Typical Investigative Steps and Legal Framework

Thomas K. Clancy
Director

www.NCJRL.org

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
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
Compelled Production – types of process under SCA

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

more process = more info

Compelled Production – subpoenas

- Subpoenas: get basic subscriber info
  - 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)

no prior notice to subscriber needed

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. Farley-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
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://www.geoio.com

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 seize 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

- Gov’t fed his addiction: too stupid to talk about
applicability and satisfaction

IN EVERY CASE, ....

1. Does the 4th Apply?
   A. gov't activity: "Search" or "Seizure"
   B. Protected interest: liberty, possession, privacy

2. Is it Satisfied?
   "Reasonable"
   Warrant Clause requirements

[3. Remedies?]

Typical applicability issues

A. need Government Intrusion: "Search"
   assume government is examining digital evidence on computer

B. Intrusion must invade protected interest:
   reasonable expectation of privacy of 
   suspect

Expectation of Privacy Analysis

must have legitimate expectation of privacy invaded by 
gov't search

- two prongs
  1. individual has subjective expectation of privacy
  2. society recognizes that expectation as justified

- If either prong missing, no protected interest
Who's the actor?

Who's the actor?

A. need Government Intrusion:
   "Search"

private search doctrine
   1. purely private activity
   2. govt activity replicates private

B. Intrusion must invade protected interest:
   search --- invades reasonable expectation of privacy

Private Searches and Seizures

1. Computer Hackers
2. Computer Technicians
3. Government Replication of a private search
   -- When is REP extinguished?
   -- when if scope of private search exceeded?

inside the box:
   when does person have REP in data in computer?

examined a variety of situations

1. person's own computer
   -- info on screen
   -- data in computer
2. work and gov't computers
   -- monitoring and other policies that affect REP
   -- who has access to computer?
networks (outside the box): uncertain F/A applicability

- long list of situations where F.A. inapplicable because of voluntary disclosure to 3rd party
  - (ex) P2P, chatrooms
- content vs. non-content analogies:
  - its like a letter in the mail
  - its like numbers dialed on a telephone
  - its like any info possessed by third party

Satisfaction:

search warrant issues

1. warrant
2. application
3. attachments to application -

warrant issues covered

1. scope of permitted seizure
2. particularity of description of objects to be searched for and seized
3. probable cause
4. on site vs. off site searches
5. timing of forensic exams
where you come out is a function of where you go in

Are computers merely containers or something "Special?"

view #1: Data are Documents / Container Analogy

view #2: “Special Approach” to S/ of data on computers

View #1: Analogy to filing cabinets/ containers

“no principled distinction” between digital & paper records

computers hold “functional equivalent” of written material

Computer = container

warrant authorization includes containers reasonably likely to have items described in warrant

includes “nontraditional, technological containers”

View #2: Rejects Document S/ Container Analogy

must take "special approach" to s/ of data contained on computers

premise: writings & computers:

fundamentally different, both in degree and in kind
Consequences of "special" approach

1. Warrant sets out S/ limitations
2. Warrant may have to set forth S/ methodology
3. May require use of technical S/ engines
4. May require 2nd warrant for intermingled documents
5. Limits what is in Plain View

How to get that digital evidence without a warrant?

some traditional methods:

1. Search incident to arrest
2. Inventory
3. Consent

- registration
- agendas
- publications
- course descriptions
- scholarship info

this course

See handout

Power points and reference materials available at:

WWW. NCJ RL.org