Mr Jay Shapiro on

Riley v. California and *United States v. Wurie*: Supreme Court Determines Legality of Cell Phone Searches Incident to Arrest

2014 Emerging Issues 7239

Click here for more Emerging Issues Analyses related to this Area of Law.

Keeping up with technology is an everyday fact of life. From considering what mobile computing device works best to how to download the latest video from the Internet, so many Americans face challenges presented by ever-changing technology. The courts are not immune to these concerns. Five years ago, in *People v. Weaver*, 12 N.Y.3d 433, 882 N.Y.S.2d 357, 909 N.E.2d 1195 (2009), the New York Court of Appeals directed that a search warrant be obtained in order for law enforcement to use a GPS device placed on the inside of a target's motor vehicle. Explaining its concerns, the court described the pervasive manner of search that could be conducted through the electronically enhanced search, warning that law enforcement could use the GPS device to learn about "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, the synagogue or church."

Now, the United States Supreme Court has issued a decision that will certainly impact arrest processing and investigative activities around the country. In an opinion that addressed appeals from one state and one federal court, the Supreme Court delivered an opinion that describes clear limitations on searches of cell phones that are conducted incident to arrest.

Both cases, *Riley v. California* and *United States v. Wurie,* decided June 25, 2014, involved searches of cellular devices that were taken from defendants following their arrests, although there were significant differences in the devices. In *Riley,* the defendant was stopped for a motor vehicle violation concerning his registration. After his car was impounded when the police determined that his license had been suspended, two handguns were found hidden beneath the vehicle's hood and he was charged with weapons offenses. When Riley was searched, the police seized items revealing his street gang affiliation as well as his cell phone which was in his pants pocket. This "smart phone" had "a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity."

One of the officers saw that the phone contained data with the prefix "CK", which stood for "Crips Killers", a reference to members of the Bloods street gang. Within hours of the arrest, a detective closely examined the phone, searching for images of gang members with guns and saw some videos of that nature. The search also revealed photographs of Riley standing in front of a vehicle that the police believed had recently been involved in a shooting. Riley was ultimately charged with that shooting and the trial court denied his motion to suppress the evidence obtained from the cell phone search based upon a claim that it was an illegal search. Evidence from the search was used to support the prosecution's position that Riley was involved in gang activity. He was convicted and sentenced to 15 years to life in prison. His conviction was affirmed by the California Court of

Appeals, which held that the warrantless cell phone search was proper, having occurred incident to arrest and because the phone was closely associated with Riley, having been taken from his clothes.

The arrest in *Wurie* followed an observation of a drug sale. Unlike the cell phone that Riley possessed, the phone (one of two) that was taken from Wurie by the police incident to his arrest was a simple "flip phone." During the arrest processing, the police noticed that there were incoming calls to that phone from a number denominated "my house." The police opened the phone and noted that the wallpaper was a photograph of a woman holding a baby. The police accessed the call log from the phone and identified the "my house" number. They then used that information to find the address associated with it, an apartment building. The police went to the location, noted a mailbox with Wurie's name on it, and "observed through a window a woman who resembled the woman in the photograph on Wurie's phone." They then obtained a search warrant and during the execution "found and seized 215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash."

Wurie was prosecuted for the federal offenses of distributing crack cocaine, possessing crack cocaine with intent to distribute, and being a felon in possession of a firearm and ammunition. The district court denied Wurie's motion to suppress the evidence seized pursuant to the search which was based upon a claim that it was the product of an illegal search of the cell phone. Wurie was convicted after trial and sentenced to a prison term of 262 months. The Court of Appeals for the First Circuit reversed the ruling on the suppression motion and vacated the conviction. The court held that the amount of personal data obtained through the search of a cell phone makes it different from other articles searched incident to arrest.

The Supreme Court's review of these two cases addressed "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." In each case, the prosecution maintained that the searches were valid because they were conducted incident to valid arrests. But the Court determined that the line of cases that established the applicable precedent could not be extended to permit these warrantless intrusions.

At the heart of the Court's analysis, written by Chief Justice Roberts, were the following: 1) searches of cell phones incident to arrest do not satisfy the justifications that flowed from the line of cases starting with *Chimel v. California*, 395 U.S. 752 (1969); 2) there is little justification for the support that searches of cell phones incident to arrest will serve to prevent the destruction of evidence; and 3) recognition of the vast breadth and depth of information available through a cell phone search mandates the use of a search warrant rather than a warrantless search incident to arrest.

Through its analysis, the Court made the following points:

- "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."

  In respect to this determination, the Court noted that the police can examine the cell phone to look for any type of hidden weapon.

- Adequate steps can be taken by law enforcement to prevent a third party from destroying data on the seized cell phone.

The court found that "remote wiping" and data encryption could be addressed by the police by using such techniques as removing the battery from the phone or placing the phone in a "Faraday bag" which would prevent remote access.

The Court balanced the law enforcement justifications for warrantless access to cell phone data against the type of information accessible to law enforcement through a successful search. The Court wrote, "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." In describing this difference, the Court addressed the vast capabilities of cells phones:

> The storage capacity of cell phones has several interrelated consequences for privacy. 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, a cell 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, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of 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, as would routinely be kept on a phone. (Internal citation omitted.)

In addition to the data maintained on a cell phone, the Court pointed out that allowing the police to search cell phones without a warrant would also provide access to the incredibly vast storage capacity beyond the phone---on the "cloud."

The Court was emphatic in its view it was not holding that all such warrantless searches were illegal, but instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest." Consequently, the Court did leave the door open for those circumstances when a warrantless cell phone search would be appropriate. What would justify such an intrusion will certainly be the subject of future litigation and, perhaps, further pronouncements by the Supreme Court.

Click here for more Emerging Issues Analyses related to this Area of Law.

About the Author. Jay Shapiro is a partner in the New York office of White and Williams LLP. Jay has more than 30 years experience concentrating his practice in litigation matters. He began his legal career as a prosecutor in the Bronx County District Attorney's Office (1980-1988) and later joined the King's County District Attorney's Office (1990-2002) where he became the Deputy District Attorney in charge of the Rackets Division before going into private practice. Mr. Shapiro has tried

more than thirty-five cases in state and federal court. In private practice, he has handled litigation involving insurance fraud, white collar crime and Lanham Act (trademark) violations.