# LEGAL PROCESS FOR OBTAINING INFO FROM CELL PHONE & ISPs

Presented By:

Casey Silvia
Captain, Search Warrant Team

Jamie Michael Charles
Deputy Captain, Search Warrant Team

# OBTAINING NETWORK PROVIDER RECORDS

- Two categories:
  - Phone companies (Verizon, Sprint, T-Mobile, etc.)
  - ISP providers (Facebook, Yahoo, Google, etc.)
- Do you need a SEARCH WARRANT?
  - SW necessary: data that contains the substance of a communication (e.g. voicemail, e-mail, text messages, photo), any real-time capture of communications or tracking of a person's movements using their own device, or the history of a person's continuous movement for a period longer than 6 hours (e.g. historic cell site records)
  - SW is not necessary: information that does not contain the substance of a communication in any form (e.g. subscriber info, customer care records, toll records) or a history of tracking a person's movements for less than 6 hours

# STEP ONE: PRESERVATION/FREEZE LETTERS

- Preserve the records you want ASAP
- Use sample letter & submit by fax or e-mail
- Preservation request lasts 90 days
- Can renew for additional 90 days

# SUBSCRIBER NOTIFICATION

- Typically, will want to request company NOT notify subscriber
  - 18 USC § 2703(c)(2) does not require notification
  - However, many providers will notify
- Insert language into body of affidavit
  - works with phone companies
  - does not typically work with internet companies
- If company pushes back, consult an ADA and secure judicial order from a judge

# STEP TWO: CONTENT v. NON-CONTENT

- Usually the key distinction in determining whether warrant necessary
- All content information requires
  - A showing of probable cause, and
  - Search Warrant authorizing seizure
- People have a heightened expectation of privacy in the content of their communications

# EXAMPLES
# CONTENT v. NON-CONTENT

- Content (SW required)
  - Emails
  - Text messages
  - Videos
  - Photographs
  - Postings
  - Chats
- Non-Content (Subpoena sufficient)
  - Subscriber name, address, DOB, payment method
  - Screen names, User IDs, ISP
  - Records of use: call/text logs, log-ons, IP addresses

# LEGAL PROCESSES FOR OBTAINING INFORMATION

Consider Stage of your Investigation and Nature of Information Sought:

1. **Administrative Subpoena**
2. Grand Jury Subpoena
3. Trial Subpoena
4. **2703(d) Application & Order**
5. Rule 17 Motion & Order
6. **Search Warrant**

# ADMINISTRATIVE SUBOPOENA
# G.L. c. 271, § 17B

## Overview

- What info can you get with an admin subpoena?
  - Non-content subscriber information from phone companies, internet providers, websites, email services, etc.
- How do you get an admin subpoena?
  - Telephone Company requests to SIU
  - Internet Service Provider (ISP) requests to Cyber Protection Unit
- What legal showing is required?
  - Relevant and material to an ongoing criminal investigation

# ADMINISTRATIVE SUBPOENAS

- CAN get non-content subscriber information
  - Name
  - Address
  - Phone number
  - Billing info
  - IP addresses used
  - Call logs, including contact number, time, and duration
  - SMS text logs showing contacts
- CANNOT get content – so no voicemails, text messages, etc.
- Information available from:
  - ❖ Phone companies (e.g., Verizon, AT&T, Sprint, T-Mobile)
  - ❖ ISPs (e.g., Comcast, Verizon)
  - ❖ Email service providers (e.g., Gmail, Hotmail)
  - ❖ Social networking websites (e.g., Facebook, Myspace)
  - ❖ Internet message boards (e.g., Youtube, Craigslist)

# ADMINISTRATIVE SUBPOENAS

- Key Advantages
  - Lower standard – don't need probable cause!
  - Easy availability – obtained without a hearing or a judge/clerk
  - Builds Case for SW (connections among suspects, etc.)
- Key Disadvantages
  - No location information
  - Must be an "ongoing" investigation
    - Cannot be used after suspect arrested or arraigned
    - Exception for continuing a broader investigation

# ADMINISTRATIVE SUBPOENAS

Points of Contact:

Nicholas Fallah, Paralegal, SIU
(781) 897-6719/nicholas.fallah@state.ma.us

Julia Souba, Paralegal, SIU
(781) 897-6717/julia.souba@state.ma.us

# SEARCH WARRANTS FOR CONTENT

1. Cell Phone Content Stored by Carrier
   - Text messages (rare)
   - Voicemails
   - Contacts
   - MUST request preservation IMMEDIATELY even for providers that retain this info – and most don't
2. Internet-Based Communication Services
   - Email providers (Yahoo, Google)
   - Social Networking Sites (Facebook, Instagram, Twitter)
   - Internet Service Providers (Comcast, Verizon)
     - Communications Sent, Received, Stored On-line
       - emails, posts, and other forms of messaging
       - photos, videos, and other stored content
       - history of websites viewed, accessed, edited

# PROBABLE CAUSE FOR CONTENT

Do we have probable cause to believe that

- Phone Records
- Content stored on phone
- Email
- Social media content or activity

will contain evidence of the crime?

**Not enough to say that suspect has a cell phone or a FB account and "experience" makes it likely he used it…need a concrete link that evidence is reasonably like to be found in records. (CW v. Broom, 474 Mass. 486 (2016))

# SCOPE OF SEARCH REQUEST

Now that we have probable cause…

- Limit scope of communications and other files to be searched.
- Only communications and other files that are evidence of the crime.
- Should typically be limited to:
  - Time period
  - Parties involved (useful to identify sender/recipient)
  - Types of content (relationship to crime, etc.)

# OBTAINING GEOGRAPHIC LOCATION INFORMATION

- Historic or Real-Time Location Information
  - Cell Tower Locations
  - GPS
- Generally, tracking a person's movements by converting their own phone/car into a tracking device requires a Search Warrant issued upon a finding of probable cause.
  - NOTE: 18 USC 2703(d) lower standard is sufficient to obtain records in only very limited circumstances. **Check w/ MDAO SW Team if considering 2703(d) order.**

# CELL SITE LOCATION INFORMATION

- Historical location information
- What are cell site locations?
  - Towers/transmitters used by a cellular phone are recorded by service provider.
  - Location can provide a rough estimate of the location of the caller.
- How do you get them?
  - Search Warrant
  - No longer through 18 U.S.C. 2703(d) order except in limited circumstances
- What can we use them for?
  - Showing historical locations and movement over time of user of cellular phone.

# SEARCH WARRANT FOR CSLI

- Limit Request to Relevant Time Period
- Ways to show probable cause for CSLI:
  - Call logs: suspect used phone at key point(s)
  - Observation: suspect had phone on him at time
  - Nature of crime: planning, coordination
  - Value of Location Evidence
    - puts suspect at scene and/or with other suspects
    - corroborate or disprove accounts and timelines
    - identify course of flight, locations for missing evidence, other witnesses or participants

# REAL TIME GEOGRAPHIC INFORMATION

- Two Sources of Information:
  - Real-Time “Pinging” of Cell Phone by Carrier
  - Attaching GPS Unit to Suspect Vehicle

- Both Require a Search Warrant (PC)
  - Narrow Emergency Exception for Pinging
    - suspect in flight
    - immediate risk of death or serious bodily injury

# REAL TIME PINGING

- Carrier Directed to Locate Phone on Network
- Signal Sent by Carrier "Pings" on Closest Tower
- Probable Cause that D's Present Location is Evidence of the Crime?
  - usually used for suspect evading arrest
  - get an arrest warrant first
  - evidence showing D aware that police are pursuing him and has fled

# REAL TIME PINGING

- Must be obtained in Superior Court
- Warrant good for 15 days
- Police must “prompt” carrier to send out pings
- Request 2 weeks of CSLI (historical) to establish patterns of movement

# GPS REAL TIME TRACKING

- GPS Unit Attached to Suspect's Vehicle
- Continuous Updates by Cell Signal
- Shows continuous course of movements
  - not just when "pings" sent
  - not just when calls placed or received
  - downloaded onto hard drive for preservation
- Much more precise than Tower Locations

# COMMONWEALTH V. CONNOLLY

- A court has authority to issue a GPS warrant even where it is not named in G.L. c. 276, § 1
- We need a warrant to install the device
- We need a warrant to monitor
- Depending where car is parked, we may need warrant to gain access to install and maintain (ex. private garage)
- All of these can be obtained from the same warrant – but we need permission for each of these intrusions.

# STANDARD TO OBTAIN GPS TRACKING WARRANT

- Probable Cause to believe that criminal offense has been/is being/or is about to be committed

AND

- Probable Cause that GPS monitoring of vehicle will produce "evidence of such offense or will aid in the apprehension of a person who the applicant has PC to believe has committed/is committing/about to commit such offense."

# GOOD PRACTICE WITH GPS MONITORING

- Not a substitute for surveillance!!
- Adhere to process SJC approved in Connolly
  - Affidavit contained specific info about vehicle, including make/model/plate/VIN.
  - PC to believe the target vehicle was been consistently used in course of continuing criminal conduct AND that GPS monitoring would be likely to produce additional evidence of that criminal conduct
  - Install GPS as soon as possible after obtaining warrant.
- We recommend demonstrating surveillance efforts in affidavit

# GPS REAL TIME TRACKING

- Length of Monitoring: 15 days from issuance.
- Return: Initial return in 7 days/final return in 15 days.
- What to write on the status report:
  - "GPS Unit X was installed on target vehicle on [DATE]. Monitoring will be performed in accordance with the terms of the search warrant. A final return will be submitted at the conclusion of the monitoring period."
- What to write on the final return:
  - "Electronic data on movement of target vehicle was gathered consistent with the terms of the authorizing warrant. A full report of the results will be provided to the defense in the pre-trial discovery process."

# SEARCH WARRANT TEAM CONTACT INFO

SW Daily Duty ADA (Business Hours):

781.897.6825

24 Hour Duty ADA (**Urgent** Matters ONLY on Nights and Weekends):

617.756.3670