Policy 1017

Subject	
MOBILE DEVICE SEARCHES	
Date Published	Page
1 August 2016	**1 of 3**

By Order of the Police Commissioner

POLICY

The United States Supreme Court in *Riley v. California*, October Term, 2013, No.: 13-132, ruled that absent exigent circumstances, warrantless searches of cell phone data, incident to an arrest, are unreasonable under the Fourth Amendment of the United States Constitution.

This policy addresses Baltimore Police Department (BPD) issued and privately owned cell phones of sworn and civilian employees, who have recorded events, which might contain evidence.

Employee Privacy Advisory

1. Employees DO NOT have any reasonable expectation of privacy when using any BPD issued communications device. The BPD retains the right to monitor the content of all communications and the usage of any BPD issued personal communications device.

2. BPD supervisors may access without notice: data or text caches, pager memory banks, and voice mail boxes or accounts and other employer-provided electronic storage systems where there are reasonable grounds to believe a search is necessary for either non-investigatory work-related purpose or for the investigation of work-related misconduct. See Policy 1307, *Personal Communication Devices*.

REQUIRED ACTION

Member

Cell Phone / Personal Communication Device / Tablet

In keeping with this ruling, members must obtain a search warrant prior to a search of a cell phone, when an exigent circumstance is not present.

1. When recovering a cell phone from an individual:

   1.1. Do not allow anyone to manipulate the phone, if possible.

   1.2. Try to determine if the phone is protected by any type of security lock or if it is encrypted. If so, try to obtain the code. Do not assume the security lock can be defeated.

1.3. Cell phones must not be accessed by someone who is not properly trained to extract digital evidence, if the evidence is going to be discoverable.

NOTE: Today's phones have numeric pass codes and/or passwords, facial recognition (which will only unlock by detecting the owner's face), signature locks which recognize the owner's handwriting, encryption (data within the phone is unreadable without the encryption key), and can be remotely locked and/or wiped from a laptop personal computer or another phone in a matter of one minute. If possible, have the owner remove the security lock before examination.

2. Submitting cell phones to Cyber and Electronic Crimes Unit for examination :

2.1. If you are seizing a phone/tablet in the field:

2.1.1. If it is off, leave it off. Remove the battery.

2.1.2. If it is on, remove the battery.

2.1.3. Do not attempt to manipulate the phone (ie, guess the password, look at photos, thumb through the phone, or power it on). These actions can cause the phone to be locked, wiped, and are sometimes recorded by the phone which will conflict with any search warrant later written.

2.1.4. If you are unable to turn the phone off or remove the battery for any reason, (eg, bio-hazard), request the Crime Laboratory Section to recover the device with the use of a Faraday Bag or Arson Can.

2.1.4.1. If the phone is bio-hazard, label it according to the Evidence Control Unit's guidelines and make a note of this on the Cyber and Electronic Crimes Unit request form.

NOTE: Given the nature of the bio-hazard, the Cyber and Electronic Crimes Unit might not be able to examine the phone due to the risk of contamination of the equipment and the risk of cross contaminating other devices awaiting examination.

3. When submitting phones to the Evidence Control Unit, which are to be examined later by the Cyber and Electronic Crimes Unit:

3.1. Submit no more than one device in either a yellow evidence envelope, an Arson Can and/or a Faraday Bag.

3.2. Only submit the device and any USB/power cords that come with the phone. NO OTHER PROPERTY OR EVIDENCE.

3.3. If necessary, submit the device to the Trace Laboratory before submitting a request to the Cyber and Electronic Crimes Unit.

ASSOCIATED POLICIES

Policy 1016, *Citizen Observation/Recording Of Officers*
Policy1307, *Personal Communication Devices*

RESCISSION

Remove and destroy/recycle Policy 1017, *Cell Phone Searches* date 31 October 2014.

COMMUNICATION OF POLICY

This policy is effective on the date listed herein. Each employee is responsible for complying with the contents of this policy.