ELECTRONIC FRONTIER FOUNDATION

Digital Device Searches

A Guide for Criminal Defense Attorneys

EFF One-Pager
Revised 4.25.18

Support our work on Digital Device Searches: eff.org/donate

What are they?

- Device searches are examinations of data stored on devices that use a computer or microcontroller to record digital information. Most frequently, these searches involve cell phones, tablets, laptops, or desktop computers, but could conceivably include any type of electronic device, like medical devices such as pacemakers, hearing aids, heart-rate monitors, or smartwatches.

How do they work?

- Digital device searches may occur manually (looking through data on the device as a user would) or forensically (with assistance from other computers or software).
- Forensic device searches typically occur in 2 steps:
    1. "Imaging" – after physically seizing a device, law enforcement makes a complete digital copy, or "image," of all information on the device
    2. "Analysis"– the government uses forensic software to examine the digital copy of the device, allowing the government to organize, methodically search, and view data on the device, including data the user may have believed was deleted.

What are DOJ Guidelines for Executing Digital Device Searches?

1. 1994 NIJ guide on Forensic Examination of digital evidence: https://eff.org/DOJNIJ1994
2. 2009 DOJ CCIPS Criminal Division Manual on Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations: https://eff.org/DOJDSM2009
3. 2011 DOJ Guide on admitting Electronic Evidence: https://eff.org/DOJOAEE

What Programs Do the Cops Use?

Police use a variety of forensic extraction programs like: Cellebrite, Securview, Oxygen, FTK Imager, or Encase, that have the capacity to collect metadata and content, help bypass encryption, classify images, restore deleted data, track GPS locations over time, search for specific keywords, and map relationships.

How Do I Challenge Digital Device Searches?

- Digital device searches require a warrant. *See* Riley v. California, 134 S.Ct. 2473 (2014).
- Even if a warrant was obtained, there may still be grounds for suppression. Many warrants are boilerplate, so challenge them where they:
    1. Lack specificity/particularity about the object of the search and place(s) to be searched.
        a. Warrants should be as specific as possible about the files to be searched and the locations on a device where those files are likely to be located.
        b. Where the govt uses the device to access content stored remotely in the "cloud," object if remote data is not specifically mentioned as an object of the warrant or isn't within the scope of PC articulated in the SW affidavit.
    2. Lack Probable Cause – e.g., lacking a nexus between the device seized and the specific suspect/incident being investigated.
    3. Are overbroad in scope: Make objections to the initial seizure based on the threshold factors identified in U.S. v. Griffith, 867 F.3d 1265, 1272-1273, (DC Cir. 2017): that client own, use, or possess a device, that it will be found in a particular place at a particular time (like the client's home), and that it contains incriminating evidence about the suspected offense
- Rely on more privacy-protective CalECPA state law, which requires notice contemporaneous with execution; for the SW to specify time period(s) and target individual(s); and provides a statutory suppression remedy for failure to comply with state law (CA Penal Code §§1546.1-.2)
- If you are able to intervene prior to the search of your client's device, advocate for specific limitations on the scope of any search, like requiring:
    1. Govt must waive reliance upon the plain view doctrine;
    2. Forensic analysis must be done by specialized personnel or an independent 3rd party;
    3. Govt must disclose actual risks of destruction & other avenues of access;
    4. Search protocol must be designed to seize only info for which govt has PC;
    5. Govt must destroy or return non-responsive data; *see* U.S. v. Comprehensive Drug Testing, Inc (CDT), 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, J. concurring).
- Review digital search cases within your jurisdiction:
    1. *US v. Flores*, 802 F.3d 1028 (9th Cir 2015) – Court approved search of 11k pages of FB data, even where only 100 were responsive to SW
    2. *US v. Garcia-Alvarez* (S.D. CA 2015) - Judge Miller refused to limit cell phone search to "recent data" because govt had no evidence smuggling was only recent
    3. *US v. Nazemzadeh* (S.D. CA 2013) – Judge Lorenz approved SW to seize entire email server because govt said on-site search would take too long

Stephanie Lacambra, Criminal Defense Staff Attorney 415-436-9333 x130, stephanie@eff.org