SEARCH WARRANTS FOR DIGITAL STORAGE DEVICES & EVIDENCE

Presented By:

Casey Silvia
Captain, Search Warrant Team

Jamie Michael Charles
Deputy Captain, Search Warrant Team

DIGITAL STORAGE DEVICES

Digital storage devices include:

- Cell phones
- Computers
- iPads & tablets
- Digital cameras
- GPS (global positioning system) device
- External hard drives
- CDs, DVDs, USB thumb drives

GENERAL PRINCIPLES

- Always need a search warrant to enter into or access a digital storage device UNLESS warrant exception applies
- NOT enough that someone is suspected of a crime and has a cell phone!!
- Requirements:
  - Probable cause of a ***crime***
  - Probable cause that there is ***evidence*** related to the crime
  - Probable cause that the ***evidence will be found*** in the location to be searched

GENERAL PRINCIPLES

- Recently, SJC & other courts have dismissed the McDermott container analogy
    - Riley v. California questions this analogy
    - SJC acknowledges distinction in CW v. Dorelas, 473 Mass. 496 (2016)
- Large amount of data on digital devices render them "distinct from the closed containers regularly seen in the physical world"

    - CW v. Broom, 474 Mass. 486 (2016)

GENERAL PRINCIPLES

- Search warrants for digital devices must be conducted with "special care and satisfy a more narrow and demanding standard"
- Per Dorelas, "a computer search may be as extensive as *reasonably* required to locate the items described in the warrant"

PROBABLE CAUSE FOR DIGITAL EVIDENCE

- Generally no different than other cases
- Authorities can use circumstantial evidence, eyewitness accounts, CI's, etc.
- Boilerplate alone does not establish probable cause (see Broom, 474 Mass. at 497)
- However, training & experience is IMPORTANT
  - Explains forensic search/analysis methods
  - Likely to contain explanation of relevant digital media

SEARCH METHOD

- Particularity requirement is that authorities describe what they will search for and seize
- Appears to be heightened in post-Dorelas world
- Does not generally require description of how authorities will locate the evidence
- *Exceptions:*
  - Privilege protocol situations (governed by Preventive Medicine v. CW, 465 Mass. 810 (2013))

PARTICULARITY REQUIREMENT

- ‘Documents’ includes digital documents
- ON THE FACE OF THE WARRANT (description in affidavit is not sufficient)
- Look for particular detail with regard to:
  - Identification of technical devices
  - Date descriptions
  - File/document types
  - Specific parties/contents
- But note, per McDermott files can/may need to be summarily reviewed

PARTICULARITY REQUIREMENT

- Always particularly describe the target matter by subject matter, e.g., “child pornography,” “drug ledger” or “records involving purchase and sales of narcotics,” “photographs of X,” “information regarding relationship between X and Y.”

- Where possible that evidence may be in physical or digital form, you can describe the evidence a bit more generally by stating “in paper or digital format” and ask permission to search any devices seized.

STALENESS

- Rarely a significant issue with digital evidence
- Consider:
  - Nature of offense
  - Nature of evidence
  - Nature of offender
- Evidence can be retrieved if deleted
  - BUT: do not forget to include boilerplate language explaining why this is the case in your affidavit

SEARCHING DIGITAL STORAGE DEVICES: ONE V. TWO WARRANTS

- With one warrant, asking permission to remove electronic storage device from a particular location and also to enter that device to search for evidence of the crime
  - Appropriate where central focus of warrant is digital evidence or evidence most likely to be found in digital format
- With two warrants, asking permission to search previously seized electronic storage device for particularized evidence
  - Appropriate where:
    - Digital devices are one subset of a larger search request; or
    - Further information comes to light during and/or following seizure of digital devices

HOW TO SEIZE A COMPUTER

- If the computer is turned off, leave it off.
- If the computer is on, photograph the screen, then unplug it.
- When you seize a laptop, remove the battery.
- Photograph important information, such as serial numbers, connection points, etc.
- If you have questions during execution, call a forensic examiner – they will walk you through it.
- Remember to document your steps!

CHECK FOR WIRELESS ROUTERS

- An affidavit in support of a search warrant needs to show a nexus between criminal activity and the place to be searched.
- Anyone can access an unsecured wireless router and all connections to that router will have the same IP (internet protocol) address.
- To avoid a later claim of lack of nexus on the ground that someone else logged onto the suspect's unsecured router, conduct surveillance and check for wireless networks in the area.

CIVILIAN ASSISTANCE

- Frequently needed in digital evidence sphere
- SJC concluded that such assistance "actually enhances the reasonableness of the search by lessening its intrusiveness"
- Affidavit may include paragraph requesting civilian assistance
- But: no requirement that affidavit/warrant specify particular individual or entity

ON SITE PREVIEW

- Can investigators preview? ***Yes***
- Should language to preview be in the warrant? ***Not necessarily***
- Must all searching take place on site? ***No***
- Should all searching take place on site? ***No***
- See McDermott, 448 Mass. 750 (2007)
- Note: arrange for civilian/law enforcement analyst to be present in advance

SEARCH WARRANT RETURN

- General Laws c. 276, §§ 2 & 3A
- Examination can continue beyond 7 days
- However, Ericson holds that authorities must 'attempt to complete' examination within 7 days
  - This means the device must be *submitted* for forensic evaluation within 7 days
  - State in the affidavit if the examination cannot be completed in 7 days and why (e.g., due to a backlog or software issues). Include this information in the return along with the date the device was delivered to the forensic examiner

REDACTION OF PERSONAL INFORMATION

- Search warrant documents become public upon the filing of the return.
- If the warrant pertains to evidence of a *rape or sexual assault*, coordinate with an ADA about redacting the victim's identifying information before making the return.
- Do not include *personal identifying information*, such as bank account numbers or a SSN in the affidavit unless necessary. If this information is included in the affidavit, coordinate with an ADA to redact it before making the return.

SEARCH WARRANTS FOR DIGITAL STORAGE DEVICES & EVIDENCE

SPECIAL CONSIDERATIONS FOR

DIGITAL DEVICE SEARCHES & WARRANTS

SEARCHES INCIDENT TO ARREST

- In Riley v. California, 134 S. Ct. 2473 (2014), the United States Supreme Court said:
  - Police are required to get a SW to examine any cell phone, including even simple examination of call lists
  - Exception only in cases of genuine emergency

- No "Search Incident to Arrest" justification
  - Reverses Commonwealth v. Phifer, 463 Mass. 790 (2012), which was the Massachusetts SJC case that permitted search of recent call list for evidence relating to arrestable offense.

SEARCHES INCIDENT TO ARREST

- In the **rare** event of an *exigency*, such as a missing child or information that the phone will be imminently remotely wiped, you may search the phone without a warrant.
- If there is no exigency:
  - You may secure the phone/preserve evidence while you seek a warrant by turning it off and removing the battery — this will avoid remote wiping.
  - If the phone is unlocked, you may try to disable the auto-lock feature.
  - Plain view (i.e., ringing phone identifying caller)

THE RINGING PHONE

- Do not answer a seized cell phone, unless:
  - A search warrant has been obtained
  - Or answering is justified by:
    - Officer safety
    - Exigency: safety of persons or destruction of evidence
    - It is plausibly evidence of crime for which officers are already aware (likely probable cause)
  - Remember to DOCUMENT all justifications, facts, and inferences

LOCKED PHONES (AND OTHER DIGITAL DEVICES)

The New Normal

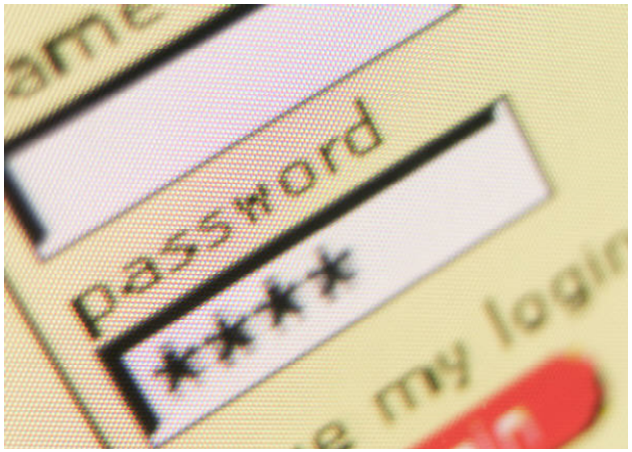
- Phone lawfully seized
- Probable cause for content
- Search warrant issued for search

BUT

- Phone is locked with PIN code
- Forensic software cannot bypass PIN code
- Apple will no longer help (iOS 8.0 & beyond)

COMPELLING PASSWORDS

- CW v. Gelfgatt, 468 Mass. 512 (2014)
- Law enforcement can compel a suspect to give up encryption keys…
- So long as it is a foregone conclusion that the evidence is there



- What does foregone conclusion mean?

FOREGONE CONCLUSION

"[W]hen the Commonwealth seeks a Gelfgatt order compelling a defendant to decrypt an electronic device . . . art. 12 requires that, for the foregone conclusion to apply, the Commonwealth must prove **beyond a reasonable doubt that the defendant knows the password**."

Commonwealth v. Jones, SJC-12564 (March 6, 2019)

How do we demonstrate such knowledge?

- Observe/document behavior prior to digital device seizure
- When possible, engage suspect in questioning that tends to suggest possession/use
- Request general info from device that will induce suspect to unlock
- If suspect offered phone call, suggest they use their phone

CONTENTS OF E-MAILS

You have probable cause to believe that the suspect's email account contains evidence of the crime. Should you apply for a search warrant?

Yes, but —

- Protect possible attorney-client communications if,
  - Target has *any* open case, or
  - Reason to believe target has retained counsel regarding investigation

SEARCH FOR E-MAILS

In Preventive Medicine Associates, Inc. v. CW,

465 Mass. 810 (2013), the SJC set out this new procedure:

- Must apply for the warrant in Superior Court
- Include specific information in the affidavit (target has open case, nature and scope of open case, relationship between SW and open case, and why SW necessary)
- Recruit ADAs uninvolved in the investigation form a "taint team" to review the search results to ensure that privileged communications are not disclosed
- Defendant has opportunity to be heard regarding this review process

SEARCH FOR E-MAILS

- If the Suspect has a pending case, these rules apply regardless of whether the **e-mails are dated before or after the indictment**.

- These rules may apply to **people who do not have an open case** – for example, “an uncharged person who is the target of an ongoing criminal investigation and who is known by the Commonwealth to have retained counsel in connection with that investigation.”

- It does not matter that you are searching the emails pursuant to an investigation that is **totally unrelated to the pending case**. For example, you may be investigating a P2P child pornography case and the suspect may have a pending OUI.