Roll Call Training Bulletin

Produced by: Ofcr Obed Magny
Prepared by:

Sam Somers Jr., Chief of Police

Volume 27

July 1, 2014

Supreme Court Ruling Regarding Searching Cell Phones Incident to Arrest

Based on legal opinions/interpretations of the Supreme Court's recent ruling by the CPOA and Atty. Bruce Praet, combined with procedures for our Digital Forensics Unit, this bulletin provides critical search and seizure information that will impact how we do our job.

Background

The Supreme Court decision in *Riley v. California, 2014 U.S. Lexis 4497* states that **officers must generally get a warrant before searching the data stored on a cell phone. The "search incident to a lawful arrest" exception to the Fourth Amendment will no longer excuse the need for a search warrant when it comes to looking through a phone of an arrestee**. Basically, just because you have a desire (hunch) to search a phone does not mean you have a legal, justified, or probable cause right to do so.

The ruling stems from two different cases. The first was regarding an inventory search of Riley's impounded vehicle after being lawfully arrested for a suspended license. During a tow inventory search two handguns were found under the hood of Riley's vehicle. Officers then searched Riley's cell phone that was in his pocket at the time of his lawful arrest. The cell phone search yielded photographs and videos tying Riley to a "violent street gang" and thus a large enhancement to his sentence.

The second case was a cell phone search after the lawful arrest of a subject for narcotic sales. The subject's cell phone was searched incident to arrest to determine his true address. A warrant was then obtained for the true address and drugs were found inside. The First Circuit suppressed the evidence based on the initial search of the phone.

Furthermore, the Supreme Court noted that information on a cell phone (and remotely on a "Cloud") contains private information that is vastly different from the classic physical evidence one might find by the original search incident to arrest exception to the Fourth Amendment. The Court also noted that a cell phone is usually not a weapon and that it can generally be secured while officers obtain a warrant before inspecting the contents of an arrestee's cell phone.

When can I search a cell phone without a warrant?

There are still many situations where you can search a subject's cell phone without a warrant:

- Consent
- Probation, parole and PRCS status
- Factually specific evidence of an "imminent and immediate remote wipe" of the device
    - Must be detailed and able to articulate more than a standard "destruction of evidence" possibility.

- Intervene to prevent harm to someone in imminent danger
- Apprehend a fleeing felon (again, articulate facts needed for this one)
- To avoid detonation of a bomb

If you have reason to search a phone and you will have to go to another location to write your warrant or release your suspect, to prevent a remote wipe of the device, the Court suggests removing the battery or placing it in a "Faraday bag." A Faraday bag is simply a bag that will prevent radio waves from traveling to or from the phone. Soon Faraday bags will be found at all booking locations as well as a limited number with CSI. In a pinch, wrap the phone in foil, put it in a plastic bag and then in a closed paint can – your own Faraday bag!

- Manipulation of a phone to put it in airplane mode is considered a search and not allowed.
- Mirroring, copying or downloading of the phone **is** permitted according to the Court to preserve the evidence but the information obtained *shall not* be viewed prior to obtaining the warrant and it is advisable to indicate in the warrant that the data has already been preserved.

As with any new change in the law or the way we do our jobs, there are often nuances and each circumstance is different from the next and no doubt, in the near future, there will be more discussions. Discussions about creating a template search warrant for cell phones incident to arrest is on-going and likely to be the topic of another *Roll Call Bulletin*.

In the event a situation arises where there is an immediate need to download a cell phone to preserve evidence, contact the **Digital Forensics Unit** at **808-0564**, Monday through Friday during normal business hours. During non-business hours, coordinate with your sergeant or area CSU/GET as they can assist in cell phone downloads and warrants.

Senate Bill 178- California Electronic Communications Privacy Act

There is a new state law that will take effect on January 1, 2016. It is SB 178-The California Electronic Communications Privacy Act. Absent any exigency the bill requires government agencies to obtain a search warrant, wiretap, subpoena, or court order, to obtain information from electronic devices, and electronic communications.

In addition to cell phones, electronic devices include but are not limited to: Tablets, iPad's, computers, etc. Information maintained by service providers would also be subject to a search warrant or subpoena, unless the service provider is not prohibited by state or federal law from voluntarily disclosing certain information. If the information is voluntarily released by a service provider, government agencies must purge the information within 90 days unless a specific exception applies.

SB 178 is consistent with the Riley v. California (2014) decision by the U.S. Supreme Court when it held that absent exigency, law enforcement agencies could not engage in the warrantless search of a smart phone, incident to arrest since it would violate a person's constitutional rights.