

Electronic Law and Evidence

Searching Computers

(2010 Student Handbook pp. 207-38, 451-73)



(b)(6)

Senior Legal Instructor, LGD

(b)(6)

PART I – Electronic Law

EPOs

- TITLE III: Identify the federal requirements governing the use of electronic devices that intercept wire, oral, and electronic communications.
- GPS/Tracking: Identify the federal requirements governing the use of electronic devices that track the movements of suspects.
- Phone numbers: Identify the federal requirements governing the use of electronic devices that trace telephone calls and electronic communications.
- Video only surveillance: Identify the federal requirements governing the use of video-only surveillance in locations where an individual has a reasonable expectation of privacy.
- Stored emails: Identify the federal requirements governing access to stored electronic communications.

QUESTIONS FOR PART I:

What authority/paper is required to do this?

- Record a conversation with the suspect?
- Monitor a call between a CI and the suspect?
- Bug my office to record conversations I have with people?
- Bug someone else's office?
- Wiretap a phone?
- Intercept emails and fax transmissions?
- Find out who a suspect is calling on the phone?
- Find out who is calling the suspect?
- Put a beeper in a package and give it to the suspect?
- Monitor where that package goes?
- Obtain emails and other data stored with Internet Service Providers?

Depending on what you want, you may need

- No special authority or paper.
- Consent of someone.
- A subpoena.
- A court order.
- A search warrant.
- A Title III court order.

Easy



Hard

Some History of Elsur Law

- *Olmstead v. United States (1928):*
 - *Wiretaps OK.*
 - *Supreme Court: 4th Amendment protects places.*
 - *Congress invited to pass wiretap legislation.*
- *Federal Communications Act of 1934:*
Prohibited wiretapping by anyone without consent of both parties.
- *Katz v. United States (1967)*
 - *Microphone on top of phone booth.*
 - *Establishes standard of REP.*

Congress Responds to Katz

- **Omnibus Crime Control and Safe Streets Act of 1968 (Title III)**
 - *Codified REP requirements when intercepting oral communications.*
- **Electronic Communications Privacy Act (1986)**
 - *Extended Title III protection to data communications.*

The Effect of Title III

- Government action must NEVER fall below 4th Amendment requirements –
- BUT, Congress can grant more protection than the 4th Amendment requires.
- Title III does that.

When is a Title III order required?

Oral communications

- Real time interception
- Of a **REP** communication
- With a device
- No REP – No Title III.

Wire & electronic communications

- Real time interception
- Of a communication
- With a device
- Whether REP or not.

Device = other than the human ear

Real time interception = while ongoing

Consent of one party?

Feds – No Title III !

States – www.rcfp.org/taping

State Laws

- In 12 states all parties involved must consent before one of them may legally record the conversation.
 - California
 - Connecticut
 - Florida
 - Illinois
 - Maryland
 - Massachusetts
 - Michigan
 - Montana
 - Nevada
 - New Hampshire
 - Pennsylvania
 - Washington

www.rcfp.org/taping

Georgia Code Ann. § 16-11-62

- Secretly recording or listening to conversation held in a private place without consent of all parties, whether carried out orally or by wire or electronic means, or use of hidden camera to record activities of another occurring in a private place, is a felony invasion of privacy.
 - Applies to clandestine interception or recording of private conversations where interceptee is not party to conversation.
 - Does not apply if party to conversation consents to recording.
- Statute does not prohibit parents from monitoring or intercepting their minor children's phone conversations for the purpose of ensuring the welfare of the minor child.
- **Maximum penalty: imprisonment for one to five years, fine up to \$10,000, or both.**

DEFINITIONS AND EXAMPLES

(18 U.S.C. § 2510)

■ **Oral Communications:**

Face-to-face voice communications not involving transmissions by wire or other electronic means.

■ **IF REP exists, TIII required.**

– *E.g., using parabolic microphone to intercept conversation*

■ **No REP, No Title III.**

– *Public meetings*

– *Police car recorders*

– *Conversation with undercover agent or CI*

– *Conversation heard w/ naked ear or ordinary hearing aid*

■ ***What about signing by the hearing impaired?***

DEFINITIONS AND EXAMPLES

(18 U.S.C. § 2510)

- **Wire Communications**: Human voice transmitted in whole or in part through wire, cable, or other similar connection.
 - Phone conversations.
 - Corded, cordless and cells
 - Voice Pagers.

DEFINITIONS AND EXAMPLES

(18 U.S.C. § 2510)

- **Electronic Communications**: Data transmitted in whole or in part over wire or other mechanical means.
- Examples:
 - Computer data transmissions
 - Fax
 - E-mail
 - Digital display pagers
 - Instant and text messaging (IM chat)

When is a T III permissible? Who must approve prior to Judge?

Wire & Oral Communications

1. Offenses listed at 18 USC § 2516(1)
2. Approval by AAG/Crim Div at DOJ

Electronic Communications

1. Any federal felony
2. Approval by AAG/Crim Div at DOJ
(Digital pager? - AUSA)

What exactly is a Title III (“Wiretap”) Order?

- A special kind of search warrant.
- Requires more than usual showing of PC to search
- Also requires -
 - Showing of necessity – “exhaustion of other means”
 - Plan to avoid intercepting innocent conversation
 - Prior written approval by DOJ
 - Final approval by a US District Court Judge (US Magistrate Judge cannot approve T III.)

Contents of Title III Application

A. Identification of -

- **Predicate crime(s)**
- **Persons expected to be intercepted**
- **Identity of communications to intercept.**

B. Statement of Facts showing PC that –

- 1. Interceptee(s) engaged in predicate crimes**
- 2. Target phone being used to commit predicate crimes**

C. Necessity Statement

D. Previous Applications as to interceptees

E. Minimization Statement

F. Request for Covert Entry

S/W v. Title III: Application and Approval Process

Ordinary warrant

- **Application: under oath**

Agent with PC

AUSA

and signed by Affiant

- **Order good for 30 days**

Magistrate Judge
(Issues warrant)

- **May be re-newed**

Title III

Agent with PC

AUSA

DDJ (digital page AUSA)
(Approve application)

District Court Judge
(Issues order)

When is a T III order NOT required?

■ **Public conversations**

- conversations in the open that can be overheard
- right to be = right to hear
- even if speakers intended conversation to be private

■ **Non-Public conversations**

- Speakers assume risk that other speaker will divulge what is said
- Speaker may have “EP” but no “R”

When is a T III order NOT required?

■ **Consensual monitoring (CI or UCO calls Target)**

– **DOJ Policies**

- Prior AUSA approval if face-to-face
- No prior AUSA approval for electronic consensual monitoring
- Recording/transmitting device must
 - be on consenter's person, or
 - consenter must be physically present where device located.

– **AGENCY POLICY**

- get AUSA approval to protect from entrapment

When is a T III order NOT required?

- Tone only pagers
- Tracking devices
 - beepers or transponders
- Video ONLY surveillance (no audio)
- General public communications, such as:
 - AM/FM radio/TV
 - CB, Ham, Walkie-Talkie
- Pens and Traps

Criminal Violations - 18 USC 2511

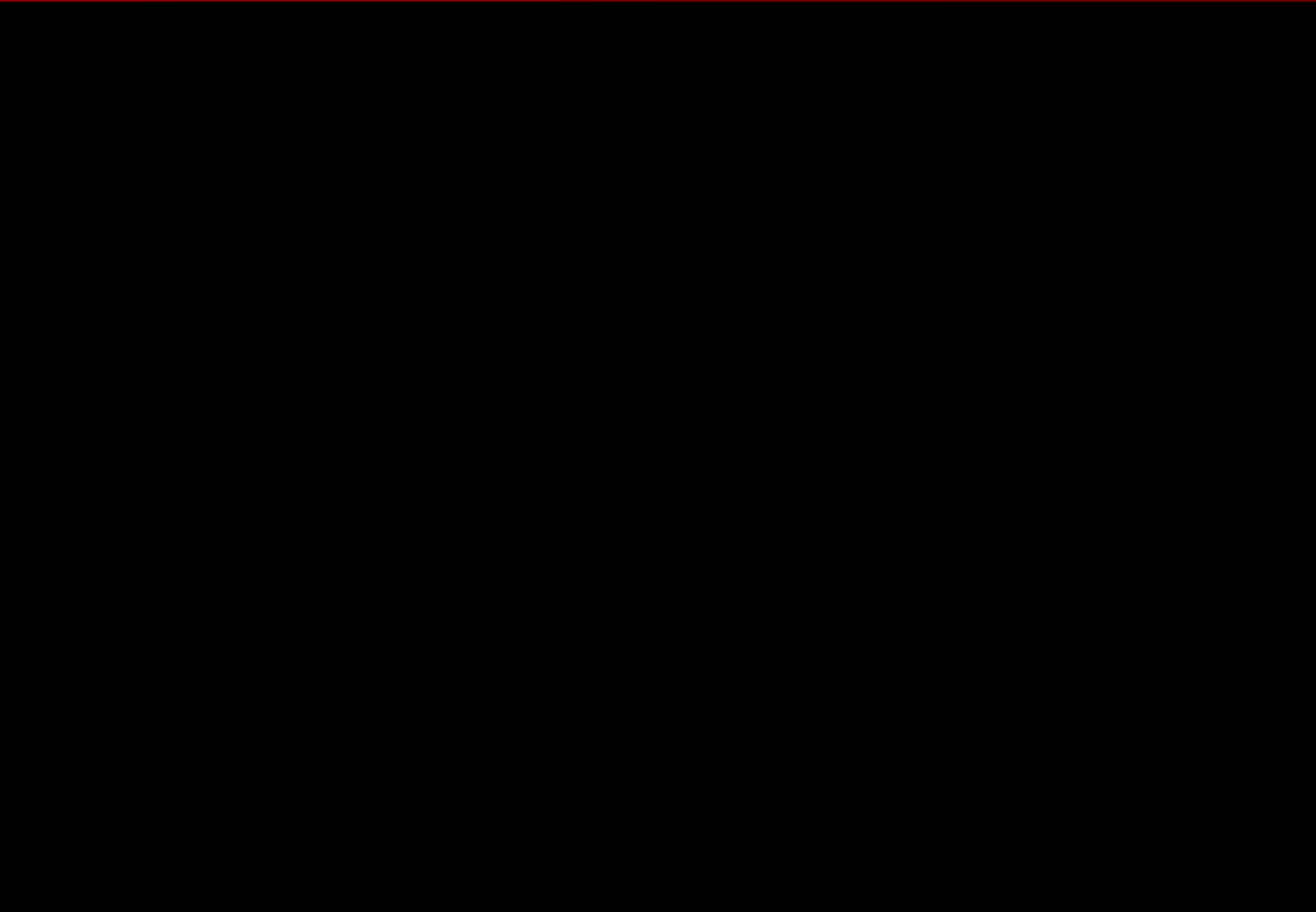
- ◆ Failure to comply with statute resulting in unlawful intercept -
 - ◆ Felony violation
 - ◆ **No LEO exception!**
 - ◆ Basis for
 - ◆ Indictment
 - ◆ Civil lawsuit

U.S. v. Hollern (6th Cir. 2010)

- Chiropractor was convicted of violating 18 USC § 2511 for having installed video camera & sound recorder in patient treatment rooms.
- Defendant's patients had signed consent form allowing him "to record my medical information, including consultation and examination," but form did not mention video monitoring or taping of unrelated conversations.
- Defendant insisted that 18 USC § 2511 was unconstitutionally vague and that, even if that statute is constitutionally sound, his patients' consent had allowed such recording.
- The Sixth Circuit found that –
 - while § 2511 is not vague, the language in the defendant's consent forms certainly was.
 - **defendant's convictions upheld.**

EPO: Identify the federal requirements governing the use of electronic devices that track the movements of suspects.





Electronic Tracking Devices

4th Amendment Governs

1. Was the **installation** legal?
2. Was the **monitoring** legal?

Installing

- ❖ **GENERAL RULE:** Warrant or consent required to install IN or ON private property.
- ❖ Connected to vehicle wiring: Warrant.
- ❖ NOT connected to vehicle wiring: No warrant
- ❖ Enter onto REP area to install: Warrant.
- ❖ In or on Government property: No warrant.

Installing Device

Location OF Vehicle	REP	No Rep	REP	No Rep
Location ON Vehicle	REP	No Rep	No REP	REP
	Warrant	No warrant	Warrant	Warrant

Monitoring

REP in area monitored?

- **No – no warrant required**
- **Yes – need a warrant**

Warrants to Install and Use GPS Tracking Devices

Fed R. Crim. Pro. 41

- Judge in district where vehicle located issues warrant.
 - 10 days to install – daytime unless judge authorizes night installation
 - Good for 45 days
 - May be renewed
- LEOs may track in any district.
- “Return” to “trackee” w/in 10 days after tracking ends.
 - BUT - Judge may authorize a delay in the return.

Extended Warrantless GPS Tracking: U.S. v. Maynard (DC Cir. 2010)

- Agents installed GPS tracking device on defendant's vehicle w/o warrant while vehicle parked in public place.
- Agents tracked defendant's vehicle 24/7 for 4 months, but only in public places.
- Agents used tracking data to corroborate cell and other data concerning defendant's whereabouts during drug trafficking conspiracy.
- Defendant moved to suppress all tracking data.
- What result?

Extended Warrantless GPS Tracking: U.S. v. Maynard (DC Cir. 2010)

- DC Circuit held –
 - 24/7 warrantless GPS tracking of defendant, even in public places, constitutes an intrusion into the REP of vehicle owner/operator.
 - Such tracking requires a Rule 41 warrant based on PC that tracking will produce evidence of a crime.
 - Court acknowledged that GPS surveillance of vehicle in public places, if surveillance is of short duration, i.e., not 24/7, would not require a search warrant.

Recent Caselaw

- *U. S. v. Pineda-Moreno* (9th Cir. 2010)
 - Agents attached tracking device to defendant's car while it was parked in his driveway at 4 a.m.
 - Government concedes car in curtilage (stupid!)
 - Ninth Circuit:
 - Driveway “only a semi-private area” where property owner has done nothing to enclose, barricade or shield driveway from public access
 - Thus, Pineda had no REP in area underneath car and tracking device data was admissible.
 - **Ninth Circuit? Go figure!**

Cell Phone Tracking

■ Types of location data from cell phone service provider

1. approx. present whereabouts of power-on cell phone from cell site data
2. Nearly exact location of cell phone from triangulated cell site data

■ Is acquisition of real time cell site info the legal equivalent of using GPS tracking device?

- If yes, LEO need not obtain S/W if cell phone stays in public place.
- If no, it's probably "stored electronic info," requiring 2703(d) order (later).

Cell Phone Tracking (con'd)

- So, what's the problem?
 - Cell phone service provider
- Their primary interest?
 - Their subscribers.
 - Won't give up subscriber info unless legally compelled.
- Still another issue?
 - **cell phone usage likely will be in both public and private areas.**

Cell Phone Tracking: What the Courts say

- **Two views re: authority required for government to obtain real time and prospective cell site information**
 - **Majority view:**
 - 18 USC §2703(d) order sufficient to obtain stored cell site information but PC & Rule 41 S/W required to compel disclosure of real time & prospective cell site data.
 - **Minority view:**
 - Government's pen register/trap and trace authority sufficient to obtain single cell site information in real time.
 - **Caveat:**
 - Government needs S/W in order to obtain multiple cell site triangulation information.

Trap / Trace & Pen Registers



EPO: Identify the federal requirements governing the use of electronic devices that trace telephone calls and electronic communications.

- ▶ **Pen Registers: Outgoing**
- ▶ **Trap & Trace: Incoming**

Trap / Trace & Pen Registers

- **18 USC §§ 3121-3127 (not Title III)**
- **Requires court order.**
 - **AUSA makes application.**
 - **“Relevant to an ongoing criminal investigation.”**
- **Good for 60 days.**
- **Can also subpoena toll records.**
- **Can also be used to obtain email addresses of correspondents.**
 - **But NOT the content of the email.**



Covert video camera in clock

EPO: Identify the federal requirements governing the use of video-only surveillance in locations where an individual has a reasonable expectation of privacy.

Video-Only Surveillance

Fourth Amendment, not Title III

But, “court-imposed heightened requirements.”

- Necessity Statement
- Minimization statement
- Description of premises
- Duration (30 days from date of order, with NO 10-day grace period)
- Name of person under surveillance, if known

Caselaw

U.S. v. Jackson (10th Cir. 2000)

- FBI & Elk City OK PD set up video cams on the tops of telephone poles for surveillance of suspected illegal drug activities at two residential properties.
- Cameras could be remotely adjusted by LEOs and could zoom in close enough to read a license plate, but could not record sound or view the inside of the suspects' houses.
- Tenth Circuit held that defendants had no REP requiring a S/W because the cameras were incapable of viewing inside their houses and could only record what any passerby could easily have seen.

Caselaw

U.S. v. Cuevas-Sanchez (5th Cir. 1987)

- Federal LEOs obtained court order to install & monitor video cam on public power pole in order to see over defendant's 10 ft fence around his marijuana garden.
- LEOs' affidavit set forth PC, that conventional law enforcement techniques had been attempted but failed to uncover enough evidence to convict defendant.
- Court's order limited surveillance to 30 days, mandated minimization, and directed LEOs to discontinue surveillance when defendant not on the premises.
- Defendant moved to suppress video evidence.
- Government's response:
 - No warrant required because defendant had no REP but in abundance of caution we got one anyway.
 - Anyone on top of pole could see over defendant's 10-foot fence so no intrusion of REP.

Caselaw

U.S. v. Cuevas-Sanchez (5th Cir. 1987)

- Court held that:
 - Defendant exhibited *subjective* expectation of privacy by erecting fence to hide activities in backyard (curtilage).
 - Indiscriminate video surveillance raises specter of Orwellian state. [*1984*, G. Orwell]
 - Govt's video cam allowed 24/7 recording of activity in curtilage, unlike minimal recording/observation from one-time overhead flight or glance over fence by passerby.
 - So, such video surveillance, if warrantless, violates 4th Am.
 - But since govt followed all requirements of video warrant, defendant's motion denied.

Caselaw

U.S. v. Urbina (EDWI 2007)

- LEOs installed video cam on public telephone pole near defendant's property.
- Video cam monitored front of defendant's residence and recorded vehicles coming and going from driveway.
- Court found that:
 - LEOs weren't surveilling anything not otherwise visible using traditional street-level surveillance techniques.
 - Where video surveillance doesn't record activities in home, or in curtilage that defendant has obscured from public view, it is no more intrusive than traditional surveillance methods and triggers no more 4th Amendment concerns than those latter methods.

But wait, there's more...

Brannum v. Overton County School Board (6th Cir. 2008)

- School authorities installed hidden cameras in girl's dressing room and recorded students in underwear.
- School justification = safety & security but no evidence of past threat to school security in dressing rooms.
- School did not notify students or parents.

Brannum (continued)

- Court found that –
 - There is universal understanding that a school locker room is a place of heightened privacy.
 - OK to do what School Board did if there is demonstrated necessity.
 - But, if not, video only surveillance of children dressing and undressing in a locker room is disproportionate to the claimed policy goal of insuring school security.
 - Board members denied Qualified Immunity.

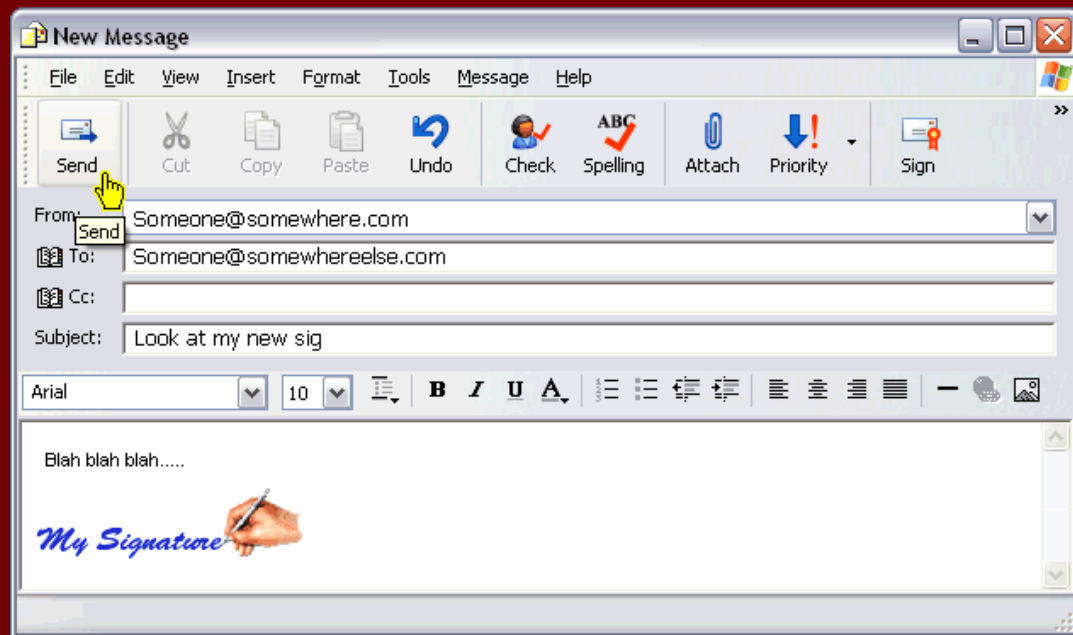
Video Voyeurism Prevention Act

18 U.S.C. § 1801

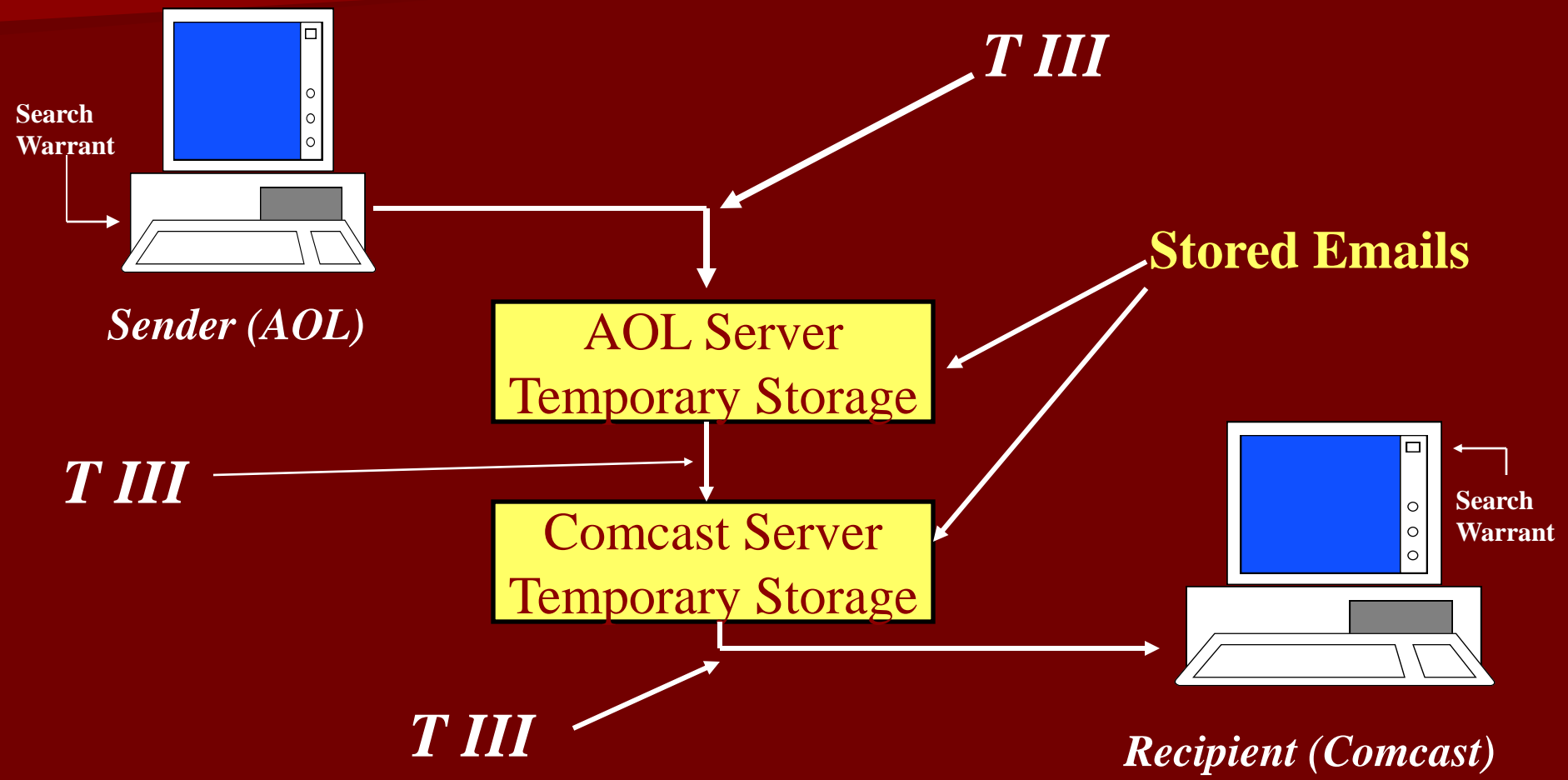
(Bonus)

- Applies only to activities on areas within the special maritime and territorial jurisdiction of the US.
- Elements:
 - Whoever knowingly
 - Captures or transmits an image
 - Of person's private "area" (genitals, pubic area, buttocks, or the female breast below top of areola) or such areas when covered by undergarments
 - Without consent of person whose image is "captured"
 - When capture or transmission takes place in REP
 - Shall be imprisoned for up to one year and fined.
- **Lawful law enforcement ops excluded.**
 - Check the scope of your warrant !!!

EPO: Identify the federal requirements governing access to stored electronic communications.



STORED E-MAILS v. TRANSIENT E-MAILS (Stored Electronic Communications)



Stored Electronic Communications

- 1. Basic Subscriber Information**
 - **Stuff about the customer**
- 2. Contents (to include subject line)**
- 3. Transactional records**
 - **How person “transacts” with his account.**
 - **That which is not basic subscriber or content.**

The “paper” you need

- Consent of the subscriber always works
 - But you will tip your hand.
- “minimum” paper you need:
 - Subpoena?
 - Court Order?
 - Search Warrant?
- Remember: You can always use more paper than you need.

Basic Subscriber Information

- **Name and address**
- **Session records**
- **Telephone numbers**
- **Payment method**

Minimum Paper - Subpoena

Contents

Opened (Retrieved)

- Subpoena

Unopened

- Stored > 180 days
 - Subpoena
- Stored 180 or less
 - Search warrant

Transactional Records

- **E-mail addresses of correspondents**
- **Web sites visited**
- **Cell-site data for cellular phone calls**

Minimum Paper: 2703(d) Court Order
(“Relevant and material to an ongoing criminal investigation”)

Notice Requirements

- When *no notice* is required, or where *notice* may be *delayed*,
- Court order may prevent the ISP from notifying the subscriber.

Summary Chart: Access To E-mail Info

Authority → Info Sought ↓	Search Warrant	2703(d) Order	Subpoena
Subscriber Information	Yes	Yes	Yes
Transactional Information	Yes	Yes	No
Content: un-opened & < 180 days old	Yes	No	No
Content: Opened <u>or</u> > 180 days old	Yes	Yes	Yes

Delaying or Preventing Notice by ISP to Customer/Subscriber

- ▶ **ISP must notify Customer/Subscriber of disclosure of info to government via S/W.**
- ▶ **Gov't must notify Customer/Subscriber if disclosure of info by ISP in response to subpoena.**
- ▶ **Court may delay ISP notice if government shows reason to believe notice will -**
 - ▶ **Endanger someone's life or physical safety;**
 - ▶ **Cause flight from prosecution;**
 - ▶ **Result in destruction of or tampering w/ evidence or intimidation of witnesses;**
 - ▶ **Seriously jeopardize an investigation or unduly delay a trial.**

Preservation Letters

- If you need stored emails, do this **first** !
- Agent may obtain 2703(f) preservation letter (ASAC) and serve on ISP.
 - This prevents ISP from deleting stored emails.
- Good for 90 days.
 - Renewals possible.
- Not prospective.
 - Just the stored emails on date of the order.

U.S. v. Beckett (11th Cir. 2010)

- LEO investigating def't for blackmailing kids into having sex w/ him.
- LEO obtained subscriber info from ISP & cell phone provider using the "emergency" exception to 18 USC §2702(c)(4) rather than a S/W, §2703(d) order, or a subpoena.
- Defendant moved to suppress arguing no exigent circumstances.
- Court found that –
 - ECPA allows ISP to disclose subscriber & trans. info to gov't if ISP believes such info. is relevant to emergency involving threat of death or serious physical injury to any person.
 - Emergency existed in this case justifying ISP's disclosures.
 - Even if exigency didn't exist, defendant lacked REP in the info. obtained.
 - ECPA lacks suppression remedy so that's not proper remedy for violation

Multi-Jurisdiction Warrants for Stored Email

- What if the email servers are located in more than one district?
 - Do you need a warrant from magistrate in each district?
- For data, you need multiple warrants.
- **Special rule for email:**
 - A judge in a district with “jurisdiction over the offense under investigation” may issue a warrant.

PART II - Searching Computers

EPOs

- Warrantless searches: Describe when computers may be searched and/or seized without a warrant.
- Data warrants: Describe special considerations in preparing a search warrant to search and/or seize computers.
- Executing the warrant: Describe special considerations in executing a search warrant to search and/or seize computers.
- Authenticating data: Describe special issues involving authentication of information contained on computers.

EPO

Describe when computers may be searched and/or seized without a warrant.

4th Amendment & Computers

- Just like searching anywhere else.
- Is computer located in REP area?
- Does owner have REP in computer data?
- Is government attempting to intrude?
- Is there exception to 4th Amendment that applies?

4th Amendment not Triggered

■ Private search.

- Person using another's computer.
- Computer turned in for repair.
 - A private search may be replicated.
 - But may not exceed the scope of the private intrusion.

■ No REP.

- Exposure to public – divulging to others
- Stolen computers
- Abandoned computers

Exception – Actual Consent

- By person who actually has REP.
- Co-user consent.
 - Consent by one co-user sufficient.
 - Objection by present co-user defeats consent of others.
 - Consent of person with apparent authority?
 - Encrypted or password protected files?
- Scope
 - Can be limited
 - Does it include media?
- Consent can be withdrawn.

Exception - Exigent Circumstances

■ Factors:

- Urgency
- Time to obtain warrant
- Is evidence about to be removed or destroyed
- Danger at location of the evidence
- Does possessor of evidence know the police involved?
- Is the evidence readily destructible?

■ Data can be easily destroyed.

- Loss of power, delete commands, magnetism.

Exigent Circumstances - Applied

- **When the exigency ends, so must the search!!!**
- **Seizure versus search**
 - Seize the evidence to prevent destruction.
 - Then get a warrant to search.
- **Some judges skeptical of “exigent circumstances.”**

Exception - Plain View

- **Right to be, right to see.**
- **REMEMBER:**
 - Plain view is **NOT** a searching tool.
 - It is a seizure tool.
- **Example: Data on screen - plain view**
 - Seize, but does not authorize a search of the computer.
- **Example: Seeing the storage media or file name is **NOT** plain view of contents.**
 - If LEO must open the file to see it, the contents are not in plain view.
- **Best rule.** If you see evidence possibly outside scope of warrant, stop and get new warrant.

CAVEAT: Recent Court Trend On Plain View & Data

- Courts have noted that -
 - computers contain vast quantities of intermingled data, and
 - therefore are not mere “containers.”
- LEO who searches computer containing intermingled documents must -
 - take the intermediate step of sorting various types of documents, and
 - then only search the ones specified in a warrant.

U.S. v. CDT

- U.S. v. CDT (9th Circuit 2009)(en banc 2010)
 - Baseball steroid testing case
 - 9th Cir. Reversed lower court's ruling that files of players not on S/W list were properly seized under plain view
 - Said government was required to use a judicially-approved mechanism to separate computer evidence not covered by S/W from other evidence on computer (even if of another crime)

Compare U.S. v. Mann **(7th Cir. 2010)**

- High school coach installed video cam in girl's dressing room.
- Student found it and turned it over to police.
- Police found images on camera of coach installing it and obtained data S/W to seize locker room pix in violation of state voyeurism statute.
- Agents seized 2 computers & 1 hard drive from coach's home.
 - Used FTK software to locate and isolate images on computers.
 - Agents viewed thumbnails to determine if within scope of S/W
 - Find pix of female students in locker room unrelated to internet CP
 - FTK hashing software also identified 4 other CP images.
- Court held that –
 - FTK isolated locker room images found in plain view & admissible.
 - CP images found via hashing were beyond scope of S/W and therefore subject to suppression.

U.S. v. Stabile (3d Cir. 2010)

- **Court rejected *U. S. v. CDT*, 621 F.3d 1162 (9th Cir. 2010) siding with the 7th Circuit's decision in *United States v. Mann*.**
 - While executing financial crimes S/W, agent opened a Kazaa folder and found several files with sexually-explicit names.
 - Agent opened them finding child porn.
 - Stabile moved to suppress citing CDT case.
- **3rd Cir.: Plain view rule applies to computer search just like any search.**
 - LEO must not have violated 4th Amendment in arriving at the place to be searched;
 - incriminating character of evidence must be immediately apparent; and
 - LEO must have lawful right of access to the object.
- **In this case,**
 - Agent did not violate the 4th Amendment in looking at the hard drive - he had the consent and later was executing a properly granted state warrant to look for evidence of financial crime on a computer.
 - While doing so, he properly chose to look at the names of files within a Kazaa folder.
 - This was permissible because a thorough computer search requires a broad examination of files on computer to ensure file names haven't been manipulated to conceal their contents.
 - File names seen in this review were lurid and immediately suggested child porn.
 - **Therefore, the child porn files were within plain view and the file names provided PC to obtain a warrant to open those files.**
 - **Opening files was illegal but that info NOT used to get S/W.**

Exception - SIA

■ Requirements:

- Lawful custodial arrest.
- “Substantially contemporaneous” with arrest.

■ Scope: person, lunging areas, containers, passenger compartment.

■ Pagers – Yes. The data is perishable.

■ Cell phone: **Maybe? Circuits are in conflict!**

- 5th Cir.: Yes to numbers of recent calls received/dialed. (*Finley*)
- District Court, SDFL: No. (*Wall*)
- District Court, DMN: No. (*Chappell*)
- All: NO on voice mail access. Data not on the phone itself.

■ Computers and PDAs – no cases (yet)

■ *Arizona v. Gant* - ??

Exception - Inventory

- Inventory is not authority to search for evidence of crime.
- Inventory permissible to:
 - Safeguard citizen's property.
 - Protect LE from dangerous stuff.
 - Protect against false claims.
- Inventorying data may put data at risk.
 - **Do not inventory data.**

Delay of Computer Search

- *United States v. Mitchell*, (11th Cir. 2009)
 - Government agents lawfully seized hard drive on defendant's computer after he told agents it contained child porn.
 - Agents had PC to search for evidence on defendant's computer but waited 21 days to get search warrant to search hard drive.
 - Court held that was unreasonable delay and thus warrant was invalid.
 - **Child porn suppressed.**

Ouch!

EPO

Describe special considerations in preparing a search warrant to search and/or seize computers.

APR- 4-97 TUE 16:37 P. 02

FD-106 (Rev. 5-87) Affidavit for Search Warrant

United States District Court
WESTERN DISTRICT OF WASHINGTON

MAR 28 1997
CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

7214 Corregidor Road
Vancouver, Washington

**APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT**
CASE NUMBER: 97-5025m

I, Jeffrey Gordon, being duly sworn depose and say:

I am a(n) Inspector with the Internal Revenue Service and have reason to believe that () on the person or (X) on the property or premises known as (name, description and/or location)

See Attachment A, attached hereto and incorporated herein

in the Western District of Washington there is now concealed a certain person or property, namely:
(Describe the person or property to be seized)

See Attachment B, attached hereto and incorporated herein


Which is (state one or more bases for search and seizure set forth under Rule 41(b) of Criminal Procedure)

evidence of threats, assaults, obstruction, intimidation, solicitation of murder, false statements, and the unlawful use of false social security numbers

concerning a violation of Titles 26, 42, and 18 United States Code, Section(s) 7212(a); 408; 111; 115; 1505; 1959 and 1001. The facts to support the issuance of a Search Warrant are as follows:

See attached Affidavit of Jeffrey Gordon, attached hereto and incorporated herein


Continued on the attached sheet and made a part hereof. (X) Yes () No


Signature of Affiant
JEFFREY GORDON

Sworn to before me, and subscribed in my presence

March 28, 1997 @ 9:02am at Tacoma, Washington
Date City and State

J. KELLEY ARNOLD
United States Magistrate Judge
Name and Title of Judicial Officer


Signature of Judicial Officer

USAO No. 9602582 1

Pre-Search Information

- Types of computers and operating systems.
- Types of software.
- Network connections.
- Can the computer be searched on-site?
 - Or do we have to take it with us?
- Make friends with your electronic evidence experts.
 - Check with LAN administrators.
 - May require undercover ops.

4th Amendment “Particularity”

- **WHERE do you want to search?**
 - There are places other than the “computer” where data may be.
 - Media, external drives, thumb drives, flash memory, on the internet, gaming devices, cell-phones, PDAs.
- **Independent component “doctrine”**
 - Treat each place the evidence might be as separate – and develop PC for each.

4th Amendment “Particularity”

- **What are you looking for?**
- Is it data that you *really* want?
 - If so, describe the data.
 - Don’t ask for “Records in any form”
 - Be specific: “spreadsheets, databases, email, images, etc. relating to _____”
 - Don’t forget to include “metadata.”
 - Must connect what you are looking for to Target PC.

4th Amendment “Particularity”

- **What are you looking for?**
- Is it the hardware you want to search?
 - Hardware only searches are rare.
 - Fruits of crime, contraband, instrumentalities.
 - Sometimes you may want both computer AND the data.
 - E.g., to prove particular computer was used in a certain way.

Justifying Off-Site Data Search After On-Site Hardware Seizure

- If you can't image (copy) the data on site, ask to take the computer to image the data.
- If computer must be removed off-site
 - explain the contingencies in your S/W application
 - Include request to take computer(s)
- Effect of denying a person or business of their computer and data?

Rule 41(e)(2)(B)

Warrant Seeking Electronically Stored Information

- A warrant...may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information.
- Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant.
- The time for executing the warrant...refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Two-Step Procedure

1. Computer is seized or imaged during execution of warrant.
2. Computer or imaged data is removed for off-site review to search for information falling within scope of the warrant.

Note: Rule places no explicit time limit on duration of any forensic analysis of a seized computer,

- a. BUT 4th Amendment requires that time be reasonable
- b. Magistrate Judge may impose time restrictions on forensic analysis.

Do you need >1 Warrant?

- Warrant to search a computer does NOT authorize searching for Internet locations where the bad guy stores data.
- You must have a warrant to search each place where the data might be.
 - Why pre-search information critical.

Remember – Exception to Multiple Warrant Requirement

- A judge in a district with “jurisdiction over the offense under investigation” may issue a warrant to seize stored electronic communications anywhere in the nation (Email on ISP servers).

EPO

Describe special considerations in executing a search warrant to search and/or seize computers.

Technical Assistance

18 U.S.C. § 3105

- *A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution.*
- If technical expert req'd (usually is), best practice is to say so in the S/W application & S/W.

S/W Inventory

- In executing S/W, if LEO seizes either -
 - electronic storage media, or
 - Images electronically stored information
- S/W inventory need only describe the physical storage media that was
 - seized, or
 - copied.
- NO NEED TO ITEMIZE MEDIA CONTENTS.

EPO

Describe special issues involving authentication of information contained on computers.

Authentication Issues

- **Government must show that it is offering file(s) seized from the target computer.**
- **Were the records altered?**
 - You **MUST** handle data in order to counter claims of alteration.
- **Who wrote or created the record?**
 - Existence of data not enough.
 - Must connect it a specific person or entity.

Authorship of Electronic Records

Often circumstantial evidence is based on

- Where was the computer/data found?
- Who had access?
- Trace evidence on computer and components
- Passwords/screen names
- Software authorship tools
- Match documents to Email attachments

"HASHING"

- Method of using algorithm to create digital "fingerprint" of particular data.
- Hashing software allows confirmation that document offered now is same seized at a previous time.
 - Check out - <http://hash-software.qarchive.org>

Resources

- www.cybercrime.gov
 - DOJ Site: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations
- www.cybercopportal.org
 - Designed specifically to assist LEOs in investigating computer-related crimes
 - Secure email system

Recent Caselaw: Records S/W does not authorize search of computer

- ***United States v. Payton* (9th Cir. 2009): Trial**
- LEOs obtained S/W to search Payton's home for evidence of drug sales, buy sheets, sales ledgers, financial records, etc.
- Affidavit contained reference to computer search but S/W did not specifically authorize search of computers.
- During execution of S/W, LEO searched Payton's computer revealing presence of CP .
- Deft moved to suppress CP files seized from computer.
- Trial Court denied motion and Payton was convicted of possession of CP.

Recent Caselaw: Records S/W does not authorize search of computer

- ***United States v. Payton* – appeal**
- Court noted that computers capable of storing vast amounts of information and thus computer searches are far more intrusive than other document searches.
- LEO searching computers containing intermingled documents must sort various types of documents and then only search the ones specified in a warrant.
- Primary purpose of S/W is to advise LEOs precisely where they may search.
- Thus, specific authorization must be in S/W if LEOs want to examine contents of computer located on the premises to be searched.
- **NOTE: Not all Circuits adhere to this. Others - OK to search computer if that is likely repository of items in "wish list." (Like looking in desk drawer if S/W is for guns.)**

Recent Caselaw: Staleness

■ ***U.S. v. Frechette* – District Court**

- Target subscribes to child porn website Jan. 13, 2007 paying \$80 via PayPal.
- Target's PayPal account info includes his name, address & phone number.
- Target's ISP's records showed that one of its account holders used the ISP's IP address to access same child porn website on January 13, 2007, and that account was in Target's name/address.
- Agent submits S/W affidavit in April 2008.
- District Court granted Target's motion to suppress on grounds of staleness.

Recent Caselaw: Staleness

- ***U.S. v. Frechette* – Appellate Court**
 - Child porn not like drugs – “fleeting inventory.”
 - Evidence presented to USMJ showed that defendant still at same address.
 - Given that defendant used computer to subscribe to site, there was reasonable probability that
 - he downloaded illegal material, and that
 - illegal materials likely still on defendant’s hard drive even if he deleted them (“soft delete”).
 - District Court’s suppression order **REVERSED.**

Recent Caselaw: Best Evidence Rule

- *United States v. Bennett*, 363 F.3d 945 (9th Cir. 2004)
 - CBP board defendant's
 - GPS waypoints showed that boat had been in Mexican & international waters before entering U.S. waters.
 - Found MJ on board during search & defendant arrested for importation of controlled substance.
 - At trial, GPS unavailable & government sought to prove entry into U.S. waters by testimony of CBP officer re: waypoint observed on defendants' GPS.

Recent Caselaw

Bennett (continued)

- Appellate Court:
 - Best evidence rule requires production of original & or acceptable duplicate if contents are sought to be proved.
 - Therefore, Rule required government to produce GPS or authenticated printout of GPS coordinates.

Recent Caselaw: BER

- *United States v. Jackson* (D. Neb. 2007)
 - UC Sting: LEO posing as 14 year old girl has sexually explicit comms with defendant.
 - Gov't & Def't computers lost or destroyed before trial.
 - Gov't sought to introduce LEO's cut & paste summaries.
- Cut-and-paste summary of Internet chat logs is inadmissible under BER –
 - Where it does not accurately reflect the entire conversations between the defendant and LEO
 - Where LEO included editorial comments.
 - Where there is evidence of alteration.

EL&E (4)

- This class will commence process that will end at Phase 9 with each team in possession of a signed Search Warrant allowing search for evidence, including data, of violations of 18 USC §§1028, 641 & 922(g).
- Bring to class the **Team Laptop** and at least one flash drive.
- You may also bring your personal laptop.

ELECTRONIC COMMUNICATIONS REVIEW

- Acting without warrant, a federal LEO has Snitch wear a recording device during undercover operation and Snitch records his conversation with Bad Guy about buying marijuana. At trial, that recording of conversation between Snitch and Bad Guy is:
 - a. inadmissible because obtained without warrant.
 - b. inadmissible because obtained without Title III court order.
 - c. admissible because Snitch is a party to the conversation.
 - d. admissible because there can be no REP by Bad Guy as to public conversations with Snitch.

ELECTRONIC COMMUNICATIONS REVIEW

- Why isn't D the correct answer?
 - You don't necessarily lose REP by speaking in public, e.g., whispering in parking lot.
 - You do assume the risk and implicitly consent that anyone you speak to, in public or in private, will repeat your statements
 - to the police
 - to the jury.

REVIEW

- Acting without a warrant, a federal LEO wears a recording device during an undercover drug buy and records his conversation with Bad Guy about buying marijuana. At trial, that recording with bad guy is:
 - a. inadmissible because obtained without warrant.
 - b. inadmissible because obtained without Title III court order.
 - c. admissible because Bad Guy is party to the conversation.
 - d. admissible because Bad Guy waived his REP in his oral communication with the UCO.

ELECTRONIC COMMUNICATIONS REVIEW

- Why isn't C the correct answer?
 - Bad Guy being a party to the conversation would not make recording of conversation admissible (but Snitch or UCO being party would).
 - It is Bad Guy's implicit consent to the use or repeating of his words by UCO (or anyone else) when he spoke to him.

ELECTRONIC COMMUNICATIONS REVIEW

- LEO plants a bug in Bad Guy's house. Using the bug, LEO records conversation between Bad Guy & Criminal. LEO may use this tape at trial only if he:
 - a. had a warrant allowing entry into Bad Guy's house and the recording of conversations between Bad Guy and Criminal.
 - b. had a Title III Court Order allowing installation of the bug and monitoring of the conversations transmitted by the bug.
 - c. had a grand jury subpoena authorizing the bug.
 - d. had exigent circumstances or an emergency to justify a warrantless interception of conversations between Bad Guy and Criminal.

ELECTRONIC COMMUNICATIONS REVIEW

- LEO gets Rule 41 warrant to plant a bug in Criminal's house. Using bug, LEO records conversation between Criminal, Crook, and U/C Agent.
 - Legal or Illegal?**
 - Legal, because U/C Agent consented.**
- LEO records conversations between Criminal and Crook when U/C Agent isn't there.
 - Legal or illegal?**
 - Illegal because no consent and no Title III Court Order.**

ELECTRONIC COMMUNICATIONS REVIEW

- LEO legally puts transponder in Criminal's suitcase which criminal places in car. LEO tracks movement of suitcase as Criminal drives on public streets. This is:
 - a. Legal?
 - b. Illegal?

Legal because no REP in public travel.
- Criminal then drives into his warehouse. LEO tracks the movement of the briefcase through the warehouse using transponder. This is:
 - a. Legal
 - b. Illegal

Illegal unless LEO has warrant authorizing monitoring in REP locations.

ELECTRONIC COMMUNICATIONS REVIEW

- Federal LEO suspects FLETC instructor is stealing FLETC computers puts beeper in a FLETC computer without a warrant. LEO then tracks the beeper from FLETC to Joe's Pawn Shop, where the FLETC instructor tries to sell the computer. This evidence is:
 - a. inadmissible because LEO didn't have court order.
 - b. admissible because no court order needed to put beeper on gov't property or monitor it in public places.
 - c. admissible because LEO had RS that FLETC instructor had stolen the computer.
 - d. either b or c.

ELECTRONIC COMMUNICATIONS REVIEW

- Does LEO need a Title III court order to do the following?
- Record your cell phone conversations in real time?
- Place bug in hotel room?
- Intercept email while in transit to ISP server?
- Use water glass to hear conversation in next door hotel room?
- Intercept fax while in transmission
- Listen to two bad guys' conversation while hiding in their closet without consent?

ELECTRONIC COMMUNICATIONS REVIEW

- Does LEO need Title III court order to -
- look at print copy of fax?
- listen to CB, ham radio, walkie-talkie transmissions?
- Install and use video camera in REP area?
- Install and monitor tracking device in a briefcase?
- Use trap and trace?
- Install pen register?

ELECTRONIC COMMUNICATIONS REVIEW

- How long is a Title III Court order good for (maximum)?
 - a. 1 day
 - b. 2 days
 - c. 30 days
 - d. 60 days

ELECTRONIC COMMUNICATIONS REVIEW

- How long is a court order for a trap and trace or pen register good for (maximum)?
 - a. 1 day
 - b. 2 days
 - c. 30 days
 - d. 60 days

ELECTRONIC COMMUNICATIONS REVIEW

- What is a pen register?
 - Records numbers called from a certain phone line

- What is a trap and trace device?
 - Records the phone numbers of incoming calls (like caller ID)

- What authority does the LEO need to install a pen register or trap?
 - Pen or trap order.

- What are consequences if LEO installs unlawful pen or trap?
 - LEO in trouble, but evidence still admissible.

Electronic Communications Review

- What is a pen register?
 - Records numbers called from a certain phone.
- What is a trap and trace?
 - Records numbers of incoming calls to a certain phone.
- What authority does a LEO need to install a pen register or trap and trace?
 - A pen register or trap and trace order.
- What are the consequences if a LEO unlawfully installs a pen register or trap and trace?
 - Evidence still admissible but LEO may be in trouble.

ELECTRONIC COMMUNICATIONS REVIEW

- The LEO wants to conduct video-only surveillance in an area where criminal has REP. What legal document does he need?
- a. Title III court order
- b. 2703(d) court order
- c. search warrant
- d. none

ELECTRONIC COMMUNICATIONS REVIEW

- The LEO wants to conduct video-only surveillance of Criminal's front yard and driveway using pole camera mounted on telephone pole across the street from Criminal's house. What legal document does he need?
 - a. Title III court order
 - b. 2703(d) court order
 - c. Search Warrant
 - d. none

ELECTRONIC COMMUNICATIONS REVIEW

- The LEO wants to conduct video-only surveillance of MJ garden in Criminal's fenced back yard using pole camera mounted on telephone pole in adjacent public park. What legal document does he need?
 - a. A Title III Court Order
 - b. A 2703(d) Court Order
 - c. A Search Warrant
 - d. None

ELECTRONIC COMMUNICATIONS REVIEW

- Skippy has an AOL account. You want to get transactional information from AOL about Skippy's account. You could use:
 - A. search warrant
 - B. 2703(d) court order
 - C. subpoena
 - D. either A or B but not C

ELECTRONIC COMMUNICATIONS REVIEW

- Skippy has an AOL account. You want to get copies of his stored communications which are not more than 180 days old. What document(s) do you need?
 - A. A subpoena
 - B. A 2703(d) order
 - C. A search warrant
 - D. None

ELECTRONIC COMMUNICATIONS REVIEW

- You (the LEO) lawfully arrest Skippy. Skippy has a pager and a laptop. During the search incident to arrest, you may -
 - a. Scroll through the numbers in the pager.
 - b. Look through all the documents in the laptop.
 - c. Both a. and b.
 - d. Neither a. nor b.

Electronic Communications Review

- You (the LEO) are interviewing Skippy in his office. You notice Skippy's computer has what appears to be a CP image. Skippy starts to delete it. You may –
 - A. Stop Skippy from deleting the image?
 - B. Start searching the computer?
 - C. Arrest Skippy for possession of CP?
 - D. Seize the hard drive for later forensic testing?

ELECTRONIC COMMUNICATIONS REVIEW

- You are investigating Skippy for a federal fraud offense involving use of his computer in S.C. You want to get a single search warrant for that computer and to access his files from his Internet Service Provider in Maine. Who may issue the warrant?
 - a. A federal judge in the District of Maine.
 - b. A federal judge in the District of S.C.
 - c. Either of those two judges.
 - d. A federal judge in Washington, D.C.

ELECTRONIC COMMUNICATIONS REVIEW

- LEO searched Skippy's computer and found a file full of child pornography. In order to make certain that this file will be admitted at trial, LEO should:
 - a. ensure that file isn't altered after seizure
 - b. bag and tag the computer's hard drive
 - c. create a clone of computer's hard drive
 - d. document the government's possession of the computer until trial

Electronic Law and Evidence

Searching Computers



(b)(6)

Senior Legal Instructor, LGD

(b)(6)

