Interactive Warm-Up
Interactive Warm-Up (cont.)
1. The Technology Behind Searching a Cell Phone
2. Extraction Reports and a Live Demonstration
3. Cell Phone Search Warrant Issues
4. Cellular Network Basics
5. Carpenter and Historical Cell-Site Location Information
6. Real-time Tracking
The Technology Behind Searching a Cell Phone

WHAT CAN BE DONE AND HOW
Cellebrite UFED Touch2

- Cellebrite is a digital forensics company specializing in mobile devices (i.e. cell phones and tablets)
- UFED = Universal Forensic Extraction Device
Extractions

- Extraction - The process of obtaining mobile device data and storing it in an approved location for processing

- Three Main Extraction Types
  - Physical
  - Logical
  - File System

- The type of Extraction that can be performed depends on the device, its operating system, and the status of the device
Cellebrite Advanced Services

- Cellebrite Advanced Services (CAS)
  - Formerly Cellebrite Advanced Investigative Services (CAIS)
- Unlocks phones that the available software and hardware cannot
  - Most notably new iPhones and Samsung Galaxies up to S8+
- $1,500 per phone or $250,000 a year subscription
- Requires a warrant
- Secret process performed at Cellebrite’s lab
- Frye Challenge
GrayKey is made by Grayshift, a competitor to Cellebrite

- Unlocks previously unlockable phones like CAS
- Secret process but with a much different approach
  - Product, not a service
- Law enforcement only
- Frye Challenge
Cloud Analyzer

- Cellebrite UFED Cloud Analyzer
- What is “the cloud”? 
- Common “cloud” services 
  - iCloud, Dropbox, Google Drive, etc.
- Email and Social Media 
  - Gmail, Yahoo, Facebook, Twitter, etc.
- Broken phone?...was it backed up to iCloud or Google?
- Even more invasive than an unrestricted search of a phone
JTAG/Chip-Off

- JTAG (Joint Test Action Group)
  - An extraction procedure which involves connecting to the Standard Test Access Port (TAPs) on a phone and transferring data stored on the phone’s memory chip.

- Chip-Off
  - An extraction procedure which requires physically removing the phone’s chip and using an external specialized reader to read the data.
Extraction Reports and a Live Demonstration

WHY THE FORMAT OF RECEIVING THE DATA/INFORMATION MATTERS
Type of Reports

- Extraction, extraction, extraction – This is what we need
- UFED Reader Report – Temporarily Acceptable
- PDF – Not Acceptable
- Printed out copy – Absolutely not acceptable
- Why is this important?
Live UFED Reader Demonstration

*Fingers crossed we have no issues*
<table>
<thead>
<tr>
<th>Date</th>
<th>Type</th>
<th>Description</th>
<th>Timestamp</th>
<th>Source file information</th>
<th>Extracted</th>
<th>Physical</th>
<th>Powering Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/15/2014</td>
<td>SMS Messages</td>
<td>10/15/2014 4:46:28 PM (UTC-4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11/11/2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/9/2015</td>
<td>SMS Messages</td>
<td>4/9/2015 3:44:42 PM (UTC+2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/22/2015</td>
<td>SMS Messages</td>
<td>4/22/2015 5:23:59 AM (UTC+2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5/1/2015</td>
<td>Powering Events</td>
<td>5/1/2015 5:42:33 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Extracted Photo Metadata Example
Cell Phone Search
Warrant Issues

FREQUENT ISSUES PRESENT IN MANY CELL PHONE SEARCH WARRANTS
YOU ARE FURTHER AUTHORIZED to download, copy, and search all of the contents of the Target Cellular Telephone for data and information stored therein, to the extent reasonably necessary to ascertain whether it contains records of the type described herein above.

You are therefore commanded to make an immediate search, including downloading of all data and information contained therein, of:

IT IS FURTHER ORDERED that a search of all files and data stored in the target devices is authorized, irrespective of how the data is filed, labeled, designated, encrypted, hidden, disguised or otherwise stored.
a. any and all records, data and documents related to the commission of the above-mentioned crime including, but not limited to, stored electronic communications, data, information and images;

b. any and all records and other evidence of proceeds related to the commission of the above-mentioned crimes, including but not limited to documents and records in any format including, but not limited to, stored electronic communications, data, information and images, such as cash transactions or financial transfers derived from the possession of cash, currency, money orders, bank receipts, stocks, bonds, bills and receipts for goods and services, documents relating to real estate holdings and other property, and any title or registration to motor vehicles, or other financial receipts, and records;

c. any and all records, however created or stored, which tend to demonstrate ownership and use of the Target Devices, and identification bearing the name or photograph of any person, telephone-books, address books, date books, calendars, personal papers, and photographs of persons contained in the Target Devices;

d. data, information, and images, including but not limited to names, nicknames, addresses, e-mail addresses, numbers (including telephone numbers and bank account numbers), letters, symbols, stored messages (e-mails, voice and/or text), photographic images, notes, correspondence, instructions, and orders contained in the Target Devices;

e. any and all evidence tending to implicate yet-to-be identified accomplices or conspirators in the above-mentioned crimes; and

f. any and all evidence showing or tending to show the identity of the maker or user of the data and information contained in the Target Devices, such as passwords, sign-on codes, and program design.
“1. Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.

2. Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.

3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.

4. The government’s search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.

5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.”
People v Brown, 96 NY2d 80 [2001] – Severance

Groh v Ramirez, 540 US 551 [2004] – the SW application cannot save an overbroad SW


United States v Griffith, 867 F3d 1265 [DC Cir 2017]

People v Covlin, 58 Misc3d 996 [Sup Ct, NY Co 2018]
CPL 690.30(1): “A search warrant must be executed not more than ten days after the date of issuance and it must thereafter be returned to the court without unnecessary delay.”

People v Jacobowitz, 89 AD2d 625 [2d Dept 1982]
People v Kiah, 156 AD3d 1054 [3d Dept 2017]

IT IS FURTHER ORDERED that, for purposes of the requirement that a search warrant be executed within ten days as mandated by C.P.L. Section 690.30(1), the warrant be deemed executed upon the initial accessing of the Target Device for the purpose of beginning a forensic search pursuant to the warrant, and that the search may continue thereafter for whatever reasonable time is necessary to complete a thorough search pursuant to the warrant.
Cellular Network Basics

HOW DOES A CELL PHONE WORK? HOW ARE CALL DETAIL RECORDS USED?
How Does a Cell Phone Communicate with Other Phones?

- Transmitting and Receiving
- Cellular networks are connected to the plain old telephone system
- Cell Towers (Base Stations)
  - Sectors
  - Azimuth
  - Overlapping Coverage
  - Handoff
- How does your phone choose a tower?
  - The Strongest Signal
Cell Phone Towers

2014 T-MOBILE TOWERS MAPPED FOR MANHATTAN
Call Detail Records Mapping Example
Carpenter & Historical Cell-Site Location Information
The Third-Party Doctrine

  - The Court held that the seizure of the defendant’s bank records via a government subpoena did not violate his Fourth Amendment rights. The majority concluded Miller had no right to privacy in his bank records because he voluntarily gave them to a third party (i.e. the bank), who then provided the records to the government.

- **Smith v Maryland**, 442 US 735 [1979]
  - The Court found that the use of a pen register without a warrant did not constitute a Fourth Amendment violation. The Court decided that a person did not have a reasonable expectation of privacy in the telephone numbers recorded by a pen register because the dialed numbers were regularly and voluntarily supplied to the telephone companies by the customer to be used in the regular course of the phone company’s business.
The Road to Carpenter: The Dawn of the Fourth Amendment in the Digital Age

- **People v Weaver**, 12 NY3d 433 [2009]
  - Warrant required for GPS device tracking (NY State Constitution)
- **US v Jones**, 565 US 400 [2012]
  - Warrant required for GPS device tracking
- **Riley v California**, 134 SCt 2473 [2014]
  - Warrant required to search a cell phone
- **Carpenter v US**, 138 S Ct 2206 [2018]
  - Warrant required to “search” and “seize” historical CSLI
“Disclosed in the data retrieved from the transmitting unit, nearly instantaneously with the press of a button on the highly portable receiving unit, will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on. What the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits.” Weaver at 441-442.
TheStoredCommunicationsActstandard(18USC2703(d))

- "...specific and articulable facts showing that there are reasonable grounds to believe...the records or other information sought, are relevant and material to an ongoing criminal investigation."

- "Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in Jones or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search." Carpenter at 2216.
Limitations and Undecided Issues

- Exigent circumstances
- Seven or more days
- Tower Dumps
- Real-time tracking
- Foreign Affairs and National Security
- When does the search and seizure take place?
  - What constitutes the search and/or the seizure?
- “We hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party.” Carpenter at 2222.
Katz Test is supplemental

5 Part Test

1. Bailment
2. Complete ownership or exclusive control of property is not always a necessary condition to the assertion of a Fourth Amendment right.
3. Positive law can be informative
4. A “constitutional floor”: Positive law cannot diminish a Fourth Amendment right
5. Subpoenas cannot typically be used to circumvent the Fourth Amendment

Positive law “typically consists of enacted law — the codes, statutes, and regulations that are applied and enforced in the courts.” POSITIVE LAW, Black’s Law Dictionary (10th ed. 2014)
How Do I Know Which Company to Subpoena?

- Ask the person whose phone it is – Not always an option
- Law enforcement databases – Law enforcement only
- Commercial databases (CLEAR, Accurint, etc.) – Cost money, limitations
- CarrierLookup.com – Free
- FreeCarrierLookup.com – Free
Real-Time Tracking

GPS PINGING, A-GPS, AND CELL-SITE SIMULATORS
GPS Pinging

- What is GPS?
- The Enhanced 911 (E-911) System?
  - Location improvement to the traditional 911 system
- Using E-911 to ping a phone
- Forcing the phone to transmit GPS data
- Real-Time Tracking
- Does the Third-Party Doctrine apply?
# Pinging Report

## GPS Location Alert

<table>
<thead>
<tr>
<th>Type</th>
<th>Received Time</th>
<th>Email Time</th>
<th>Latitude</th>
<th>Longitude</th>
<th>Radius</th>
<th>Google link</th>
</tr>
</thead>
</table>
From: <TelAlert>
Date: 
To: <>
Subject: Tel Alert

E911 Location Updated
Target: 917
Target Name:
Switch time: 2017 09:29:55.0
Latitude: 40.
Longitude: -73.
Radius: 21.0

Link to map: http://maps.google.com/?q=
GPS Pinging Case Law

- People v. Moorer, 39 Misc3d 603 [Co Ct, Monroe Co 2013]
- People v. Wells, 45 Misc3d 793 [Sup Ct, Queens Co 2014]
- People v. Watkins, 125 AD3d 1364 [4th Dept 2015]
- US v. Lambis, 197 FSupp3d 606 [SDNY 2016]
- People v. Hernandez, 56 Misc3d 586 [Sup Ct, Kings Co 2017]
- People v. Gordon, 2017 NY Slip Op 27364 [Sup Ct, Kings Co 2017]
- People v. McDuffie, 58 Misc3d 524 [Sup Ct, Kings Co 2017]
A-GPS and Find My iPhone

- A-GPS = Assisted GPS or Assisted Global Positioning System
- Designed to limit the errors associated with regular GPS
- Find My iPhone uses A-GPS
  - GPS
  - Cell Phone Towers
  - Wireless Connection Databases
- Wireless Connection Databases?
Find My iPhone Test
Cell Site Simulators (aka Stingray Devices)

- Cell site simulators are devices that pretend to be cell phone towers
- How are they used?
- What is the controversy?
  - Secrecy
  - Pen register orders vs. Warrants
- Third-Party Doctrine
- *US v Lambis*, 197 FSupp3d 606, 616 [SDNY 2016]
- *People v Gordon*, 58 Misc3d 544 [Sup Ct, Kings Co 2017]
Contact Information

Jerome D. Greco
(212) 298-3075
JGreco@legal-aid.org

Legal Aid Society
49 Thomas Street
New York, NY 10013