



UNITED STATES SUPREME COURT

SUPREME COURT RULING IN TWO CONSOLIDATED CASES THAT A CELLULAR DEVICE MAY NOT BE SEARCHED INCIDENT TO ARREST

Riley v. California

June 2014

For duplication & redistribution of this article, please contact the Public Agency Training Council by phone at 1.800.365.0119.
PATC Legal & Liability Risk Management Institute 5235 Decatur Blvd Indianapolis, IN 46241

Article Source: http://www.llrmi.com/articles/legal_update/2014_riley_v_california.shtml

Printable Version: http://www.patc.com/weeklyarticles/print/2014_riley_v_california.pdf

©2014 [Jack Ryan](#), Attorney, PATC Legal & Liability Risk Management Institute (LLRMI.com)

The Supreme Court has ruled in two consolidated cases that a cellular device may not be searched incident to arrest.

Exigency may justify a search but the possibility of a remote wipe or data encryption due to phone lock is insufficient to establish exigency.

The two cases as outlined by the Court:

The First Case:

In the first case, petitioner David Riley was stopped by a police officer for driving with expired registration tags. In the course of the stop, the officer also learned that Riley's license had been suspended. The officer impounded Riley's car, pursuant to department policy, 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 the arrest and found items associated with the "Bloods" street gang. He also seized a cell phone from Riley's pants pocket. According to Riley's uncontradicted assertion, the phone was a "smart phone," a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet



**FOLLOW THESE FREE
ARTICLES ONLINE AT**
<http://patc.com/news/>

Email | Mail | RSS | Facebook | Twitter | LinkedIn

©2014 Article published in the free PATC / LLRMI E-Newsletter: 800.365.0119

Link to Article online: http://www.llrmi.com/articles/legal_update/2014_riley_v_california.shtml
<http://www.patc.com> | <http://www.llrmi.com> | <http://www.fsti.com> | <http://www.school-training.com> | <http://www.patctech.com/>

connectivity. The 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.

At the police station about two hours after the arrest, a detective specializing in gangs further examined the contents of the phone. The detective testified that he “went through” Riley’s phone “looking for evidence, because . . . gang members will often video themselves with guns or take pictures of themselves with the guns.” Although there was “a lot of stuff ” on the phone, particular files that “caught [the detective’s] eye” included videos of young men sparring while someone yelled encouragement using the moniker “Blood.” The police also found photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier.

Riley was ultimately charged, in connection with that earlier shooting, with firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder. The State alleged that Riley had committed those crimes for the benefit of a criminal street gang, an aggravating factor that carries an enhanced sentence. Prior to trial, 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 rejected that argument. At Riley’s trial, police officers testified about the photographs and videos found on the phone, and some of the photographs were admitted into evidence. Riley was convicted on all three counts and received an enhanced sentence of 15 years to life in prison.

The second case:

In the second case, a police officer performing routine surveillance observed respondent Brima Wurie make an apparent drug sale from a car. Officers subsequently arrested Wurie and took him to the police station. At the station, the officers seized two cell phones from Wurie’s person. The one at issue here was a “flip phone,” a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone. Five to ten minutes after arriving at the station, the officers noticed that the phone was repeatedly receiving calls from a source identified as “my house” on the phone’s external screen. A few minutes later, they opened the phone and saw a photograph of a woman and a baby set as the phone’s wallpaper. They pressed one button on the phone to access its call log, then another button to determine the phone number associated with the “my house” label. They next used an online phone directory to trace that phone number to an apartment building.

When the officers went to the building, they saw Wurie’s name on a mailbox and observed through a window a woman who resembled the woman in the photograph on Wurie’s phone. They secured the apartment while obtaining a search warrant and, upon later executing the warrant, found and seized 215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash.

Wurie was charged with distributing crack cocaine, possessing crack cocaine with intent to distribute, and being a felon in possession of a firearm and ammunition. 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. 612 F. Supp. 2d 104 (Mass. 2009). Wurie was convicted on all three counts and sentenced to 262 months in prison.

The issue in both of these cases concerned whether or not the search of a cellular phone/device that contains personal data could be undertaken as an incident to arrest search that is allowed as an exception to the warrant requirement. The purpose of the search incident to arrest exception is to protect an officer from being harmed as well as to preserve evidence that might otherwise be destroyed.

In examining the issue of cellular phones the court noted that when deciding whether a particular search can be conducted without a warrant, the Court compares the government interest in conducting the search without the warrant versus the intrusion on the privacy right of the individual.

The Court then looked at the government interests with respect to search incident to arrest, namely harm to the officer and destruction of evidence, and concluded that this interest was not strong when it comes to digital data. In looking at the individual's interest, the Court noted that cellular devices contain significant private information by way of digital data. Thus the individual's interest in the data is significant.

In weighing the interests between individual privacy in stored digital data against the government interest of harm to the officer and destruction of evidence, the Court concluded that the individual's interest was more significant, thus generally a warrant must be obtained to search a cellular device.

In reaching its decision the Court noted that the digital data itself could not be used to harm an officer or to effectuate an escape. The Court noted that an officer could still view the device itself to determine if the device could be used as a weapon i.e. hidden razor blades.

The Court rejected an argument that an officer might be protected from harm in a case where a text or other data gave the officer notice that help for the suspect was on the way to the scene. The Court noted that the search incident to exception was created to protect officers from danger at the scene rather than danger that may be on the way. The Court went on to say that such dangers are better addressed by an articulated exigent circumstances argument on a case-by-case basis rather than by a broad bright-line exception.

The Court also rejected a destruction of evidence argument whereby remote wiping of data or data encryption was to occur. In its rejection the Court noted that there was no evidence that either of these problems occur on a regular basis. The Court noted that to avoid data encryption, law enforcement would have to come into possession of the phone while it was in an unlocked state and keep it in the unlocked state.

With respect to remote wiping, the Court noted that law enforcement has ways to prevent such action either by removing the phone from the network by shutting it off and removing the battery or by placing it in available enclosures that isolates the phone from radio waves.

On the other side, the Court noted that in contemporary society individuals maintain significant private information on their phones which is entitled to significant Constitutional protection.

The Court noted that law enforcement is not completely barred from a warrantless search and that if circumstances present themselves where officers can articulate truly exigent circumstances, beyond the basic encryption or remote wipe argument, then the exigent circumstances exception may be available to justify the search without a warrant.

Note: *Court holdings can vary significantly between jurisdictions. As such, it is advisable to seek the advice of a local prosecutor or legal adviser regarding questions on specific cases. This article is not intended to constitute legal advice on a specific case.*