain specified types of protections, and Congress was urged to enact legislation ensuring such costs were borne. Chief Justice Roberts recognized that in the area of government searches also, "privacy comes at a cost," but before the Supreme Court, the Administration vigorously resisted paying any such cost, contending that the "Court should not exempt cell phones from officers' search-incident-to-arrest authority." That position, and several full-back positions, were squarely rejected.

Chief Justice Roberts authored the Opinion of the Court, in which all the Associate Justices joined, except Justice Alito, who concurred in a separate opinion. Roberts' analysis focused on three earlier Supreme Court decisions. In *Chimel v. California*, 395 U.S. 752 (1969), Chimel was arrested inside his home, and incident to that arrest the police, without a warrant, "proceeded to search his entire three-bedroom house, including the

attic and garage." The Court held that search was excessive. In *United States v. Robinson*, 414 U.S. 218 (1973), Robinson was arrested and subjected to a "patdown search," during which the officer "felt an object that he could not identify in Robinson's coat." He "removed the object, which turned out to be a crumpled cigarette package, and opened it." Inside he found "14 capsules of heroin." The Court ruled that search was proper. More recently, in *Arizona v. Gant*, 556 U.S. 332 (2009), the Court held it was reasonable to search an automobile's passenger compartment incident to an arrest "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search" or when it is "reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle." Obviously, neither of those three cases had examined issues related to digital information.

The Court applied a test derived from *Chimel* under which it is "reasonable for the arresting officer to search the person arrested in order to remove any weapons" and "to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction." It found searching a cell phone did not meet that test.

The search of data on a cell phone did not meet the first part of the *Chimel* test because digital "data stored on a cell phone cannot itself be used as weapon." The United States and California argued that the second prong was met because there are risks of data destruction either by the arrestee or by "remote wiping" by some third party or because of "data encryption." The Court rejected the first risk on the ground that "once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone." The other risks were discounted because the Court had been "given little reason to believe that either problem is prevalent." Indeed, there was no suggestion that the police had considered either to be a risk in the *Riley* and *Wurie* situations themselves. The *Riley* search of photographs occurred "about two hours after the arrest" and in *Wurie* the police did not consider searching the flip phone until "five or ten minutes after arriving at the station" following the arrest.

Although Chief Justice Roberts' opinion focused on *Chimel* standard, it acknowledged that many years earlier the Court had declared that the government had a right "always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime." *Weeks v United States*, 232 U.S. 383 (1914). Justice Alito thought that principle deserved more recognition than reflected in the Opinion of the Court. Read literally, that search for "evidence of crimes" test would appear to authorize much broader searches than permitted under the *Chimel* test.

More and Different Data

The key to the Court's ruling here was that the amount of information accessible through a "cell phone" was perceived to be both quantitatively vastly larger and to include qualitatively different types of information than could be found through searching a wallet or a purse. While using the label "cell phone," the Court made express that it had in mind "microcomputers that also happen to have the capacity to be used as a telephone." Thus, there will be pressure to extend the present ruling to other types of computers that may be found on the person of an arrestee.

The Court stressed that one "distinguishing feature" of such devices is their "immerse storage capacity," with a smart phone having a "standard capacity of 16 gigabytes," equivalent to "millions of pages of text." This volume permits collecting in one place "many types of information," including information spanning a considerable period of time (dating "back to the purchase of the phone, or even earlier"). Thus, persons may be carrying a "digital record of every aspect of their lives."

Qualitatively different types of information noted by the Court included an "Internet browsing history" that can "reveal an individual's private interests or concerns" and location data that "can also reveal where a person has been," allowing police to "reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." The Court also focused on the availability and widespread use of apps, which "together can form a revealing montage of the user's life."

The combination of such factors produced the result that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house."

The Cloud

Beyond that, the Court gave weight to the fact that "the data a user views on many modern cell phones may not in fact be stored on the device itself," but rather in the "cloud." The Court deemed the United States to "concede that the search incident to arrest exception may not be stretched to cover search of files accessed remotely" but asserted that police "would not typically know whether the information they are viewing was stored locally at the time of arrest or has been pulled from the cloud." Down the road, this part of the Court's analysis may be cited as representing a departure from the traditional position that an individual has little protectable privacy interest in information the individual has voluntarily provided to a third party.

Fallback Positions

The United States and/or California advocated several fallback rules that might apply if the Court denied their preferred right to search all cell phone data incident to an arrest. The Court expressly rejected four of those. Authorizing a warrantless search "whenever it is reasonable to believe that the phone contains evidence of the crime of arrest" was rejected as in practice giving "police officers unbridled discretion to rummage at will." Restricting the search "to those areas of the phone where an officer reasonably believes that information relevant to the crime, the arrestee's identity, or officer safety" was also rejected as imposing "few meaningful constraints on officers." Officer freedom "to search a phone's call log" was rejected because "call logs typically contain more than just phone numbers," such as "the label 'my house' in Wurie's case." The proposal that "officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart" was rejected because of the quantitative difference between one photo in a wallet and "thousands of photos in a digital gallery," and because such a test would "launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records."

General Warrants

Chief Justice Roberts concluded his opinion by recalling the "general warrants" that "allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity" and how resentment of that practice had contributed to the Revolution. The fact that technology now allows Americans to carry "the privacies of life" in their hands "does not make the information any less worthy of the protection for which the Founders fought." Accordingly, the Court's message to the police was "simple—a warrant."