Typical Investigative Steps and Statutory Framework

National Center
For Justice And The Rule Of Law

University of Mississippi
School of Law

Thomas K. Clancy
Director

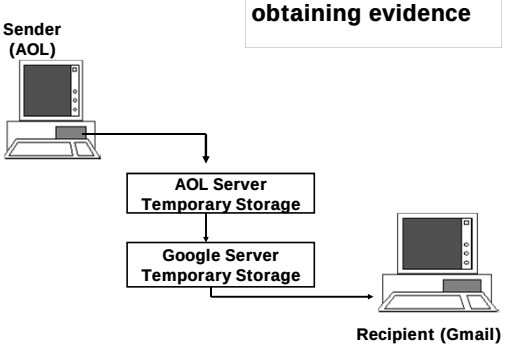
www.NCJRL.org

"inside the box, outside the box"

Outside the box

The Box

obtaining evidence



investigating on the internet /networks

three different legal frameworks

1. obtaining info that has no legal regulation
2. Fourth Amendment
3. statutory regulation

typical steps in Internet digital investigation

- part #1: Outside the box: network investigations
  - Tracing electronic communications

    E.g., finding IP (Internet protocol) address
  - Identifying suspect and account

part #2: Getting to and inside the Box:

- Identifying who was at keyboard when crime occurred
- Locating computers to be searched
- Obtaining warrant or consent to search
- Searching and seizing evidence
- Forensic analysis

uncertain F/A applicability outside the box

non-consensual interception of communications, etc, over the Internet to another party

example: email

possible analogies:

its like a letter in the mail

its like numbers dialed on a telephone

its like any info possessed by third party

statutory protections tend to supercede

Congress /states have enacted some statutory regulation of computer network investigations:

- Stored Communications Act
- Wiretap Act
- Pen Register / Trap and Trace

case example

United States v. Perrine,
518 F.3d 1196 (10th Cir. 2008)

Vanlandingham tells police

- **in Yahoo! chat room using screen name "dana_hotlips05," chatted w/ "stevedragonslayer"**
- **"stevedragonslayer" invited him to watch web cam video of nude 6 to 9 year-old girls**
- **V-- informs "stevedragonslayer" he likes "young hard stuff"**
- **"stevedragonslayer" plays videos of young girls in explicit sexual acts**
- **gives police copy of chat room conversation**

police use ECPA to get Yahoo! subscriber info for screen name "stevedragonslayer"

- **records: "stevedragonslayer" logged on to Yahoo! website from address 68.103.177.146**

- **Electronic Communications Privacy Act ("ECPA") regulates disclosure of electronic communications and subscriber information**
- **IP (Internet Protocol) address is unique to specific computer at any one time**

Yahoo records:

"stevedragonslayer" logged in on Yahoo website from IP address

68.103.177.146

what do you do next?

go to: IP locator service

http://whatismyipaddress.com/ip-lookup

publicly available tools: no legal regulation

search engines, public web sites, chat rooms, etc.

info available using advanced Internet tools

- **NS lookup, Whois, Finger, Traceroute, Ping**
- **Domain names, IP addresses, networks, contact persons**

IP address assigned to Cox Communications

- **What do you do next?**

  get disclosure order under SCA from Cox

- **Cox informs that *at the time* reported by Yahoo, IP address was used by account of**

  Steve Perrine
  11944 Rolling Hills Court
  Wichita, Kansas

  - **can get all subscriber info, including screen names, type and length of service, method of payment, etc**

next steps:

- **PA -- contacts Kansas authorities**

- **KS:**
  - **Steve Perrine has prior state conviction for sexual exploitation of child / still on probation**
  - **Wichita police obtain search warrant for Perrine's house**

warrant executed:

- **seize computer computer**
- **observe firearms / drug paraphernalia**

- **get amended search warrant to seizure those items**

- **forensic examination of Perrine's computer:**

16,000 images of child pornography

Perrine's legal claims: the big picture

- **ECPA**
  - **violations: no suppression**
  - **stds for obtaining info & what info police can get**

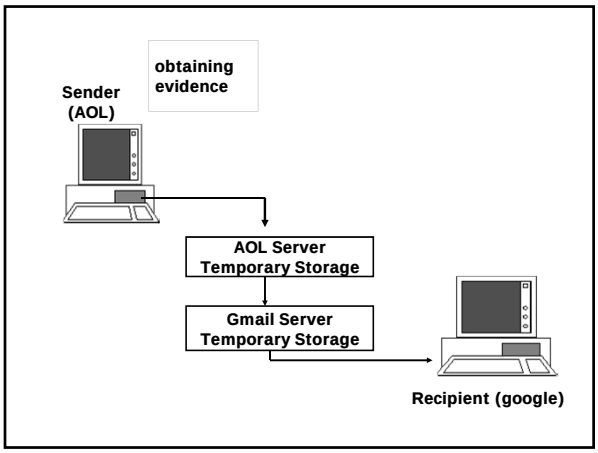
- **Fourth Amendment**
  - **no protection for subscriber info**
  - **no protection: P2P shared files**
  - **search of house did implicate F/A:**
    apply standards for warrant issuance and execution

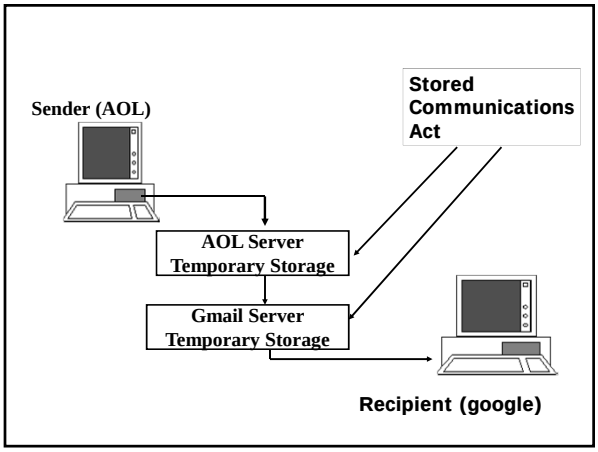
overview ---
statutory regulation of obtaining digital evidence

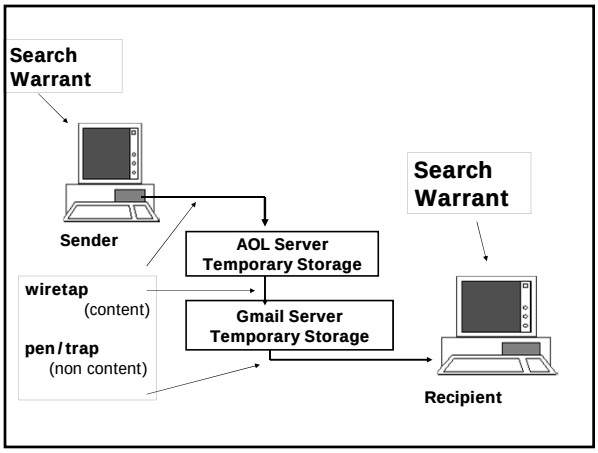
Congress /states have enacted "gap fillers"

- **ECPA**
- **wiretap**
- **pen register / trap and trace**

***See* summary in tab #1**


obtaining evidence
Sender (AOL)
AOL Server Temporary Storage
Gmail Server Temporary Storage
Recipient (google)


Stored Communications Act
Sender (AOL)
AOL Server Temporary Storage
Gmail Server Temporary Storage
Recipient (google)


Search Warrant
Search Warrant
Sender
AOL Server Temporary Storage
wiretap (content)
pen/trap (non content)
Gmail Server Temporary Storage
Recipient

significant statutory considerations

1. type of surveillance

   real time vs. stored info

2. type of information is gov't seeking

   content vs. non-content

Real time vs. stored surveillance

two types of Network surveillance

1. Real time: monitoring of communications in transit

2. stored records: retrospective surveillance

Statutory regulation depends on type of surveillance

type of information is gov't seeking

content:

the communication itself

non-content:

addressing information

pen registers

Device that records numbers dialed by telephone

Smith v. MD, 442 U.S. 735 (1979):

- robber kept calling victim
- **Have no REP in numbers dialed**
  1. doubted if any actual EP
  2. No REP
     -- voluntarily conveyed info to 3rd party
     -- assumed risk of disclosure

But what about automation?

"We are not inclined to hold that a different constitutional result is required because the telephone company decided to automate."

obtaining non-content

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

Pen Register / Trap & Trace

18 U.S.C. §§ 3121-3127

- get "dialing, routing, addressing, or signaling information"
- Not a search under 4th Amendment

  U.S. v. Forrester, 512 F.3d 500 (9th Cir. 2008)

  - to/from addresses
  - IP addresses of websites visited
  - volume of info to/from his account

Non-content Information

- Dialing, routing, addressing, or signaling information
- Basic customer or subscriber records
- Transactional information

same definitions as in SCA

Email Info with Pen/Trap

- get most e-mail header information
  - "To", "From"
  - IP address & port
  - For both source & destination
- But not
  - "Subject" line of e-mails
  - Content of downloaded file

Post-Cut Through Dialed Digits

- numbers dialed after call initially set up
- includes acct #s, pin numbers, ID #s, social security #, credit card #s

Content or Non-content?

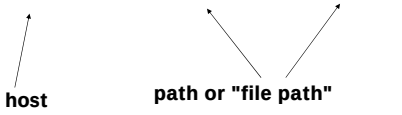
- In re Application, 515 F. Supp. 2d 325 (E.D.N.Y. 2007):

  "functional equivalent of the human voice"

URLs (uniform resource locators)

- Content or not?

www.biosupplies.com /mailorder /Anthrax.htm



In re application, 396 F. Supp. 2d 45 (D. Mass. 2005):
same as post-cut through digit extraction

Legal requirements for Pen / Traps

- gov't can get order when 18 U.S.C. § 3123
  1. authorized attorney applies under oath for order and
  2. assert that "information likely to be obtained is relevant to an ongoing criminal investigation"
- no independent judicial determination of 2

In re application

pen / trap remedies

- **no exclusion in criminal cases** ***See Forester***
- **Criminal penalties for violations**
- **Civil remedies for violations**

wiretapping -- yesteryears

Roy Olmstead

OLMSTEAD: **F / A did *not* apply**

1. **PROTECTS MATERIAL THINGS**
   - **tangible obj: -- (ex) letter**
   - **conversations not protected**
2. **LIMITED LIST OF TANGIBLES PROTECTED**
   - **phone lines not on list**
3. **AGAINST PHYSICAL INVASIONS**
   - **hearing not search or seizure**

Katz (1967)

excluding uninvited ear

- protects privacy
- protects against non-physical invasions

Wiretapping today

statutory framework has largely superceded F/A analysis

- Prohibits unauthorized government *AND* private party "real-time" interception of content
- Requires suppression of illegally intercepted oral and "wire" communications

wiretapping

wiretap?

Wiretap Act – "Title III"

18 U.S.C. §§ 2510-2522

- Regulates interception of **content** of communications in **real time** (not "stored")
- Applies to everybody (not just gov't actors)
- Establishes floor:

  state laws can be more restrictive, not less

Wiretap Orders

requirements include:

- need probable cause of specified felonies
- less intrusive techniques "reasonably appear unlikely to succeed"
- short time period (30 days)
- minimization requirements: avoid communications not subject to order

wiretap remedies

types of Communications:

Oral -- in person recording of human voice
Wire -- containing human voice
"Electronic" -- others, including email

- **statutory exclusion of evidence for**
  - **oral communications**
  - **wire communications**
- **NO suppression -- electronic communications**
- **Criminal & Civil penalties**

Stored Communications Act (SCA)

(18 U.S.C. §§ 2701-2712)

- **Controls disclosure of stored data on networked computers of –**
  - **non content &**
  - **content of stored data & communications**
- **Legal process varies, depending on information sought**

Compelled Production –types of process under SCA

- **Subpoenas**
- **Subpoenas *with notice***
- **"d" orders [§ 2703(d)]**
- **"d" orders *w/notice***
- **Search warrants**

applies to public and nonpublic providers

more process = more info

Compelled Production – subpoenas

- **Subpoenas: get basic subscriber info**

no prior notice to subscriber needed

  - **name and address**
  - **session records (time, duration)**
  - **telephone number**
  - **length of service, including starting date**
  - **types of services used**
  - **dynamic IP addresses**
  - **connection and session logs**
  - **means of payment (credit card, bank account numbers)**

Compelled Production – subpoenas with notice to subscriber

Get

- **contents in Electronic Storage more than 180 days**
- **contents in RCS, including open emails**
- **all info could have got w/ mere subpoena**

- **exception: 9th Circuit**
  need warrant for opened email
  Theofel v. Farey-Jones

Compelled Production – "d" orders

- **"d" orders [§ 2703(d)]: get account logs, transactional records**

- **all info could have got w/ lesser process**
- **Historical data involving past activity on account**
- **E-mail addresses of correspondents**
- **Web sites visited**
- **Cell-site data for cellular phone calls**
- **buddy lists**

- **Must show:**
- **specific and articulable facts that info sought is relevant and material to ongoing criminal investigation**

Compelled Production – "d" orders w/ notice

- all info could have got w/ lesser process
- Contents in RCS storage (including opened email)
- Contents in electronic storage more than 180 days

- Must show:
- specific and articulable facts that info sought is relevant and material to ongoing criminal investigation

Compelling Content Production: warrants

- Search Warrant: **gets everything !**
  - *may* always be needed when content sought
  - safer course: **Get warrant for *any* content**

SCA remedies

- **No exclusion of evidence**
- Criminal penalties for violations
- Civil remedies for violations