Digital Devices

More than cell phones…

25

Internet of Things [IoT]

- Echo, Google home
- Refrigerators
- Watches and Fitbits
- Smart home devices
- Home surveillance cameras
- Video doorbells
- Kids' toys

26

OTHER DIGITAL DEVICE SOURCES

- Drones
- LPRs
- Gaming devices

VEHICLES – EDRs

Event Data Recorder:

- Records data related to vehicle's speed, direction, etc.
- Based on a tamper-proof, read-write memory device.
- Some continuously record data, overwriting the previous few minutes vehicle stops.
- Others are activated by crash-like events

In-Vehicle Infotainment (IVI)
In-Car Entertainment (ICE)

- Collection of hardware and software in vehicles that provides audio or video entertainment.
- Systems can include steering wheel audio controls and hands-free voice control
- Includes: automotive navigation systems; video players; USB and Bluetooth connectivity; Carputers; In-car internet and WiFi

VEHICLE DATA

What can you get?

- Doors open/closed
- Bluetooth connections
- Gear Shifts
- Lights on/off
- USB attachments
- GPS location data
- Calls made
- Wifi connections
- System reboots

- All or most communications data downloaded when phone is synced to system.
- Doesn't matter if phone is locked or not

Topic 2

You Then Need to Know How to Collect it Properly

31

Search Warrants

Two kinds of search warrants:

General – search warrant to take/seize all mobile devices recovered at a particular location (including associated hardware and storage media).

Specific – search warrant to access/seize all the data in a particular device.

32

Preservation requests to include in general warrant

Ask for authorization to take steps to preserve and safeguard the data in any mobile devices encountered during the search.

- Request to access the phone to put it in airplane mode and turn off WiFi and Bluetooth
  - NOTE: keep phone powered on
- Request on-scene extraction to preserve the data.
- Request authority for biometric unlock

33

PRESERVATION OF RECORDS

- Records from ISPs, social media accounts, email accounts, phone records – all electronic records
- Probable cause NOT required for preservation request
- Preservation requests:
  - Most companies accept preservation requests online
  - If not – send preservation letter immediately

Victim-Witness Devices

- Device(s) belonging to victims and uninvolved witnesses require special privacy protections
- Consent – remember what YOU see, you will likely have to provide to the defense
- Limit search if necessary and document the limitation
- Protective orders for discovery purposes
- Be careful of screenshots – some apps will notify the sender that a screenshot was taken

35

basics related to DE search warrants

Key principles: specificity, probable cause

PARTICULARITY of the location to be searched

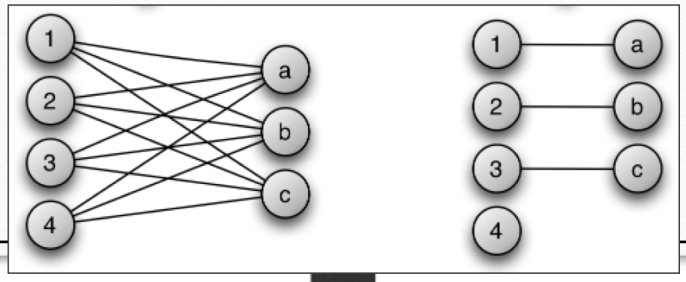
- The easy part – identify the device to be searched or the business entity that you are seeking records from
- If seeking records, list name and address of business, registered agent, and LE portal (if available)
- Search.org – list of ISP providers with contact info

PARTICULARITY of the data you want to receive

- ❖ List all the data you want to want to receive
  - ❖ For records: some data types are consistent between ISPs and some are different, find a good template or check the company's TOS/PP
- ❖ Don't forget data which tends to show possession and control of the device or account

PROBABLE CAUSE

- Reasonable grounds to believe that there is evidence of criminal activity in the location to be searched and the items to be seized.



39

- The need for attribution and authentication can justify a broad search, but…
- *"Any and all data"* IS NOT OK…nor is "including but not limited to…"

Additional Court Orders

- Order for Nondisclosure
  18 U.S.C. §2705
- Order to Not Cancel Account
- Order to Seal
- Order to Delay Notification

41

Topic 3

You Next Need to Know How to Search and Seize the Data

42

PROPERLY PRESERVE THE DEVICE

- Keep it powered on
- Faraday Bag
- Airplane mode on, Bluetooth off, WiFi off

Conditions Affecting Ability to Search

HAZARDS

TRADITIONAL DAMAGE

- Cracked screens can be fixed to allow for manipulation of device

NETWORK CONNECTION

- Separate from network to prevent remote wiping of phone

BIOLOGICAL OR OTHER HAZARDS

- Biological/Chemical
  - Water
  - Blood
  - Flame retardant
- DNA/Fingerprint

Extracting the data

LOGICAL

Uses the phones purpose built interface.

- Fast
- No decoding
- Easy to Access
- Limited Data

FILE SYSTEM

Coping Device's Full File System

- Fast
- More Data Available
- Complex
- Requires Decoding

PHYSICAL

Bit-For-Bit copy of the Internal Memory

- Ultimate amount of Information
- Highly Complex
- Time Consuming
- Requires Decoding

MANUAL

Uses the phones purpose built interface.

- Fast – Exactly what you see
- Easy to Access
- Limited Data
- Often Forgot About

Advanced extraction options

GRAYSHIFT

- iOS Only
- BFU / AFU / etc.

Cellebrite

- Android / iOS
- BFU / AFU / etc.

Advanced extraction options

- JTAG / ISP
- Chip Off
- Nuclear Option

Search of Records

- Electronic records:
  - Preserve the account – AS SOON AS POSSIBLE!
  - Submit a warrant or subpoena for the records
  - Subject the returns to a tool that will ingest the data and provide it in a more readable form

48

FINAL THOUGHTS

CONSIDER:

- What type of evidence is available?
- What is the source of the evidence?
- Do you have access to the evidence or do you need a warrant for it?
- What is the extent of the search authorized by your facts?