DENVER POLICE DEPARTMENT

Training Bulletin

ROBERT C. WHITE, CHIEF OF POLICE

Date of issue: May 15, 2015 *(revised/reviewed city attorney's office)*
Original Date of issue: June 3, 2012 (revised July 1, 2014)
Source: Detective Chuck Boyles / Detective Alfonso Cervera, Investigative Technology Bureau
Lamar Sims, Denver District Attorney's Office

CELL PHONE AND TABLET DATA EXTRACTIONS FOR ALL INVESTIGATIONS AND FOR ALL PERSONS IN POSSESSION OF A CELL PHONE OR TABLET

The United States Supreme Court issued its opinion in Riley v. California, *slip. Op.* June 25, 2014, a case addressing the "search incident to arrest" doctrine as it relates to cell phones found on an arrestee. The Court observed: "Modern cell phones are not just another technological convenience. With all they contain and all they may review, they hold for many Americans 'the privacies of life.'" *Riley* at 28. The Court ruled:

> *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. Ibid.*

Denver Police Department policy incorporates the holding of *Riley*, and extends it to include any party from whom a cell phone or tablet is seized, but who may not be an arrestee, including, but not limited to, third party witnesses. Before an officer views or extracts cell phone or tablet data during the course of a criminal or administrative investigation, he or she will obtain a search warrant or "signed written consent". The policy establishes department preference for obtaining a search warrant in these matters. DPD also incorporates and extends *Riley's* prohibition against officers "scrolling" through an arrestee's, or any other person's cell phone or tablet in an attempt to recover incriminating evidence without written consent or a warrant.

The term investigation refers to both administrative and criminal investigations. Administrative investigations include, but are not limited to, Use of Force investigations and Internal Affairs investigations.

There are rare situations when exigent circumstances may exist. Exigencies will be closely scrutinized by the courts based on the language cited below:

> In light of the availability of the exigent circumstances exception, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone. The defendants here recognize – indeed, they stress – that such fact-specific threats may justify a warrantless search of cell phone data. [Citation to record.] The critical point is that, unlike the search incident to arrest exception, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case. *Riley v. California*, 573 U.S. ___(2014).

With the wide use of cell phones and tablet devices ***cellular data, digital data and or call detail records typically exists in every investigation.*** This recovered data may provide important evidence to an investigation. This can range from text messages, phone call logs, pictures with GPS locations, as well as location data if a phone or tablet was used at or in the area of a location of interest.

The Denver Police Department – Investigative Technology Bureau (ITB) assists in these investigations by the use of the Cellebrite UFED (Universal Forensic Extraction Device) which extracts the data in a secure forensically sound manner.

What is required to View and Extract Cell Phone or Tablet Data Content:

- Either a search warrant - preferred but not required;
- Or a signed written consent to search form – specific to cell phone or tablet device is required for all extractions.
  - Verbal consent or a normal written consent form will not suffice for any data extractions.
    - Contact ITB for cell phone or tablet device consent form

- It is acceptable to locate the phone or tablet model, serial number, IMEI, IMSI, MEID or HEX (identifying phone information) listed under the battery/back cover to list on the warrant or consent.

➢ ***Data extractions will not be conducted without a search warrant, written cell phone consent or appropriate legal authority.***

Seizing of a cell phone or tablet device:

- ✓ Isolate phone or tablet from cellular or WIFI (wireless) network by turning off or removing the battery to prevent remote data deletion.
- ✓ If possible seize any attached charger or cables.
- ✓ Take precautions to not accidentally alter or create data by dialing or viewing, picture or text messaging features on the phone or tablet – ***Digital data is created indicating a file, picture or text message was viewed, accessed or created.***
- ✓ Contact the Investigative Technology Bureau if immediate data extraction is needed, with appropriate legal authority.

What data can be extracted with the Cellebrite UFED:

- Device Information – Phone Number, IMEI, IMSI, MEID, ESN & MAC ID (identifying device info.)
- Phonebook – Contact Name and Numbers
- Call Logs
- Text and Picture Messages
- Videos and Pictures (in some cases with GeoTag-location info) and creation date and time
- Audio Files
- Emails and Web Browsing Information (in some devices)
- GPS and Location Information (in some devices)
- Social Networking messages and contacts (in some devices)
- Deleted Data – Call Logs, Messages, Emails (in some devices)
- PIN Locked and Pattern Locked Bypass & Data Extraction – (on some devices – not all phones bypassed)
- Attached Media or memory card extraction (Pictures, files, app data – located on media card)
- Wireless (WI-FI) networks connected to the device (can assist in localizing a phone to a specific area)

Process to extract cell phone and tablet data:

- ➢ Contact ITB detectives to verify the phone or tablet is supported for data extraction.
- ➢ Schedule the data extraction prior to having the search warrant signed. This will ensure the search is completed within the duration of the search warrant.
- ➢ Obtain any passwords or passcodes to access a locked phone or tablet if possible.
  - Some locked devices cannot be bypassed for data extraction without a password or passcode.

What can be done if the data needed was not supported by the Cellebrite Extraction:

- ➢ In these cases manual photo documentation of each individual item of interest – "text message, pictures, calls logs, etc.", can be performed by the submitting detective or with the assistance of ITB detectives.
- ➢ This will be done only with the submitting detective present. The case detective's participation is required to identify what items may be evidence to the investigation.
- ➢ ITB Detectives will not photograph the entire contents of the phone or tablet due to this time consuming process.
- ➢ In these cases the phone or tablet can be retained as evidence for the duration of the investigation or case.
  - Detectives can also contact the Rocky Mountain Regional Computer Forensics Lab (RMRCFL) to see if the device can be extracted by other tools available at the RMRCFL.

Cellebrite Report

The Cellebrite extraction will produce a report that can be viewed on any web browser on most computers. The submitting detective will receive a disc containing the report of the data extraction for submission as evidence.

Please contact ITB Detective Chuck Boyles 5 or Detective John Medford , with questions or further assistance.