Webinar Information

- All attendees will be muted.
- If you desire to ask a question, please use the questions section of the GoToWebinar dialogue box, typically in the upper right corner of the screen.
- Please do not raise your hand for questions we can not unmute you.
- The questions will either be answered directly by a panelist or asked to the presenter who will answer.

Webinar Information

Poll questions may be asked during the webinar. They will be left open only a short period of time so please respond promptly.
Webinar Information

- At the conclusion of the webinar a short survey will appear. Please complete it before signing off.
- A link to view the recorded webinar and the Powerpoint slides will be provided to you via email after the webinar.

Poll Question

- How many cell phone searches have you conducted?

Fourth Amendment

- We know it, kinda.
- What does it mean?
- What questions must we ask?
- What do we need to know?
Fourth Amendment

- Expectation of Privacy
- Smith v. Maryland—no expectation of privacy in phone numbers dialed
- Smartphone has far more information
- Smartphone has multiple examples of “content of communications”
- Safer to treat like a computer

Fourth Amendment

- Warrant Searches
- Warrantless Searches
- Exigent/Hot Pursuit
- Consent
- SIA
- Caretaker
- Plain View/NOT A SEARCH

Federal Privacy Laws

- How can government obtain emails and network account logs from ISP’s?
- When does the government need to obtain a search warrant as opposed to a 2703(d) order or a subpoena?
- When can providers disclose emails and records to the government voluntarily?
- What remedies will courts impose when ECPA violated?
Federal Privacy Laws

- ECPA - The Electronic Communications Privacy Act (18 U.S.C. 2550 et seq)
- PPA - The Privacy Protection Act (42 U.S.C. 20003)
- CCPA - The Cable Communications Policy Act (47 U.S.C. 251 et seq)

Why do I care?

- ECPA – No suppression remedy
  Civil damages, but you lose your job!

- PPA – No suppression remedy
  Civil damages. Law enforcement officers may be held personally liable!

- ECPA – No suppression remedy
  Civil damages, but you lose your job!

- PPA – No suppression remedy
  Civil damages. Law enforcement officers may be held personally liable!
ECPA

- Extends wiretap laws to electronic communications
- Regulates how investigators can obtain stored e-mail, account records or subscriber information from network service providers; IPS’s, phone co.’s, cell phone providers, and satellite services.

ECPA

- ECPA seeks to provide certain privacy rights to network account holders by offering varying degrees of legal protection depending on the perceived value of the privacy interest involved

ECPA

- What type of info is being sought?
  - Basic subscriber info?
  - Transactional records?
  - Content in electronic storage?

- How can you get it?
  - Subpoena?
  - 2703(d) Order?
  - Search warrant?
Basic Subscriber Information

- Gives you only
  - name & address/manner of payment
  - local and LD telephone toll billing records
  - telephone number or other account identifier (such as username or “screen name”)
  - length & type of service provided
- Can get IP number & dates/times for IRC
- Can be obtained through subpoena
- Do not subpoena “all customer records”

Transactional Records

- Not content & not basic subscriber
  - § 2703(c)(1)(B)
- Everything in between
  - audit trails/logs
  - web sites visited
  - identities of e-mail correspondents
  - cell site data from cellular/PCS carriers
- Obtainable with § 2703(d) court order

What are “contents”?

- “Any information concerning the substance, purport, or meaning of that communication.”
- Attached wp files
- Attached picture files
- Subject headers of e-mails
Section 2703(d) Orders

- Articulable facts order
  - “specific and articulable facts showing that there are reasonable grounds to believe that [the requested records] are relevant and material to an ongoing criminal investigation”
- Higher standard than a subpoena, lower than probable cause
- ECPA permits service outside state of issuing district

Opened e-mail

- Do you need a search warrant?
- Subpoena – served with prior notice
- 2703(d) Order – served with notice to subscriber
- Search warrant – no notice to subscriber
- Other stored electronic communications in “electronic storage” more than 180 days (unopened e-mail)

Notification

- Investigators can delay notice for up to 90 days to avoid:
  - flight from prosecution
  - destruction of or tampering with evidence
  - intimidation of potential witnesses
  - seriously jeopardizing an investigation
  - (§ 2705)
- 2703(d) Application and Orders will contain a request for delayed notice – must state why
- Can extend delay additional 90 days
### Preservation Request

- A provider of wire or electronic communication service or a remote computing service, upon request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

### Voluntary Disclosure

- Can you accept information voluntarily disclosed by ISP?
- Providers may monitor and intercept real time communications for purposes of maintaining and protecting their equipment.
- Is the ISP required to disclose such info?

### Privacy Protection Act

“[I]t shall be unlawful . . . to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or similar form of public communication . . .”

- Prohibits use of a search warrant for such materials
- 42 USC 2000aa
Privacy Protection Act

• Provides additional protection to media from law enforcement searches


• Newspaper sued saying LE search violated First Amendment rights of paper

Basic PPA Rule

• Act requires law enforcement to rely on cooperation from Media

• Must use a subpoena
  • Less intrusive means to obtaining evidence
  • Offers better protection to innocent parties

Exceptions

• **Contraband** or fruits or instrumentalities of a crime

• Immediate seizure of materials necessary to prevent death or serious bodily injury

• Probable cause that person possessing such material has committed or is committing a criminal offense
  • Except if mere possession offense
  • Except child pornography
Who is Protected?

- Bulletin boards
- Web pages
- TV stations
- Authors
- Publishers of any medium whose intent is to publish information to the public
  - Includes publishers of legal pornography

Commingled Evidence

- What do you do when both protected material under PPA and contraband are found on same hard drive?
- Can you take computer/cell phone?
- Once you realize that you have protected material what do you do?
- Do you have an affirmative duty to return protected material?

Cell Phones

- THE CLOCK IS TICKING!!
- EVERY SECOND YOU WAIT TO COLLECT EVIDENCE, THE MORE YOU loose!!
Cell Phone Searches

- Warrant
- Exigent
- Incident to Arrest
- Consent

Warrant Searches

- Obviously preferred
- With Warrant burden on defense to quash
- Without warrant burden on us to show reasonableness
- Specificity of records
- Specificity of types of information

Search Warrants

- Include “text messages and MMS including all numbers sent to and received from, date, time, duration and all content related to each message”
- Porting—remember a number that starts on AT&T can move to another service.
- Tracfone—a booster phone. When sending search warrant, ask for “Notes and Footnotes.” Notes and Footnotes will tell you where device purchased, where payments were made and how.
- Booster phones—generally operated by Sprint/Nextel
Exigent

- Contact Carrier for their form
- Insure that you have correct person
- Inquire as to whether provider will accept more than one exigent request
- Insure that you have an “exigency” for the provider
- i.e. Homicide with suspect in wind is not necessarily “exigent”
- May be an exigent circumstance to retrieve information before it is written over—limited memory capacity

Search Incident to Arrest

- May search the arrested person and their immediate area
- Gant is limited to vehicles.
- Cell phone has been held to be “immediately associated with the person of arrestee
- Do the initial search, however, close in time to arrest.
- In California, a 90 minute delay was upheld but in Mass a 30 minute delay was too long.

Consent

- Actual Authority
- Apparent Authority—ask questions!!!
- Scope of Consent—what would resonable person believe could be searched
- Treat like the search of a closed container—tell them you are going to look at the contents of the phone
- One case says looking at pager, didn’t authroize looking at the numbers on the pager
Plain View

- Legal right to be where we see the incriminating evidence
- May need a forensic search of the cell phone.
- Have to consider temporal requirements of that search
- Get a warrant

Cell Phones

- Once you get the phone number:
- Call the carrier ask whether the number was active and billable on their network during the time in question.
- That one phone call will save hours

Cell Phones

- If so, send preservation letter.
- Follow up call to insure receipt.
- Search Warrant to carrier.
Cell Phones

- Search warrant for the following:
  - Billing Records
  - Carrier Key
  - CDR'S
  - Cell-Site information

Billing Records

- Records the customer receives from carrier.
- BR show ONLY completed and billable calls
- BR show ONLY date, time, duration and number called or received from.
- BR are incomplete for your investigation!!

Carrier Key

- Must specifically request to receive
- Provides acronyms, and any special instructions for interpreting their records.
Call Detail Records

- Have to specifically ask for these.
- WAY more information.
- Date, time, duration, number called, calling party, call reference code, text, data, cell-site, sector.
- Not all carriers give all this info.

CELL TOWER DUMP

- All activity on a particular cell-site for a specific time
- TIME SENSITIVE!!
- Each carrier has their own network of Cell-Sites
- Need “Carrier Key”
TOWER DUMP

- Recommended verbiage:
  - "Requesting a “Tower Dump” from all cell sites in the immediate area of (address or lat/long of your incident) that would support any and all communication including but not limited to calls, text messaging, data, walkie-talkie, push to talk…"

Tower Dump

- ATT—90 days only 75$ per cell site 2 week turnaround
- Metro—6 mos $50/site 2 weeks
- Sprint/Nextel/Boost up to 24 months 0-50$ 2 weeks--- special verbiage—“any tower in the area that would support communication…” that way you get all three
- Tmobile—6 mos $100/per 2 weeks NO exigency
- Verizon 90 days no charge 2 weeks

Questions?