Local Government Insurance Trust
LGIT

ROLL CALL REPORTER

June 2014

Absent a warrant or exigent circumstances, a law enforcement officer *cannot* search digital information on a cell phone seized from an arrestee.

QUESTION: **Can the police, without a warrant, search digital information on a cell phone seized from a person who has been arrested?**

ANSWER: **No. Absent a warrant or exigent circumstances, officers must obtain a warrant prior to searching information digitally stored on a cell phone.**

CASE: ***David Leon RILEY v. CALIFORNIA***
Supreme Court of the United States, Decided June 25, 2014

The Traffic Stop and Vehicle Inventory Search:

David Riley was stopped by a police officer for driving with expired 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.

The Search Incident to Arrest and the Cell Phone:

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. 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 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 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. He went through the phone for evidence because gang members often video themselves with guns or take pictures of themselves with guns. The detective found a number of things on the phone, including photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier.

The Additional Charges Related to an Earlier Shooting:

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.

The Motion to Suppress and Conviction:

Prior to trial, Riley moved to suppress all evidence that the police had obtained from his cell phone. He contended that the searches violated the Fourth Amendment because they had been performed without a warrant and were not otherwise justified by exigent circumstances. The motion was denied and the evidence from the phone was used against him at trial. Riley was convicted on all three counts and received an enhanced sentence of 15 years to life in prison. The state appellate court affirmed and the Supreme Court of the United States agreed to review the case.

What the Supreme Court Held:

The Supreme Court reversed the state courts, holding that Riley's motion to suppress the evidence seized from his smart phone should have been suppressed. It did so based upon the nature of modern cell phones themselves. The court observed that cell phones now "place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search allowed in the early search incident to arrest cases." The court further observed that the primary issues that led to the search incident to arrest exception—harm to officers and destruction of evidence—are not present "when the search is of digital data." Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate an arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon. Once an officer has secured a phone and eliminated any potential physical threats, data on the phone can endanger no one. Consequently, officers must generally secure a warrant before conducting a search of digital data.

NOTE: It is important to note that the Supreme Court recognized that officers can seize and secure cell phones recovered in searches incident to arrest to prevent destruction of evidence. The limitation, however, is that, at the same time, officers must seek a warrant to search the phone's contents. And 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 evidence. The Court also considered the issues of "**remote wiping**" of data and **data encryption**. In regard to the former, the Court said that "remote wiping" can be prevented by disconnecting a phone from the network. This can be done in at least two ways: turning the phone off or removing its battery. As to data encryption, the Court said that officers can leave the phone powered on and place it in an enclosure that isolates the phone from radio waves. Such devices are commonly called "Faraday bags" (essentially sandwich bags made of aluminum foil).

By John F. Breads, Jr., Director of Legal Services, Local Government Insurance Trust

7225 Parkway Drive, Hanover, MD 21076 · Phone 443.561.1700 · TF 800.673.8231 · FX 443.561.1701 · jbreads@lgit.org · www.lgit.org