Riley v. California

(2014) __ U.S. __ [2014 WL 2864483]

Issue

If officers arrest a person who possesses a cell phone, may they search the digital contents of the phone as an incident to the arrest, or must they obtain a warrant?

Facts

In the course of a car stop, San Diego police officers arrested Riley for possession of two concealed and loaded firearms. They also discovered a "smart phone" in his pants pocket.[1] Having reason to believe that Riley was a member of the Bloods street gang, an officer "accessed information on the phone" and noticed that some words (apparently in text messages or in contacts lists) were preceded by the letters "CK" which, he testified, stands for "Crip Killers" which is slang for members of the Bloods. No further search of a phone was conducted at the scene but, about two hours later at the police station, a gang detective testified that he "went through" Riley's phone "looking for evidence, because gang members will often video themselves with guns." He found "a lot of stuff" in the phone, including photos of Riley standing in front of a car that officers suspected had been involved in a shooting a few weeks earlier.

Riley was subsequently charged with the shooting, and the charge included a gang enhancement. In the trial court, Riley filed a motion to suppress the evidence in the phone linking him to the Bloods and the vehicle used in the shooting. The motion was denied, Riley was found guilty, and the gang enhancement was affirmed. The California Court of Appeal ruled the search of the phone was lawful pursuant to the California Supreme Court's ruling in *People v. Diaz* that a cell phone may be searched incident to an arrest because it is an object that is closely associated with the person of the arrestee.[2] Riley appealed to the United States Supreme Court.

Discussion

As a general rule, officers who have arrested a person may, as a routine incident to the arrest, search all property in the arrestee's possession to which he had immediate access or which was "immediately associated with the person of the arrestee," such as clothing.[3] These searches are permitted because (1) the property might contain something that poses a threat to officers or others; or (2) it might contain evidence that could be destroyed, or its evidentiary value compromised, if officers delayed the search until a warrant could be issued.

The Court in *Riley* noted, however, that the justification for an immediate warrantless search vanishes, or is at least weakened, in situations where officers, instead of searching a physical object (such as a wallet or purse), are searching digitally-stored information. For one thing, said the Court, such information "cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape." Or, as the First Circuit

---

[1] **NOTE**: The Court defined a "smart phone" as a "cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity."

[2] (2011) 51 Cal.4th 84.

[3] See *Arizona v. Gant* (2009) 556 U.S. 332; *U.S. v. Edwards* (1974) 415 U.S. 800, 805; *U.S. v. Chadwick* (1977) 433 U.S. 1, 15.

observed in *Riley's* companion case, *U.S. v. Wurie*, the officers "knew exactly what they would find therein; data. They also knew that the data could not harm them."[4]

The Court also concluded there was little justification for cell phone searches under the "destruction of evidence" rationale. Although it conceded that it might be possible for an accomplice of the arrestee to remotely destroy the data via "remote wiping," it noted there are "at least two simple ways" to prevent it: (1) turn the phone off or remove the battery, or (2) place the phone in a so-called "Faraday bag" "an enclosure [essentially an aluminum sandwich bag] that isolates the phone from radio waves."[5]

In addition to the lack of an overriding justification for warrantless searches of cell phones, the Court pointed out that they are potentially highly intrusive. Said the Court, "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone." Moreover, the amount of data stored in a cell phone can be massive if the device is linked to a remote server in the "cloud."

For all of these reasons, the Court ruled—and it was unanimous—that officers may not search an arrestee's cell phone as a routine incident to the arrest.[6] Instead, if they think they have probable cause, they may seize the phone and promptly apply for a warrant.[7] As the Court put it, "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."

The Court indicated, however, that officers would be permitted to conduct an immediate warrantless search of an arrestee's cell phone if they could articulate specific facts that reasonably indicated that the phone presented an imminent threat or if there was reason to believe the data would be destroyed if they waited for a warrant. Said the Court, "If the police are truly confronted with a 'now or never' situation—for example, circumstances suggesting that a defendant's phone will be the target of an imminent remote-wipe attempt—they may be able to rely on exigent circumstances to search the phone immediately." Finally, the Court said that, because of the possibility that a weapon might be disguised as a cell phone or because it might contain a weapon, officers "remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case."

The Court concluded by saying, "We cannot deny that our decision today will have an impact of the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communications among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost."

---

[4] (1st Cir. 2013) 728 F.3d 1, 10.

[5] **NOTE**: The Court acknowledged that these precautions "may not be a complete answer to the problem, but at least for now they provide a reasonable response." Some officers who are trained in this field have expressed skepticism.

[6] **NOTE**: The Court's ruling implicitly overturned the California Supreme Court's ruling in *People v. Diaz* (2011) 51 Cal.4th 84 that cell phones could be searched incident to arrest because cell phones are the type of item that is "immediately associated with the person of the arrestee."

[7] See *Riley v. California* (2014) __ U.S. __ [2014 WL 2864483] ["Both Riley and Wurie concede that officers could have seized and secured their cell phones to prevent destruction of evidence while seeking a warrant. That is a sensible concession."]; *United States v. Place* (1983) 462 U.S. 696, 706.

Comment

Riley is undoubtedly an important case. But it is probably even more important than it first appears. That is because, until now, the United States Supreme Court has been very hesitant about taking a position on the privacy of digitally-stored communications. For example, in a case from 2010, *City of Ontario v. Quon*,[8] the Court decided not to decide whether a police officer could reasonably expect privacy in text messages that he was sending and receiving over a departmental pager. The Court explained that the reason for its indecision was that the "judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." In the Fall 2010 *Point of View* we were critical of this remark because, "if the 'emerging' character of a government activity were to stand as a barrier to 'elaborating' constitutional standards for its use, there might never be a ruling on privacy in digital communications because the technology will be emerging for decades, probably centuries."

Well, at least that's no longer a problem. In *Riley,* the Supreme Court shed its timidity and essentially announced that the role of cell phones (and undoubtedly computers and tablets as well) has become so clear, and that the threat to the privacy of their contents has become so disconcerting, that increased controls have become necessary. It will be interesting to see how the lower courts interpret *Riley* in the coming years. But in light of *Riley* and the Court's recent decisions on obtaining blood samples from DUI arrestees,[9] and installing electronic tracking devices on vehicles,[10] it is possible that the Court's historical "preference" for search warrants is becoming—or has already become—more akin to a requirement that is subject to certain exceptions that require specific facts, not generalized concerns. If this is so, it will be more important than ever that law enforcement officers become adept at writing, applying for, and executing search warrants. Thankfully, this comes at a time when modern technology is making the process much easier and quicker by allowing officers to apply for and obtain warrants over secure internet sites via their desktop computers, patrol car computers, and even iPads. But modern technology does not yet have the ability to write an effective affidavit. That still requires a human brain.

Finally, the question has arisen whether *Riley* changes the general rule that officers may conduct warrantless searches of a suspect's cell phone or similar devices if he was on probation or parole with a search clause that authorized searches of personal property in his possession or control. Although *Riley* applies only to searches incident to arrest, it is at least conceivable that a court could rule that a warrant was required unless the terms of probation or parole specifically authorized a search of such devices. That is because the Court made it clear that searches for digitally-stored data are much more intrusive than virtually all other searches of personal property. So, until the courts decide the issue, officers should consider seeking a warrant if they think they have probable cause. Otherwise, conduct the search but be aware that the issue may need to be litigated. POV

Date first posted: June 25, 2014. **Updated**: July 26, 2014.
Comment added: June 27, 2014

[8] (2010) 560 U.S. 746.
[9] See *Missouri v. McNeely* (2013) __ U.S. __ [133 S.Ct. 1552].
[10] See *United States v. Jones* (2012) __ U.S. __ [132 S.Ct. 945].