

## Riley v. California

(2014) \_\_ U.S. \_\_ [2014 WL 2864483]

### Issue

If officers arrest a person who possesses a cell phone, may officers 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.<sup>1</sup> 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 (presumably in text messages or a contacts list) were preceded by the letters ‘CK’—a label that, he believed, stood for ‘Crip Killers,’ a slang term for members of the Bloods gang.” 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 this 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.<sup>2</sup> 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.<sup>3</sup> These searches are permitted because of the possibility that (1) the property might contain something that poses a threat to officers or others, and (2) any evidence inside the property might be destroyed before officers could obtain a warrant.

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, are searching digitally-stored bits of information. For one thing, said the Court, such data “cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee’s escape.” Or, as the First Circuit 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.”<sup>4</sup>

---

<sup>1</sup> 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.”

<sup>2</sup> (2011) 51 Cal.4<sup>th</sup> 84.

<sup>3</sup> See *U.S. v. Edwards* (1974) 415 U.S. 800, 805; *U.S. v. Chadwick* (1977) 433 U.S. 1, 15.

<sup>4</sup> (1<sup>st</sup> Cir. 2013) 728 F.3d 1, 10.

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,”<sup>5</sup> 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.”<sup>6</sup>

In addition to the lack of an overriding justification for warrantless searches of cell phones, the Court pointed out that they are extremely 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.” The Court added that officers who search a person’s cell phone may also be able to access a massive amount of information stored in remote servers; i.e., 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.<sup>7</sup> Instead, if they think they have probable cause, they may seize the phone and promptly apply for a warrant.<sup>8</sup> 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 went on to say, however, that nothing in its opinion would prevent an immediate warrantless search of an arrestee’s cell phone if there were exigent circumstances. 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, 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 that “[w]e 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.” POV

**Date posted:** June 25, 2014.

---

<sup>5</sup> **NOTE:** The Court explained that “[r]emote wiping occurs when a phone, connected to a wireless network, receives a signal that erases stored data. This can happen when a third party sends a remote signal or when a phone is preprogrammed to delete data upon entering or leaving certain geographic areas (so-called ‘geofencing’).”]

<sup>6</sup> **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.”

<sup>7</sup> **NOTE:** The Court’s ruling implicitly overturned the California Supreme Court’s ruling in *People v. Diaz* (2011) 51 Cal.4<sup>th</sup> 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.”

<sup>8</sup> 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.