Outside the Box: The Internet, Networks and New Technologies

Don Mason
National Center for Justice and the Rule of Law
The University of Mississippi School of Law
Objectives

- Identify and describe legal principles and statutes applicable to acquisition of digital evidence from remote network locations.
- Describe circumstances under which data transmitted or remotely stored via networks may be protected by the Fourth Amendment.
- Outline the processes by which investigators can obtain email or other data from third party providers.
Digital Evidence

**User-created**

- Text (documents, e-mail, chats, IM’s)
- Address books
- Bookmarks
- Databases
- Images (photos, drawings, diagrams)
- Video and sound files
- Web pages
- Service provider account subscriber records
Digital Evidence

Computer-created

- Dialing, routing, addressing, signaling info
- Email headers
- Metadata
- Logs, logs, logs
- Browser cache, history, cookies
- Backup and registry files
- Configuration files
- Printer spool files
- Swap files and other “transient” data
- Surveillance tapes, recordings
Digital Evidence Containers

- Home computers
- Office workstations
- Cell phones
- PDAs, other mobile devices
- Thumb drives, other external storage
- P2P network share folders
- Vehicles
- Network servers
- Internet & Online Service accounts
Internet Age Investigations

- Tracing electronic communications
  - E.g., finding IP (Internet protocol) address
- Identifying suspect and account
- Identifying person who was at the keyboard at the time of the crime
- Locating computers to be searched
- Obtaining warrant or consent
- Searching and seizing evidence
Investigators may wish to collect evidence *from networks*.

Ex’s:

- To obtain account records and stored email held by suspected fraudster’s ISP
- To conduct real-time surveillance of hacker’s account from within a victim network
- To obtain undercover chat room conversations with an online predator
“Outside the Box”

- Using Pen/Trap for Internet “DRAS” information
- Obtaining “PCTDD”
- Getting subscriber account records
- Acquiring communications from service providers
- Examining contents of private web sites
- Obtaining cell phone site location data
- Tracking via GPS devices
Information Sought

- Some is readily available to the public
  - Through search engines, public web sites, chat rooms, etc.

- Other “historical” information (domain names, IP addresses, etc.) is available through use of advanced Internet tools

- But some information may require certain legal process
Does Fourth Amendment apply?

A. need Government Intrusion: "Search"

B. Intrusion must invade protected interest:

reasonable expectation of privacy
Constitutional Protection?

Fourth Amendment protections for data transmitted or stored on networks has been, at best, unclear or debatable.
Analogies Used

Speech
- Sending data to remote computer likely eliminates a R.E.P. in the data

Letter or Package
- Sealed? – R.E.P. in contents but not exterior
- Opening sealed letter or package = “search”
  - But only while in transit
  - Delivery to 3rd party with some right of access may eliminate sender’s R.E.P.
Analogies

- Telephone
  - Calls protected against interception
  - No physical trespass required
  - Compared more to letters than to speech

- Any information held by third party
  - Bank account records
  - Telephone numbers dialed
    - *Smith v. Maryland*, 442 U.S. 735 (1979)
  - “Third party doctrine”
Can computer users ever have a R.E.P. in transmitted or remotely stored data?

What can “legitimate” expectations of privacy in remote computer data?

- “understandings that are recognized and permitted by society” [Rakas v. Illinois (1978)]
- Statutory privacy laws?

Congress and many states have enacted “gap filler” privacy protection statutes.
Statutory Protections

- **Real-time communications**
  Ex’s: telephone calls, e-mail

- **Stored communications**
  Ex’s: sent or received e-mail, voice mail, faxes

- **Subscriber account records**
  Name, address, phone numbers, type & length of service, CC no’s, etc.
Electronic Communications Privacy Act of 1986

- Authority, procedures for getting
  - live communications, or learning suspect’s location in real-time
  - communications stored in certain places
  - identifying information about communicators
Pen Register / Trap & Trace

18 U.S.C. §§ 3121-3127

For “dialing, routing, addressing, or signaling” information
- “To”, “From”, IP address & port
- For both source & destination
- No content

Not a search for Fourth Amendment purposes; analogous to use of pen register previously held (Smith v. Maryland) to not constitute a F.A. search

United States v. Forrester, 512 F.3d 500 (9th Cir. 2008)
Pen Register / Trap & Trace

But note:

At last count, 12 states require a Search Warrant for installation of a pen register, trap & trace, or DNR (dialed number recorder) under their state laws.
PCTDD

“Post-cut-through dialed digits”
Also obtainable with Pen/Trap?
Or closer to a wiretap?
Fourth Amendment analysis?
Stored Communications Act
18 U.S.C. §§ 2701-2712

- Prohibits unauthorized accessing of stored communications [§ 2701]

- Governs
  - *Voluntary disclosure* of wire & electronic communications or account records [§ 2702]
  - *Compelled disclosure* of communications or account records *to government* [§ 2703]
Voluntary Content Disclosure

- E-mails or files on company servers
  - Disclosure allowed

- E-mails or files on ISP servers
  - Disclosure not allowed unless exception applies
Compelling Content Production

- Unopened e-mail on ISP or company system
  - Need warrant (unless >180 days old)

- Opened e-mail or files on ISP server
  - Need order, or subpoena with notice, or warrant without notice

- Opened e-mail or files on company server
  - Ordinary subpoena should work – ECPA doesn’t apply
Compelling Content Production

For stored files & opened communications held by provider “to the public”

- Conventional view: May use a § 2703(d) “articulable facts” order or subpoena,
  but customer must be given notice (which can be delayed under § 2705)

- Can use a warrant without notice
Compelling Production

- Courts are reconsidering the “rules”
- In 9th Circuit, a warrant is needed even for opened email stored as “backup”

Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004)

Statutory construction result
Is there a *Fourth Amendment* R.E.P. in all email held by a third-party service provider, requiring a S.W. in all such cases?

*Warshak v. U.S.*, 490 F.3d 455 (6th Cir. 2007), *vacated*
Pager text messages

Are they private? Always?
Do users have a statutory expectation of privacy?
Or a constitutionally protected R.E.P.?

*Quon v. Arch Wireless*, 529 F.3d 892 (9th Cir. 2008),
petition for en banc review denied 1/27/09
Subscriber account records

Examples
- Name, address, telephone, IP numbers
- Connection & session logs
- Logs of web sites visited
- Other subscriber number or identity
- Payment information
Disclosure of Records

- No constitutional R.E.P. in account records – information entrusted to service provider
  
  *U.S. v. Perrine*, 518 F.3d 1196 (10th Cir. 2008)

- But at least one state – New Jersey – has held that such records are protected under the state’s constitution.
  
  *State v. Reid*, 945 A.2d 26 (2008)
Voluntary Records Disclosure

Public providers may disclose

- To law enforcement when required by warrant or other legal process
- To other than government, for any reason
- With consent of customer or subscriber
- To provide service
- To protect provider’s rights or property
Voluntary Records Disclosure

Public providers *may disclose*

- To *government* if *good faith* belief by provider that *emergency* necessitates disclosure to prevent death or serious physical injury
- To NCMEC if *child pornography* involved
Compelling Records Disclosure

A subpoena, without notice, can get “basic customer or subscriber records”

– Name & address
– Telephone number
– Length of service, including starting date
– Types of services used
– Dynamic IP addresses
– Connection and session logs
– Credit card or bank account number
Compelling Records Disclosure

- Any other “record or other information pertaining to a subscriber or a customer” (“transactional” records) requires
  - Articulable facts order [18 U.S.C. § 2703(d)]
    - Notice to subscriber *not* required
  - Can also use a search warrant or consent
Password protected web sites

- When is there a F.A. “search”?
- Is there a reasonable expectation of privacy in the contents of a web site?
- When?
- What factors determine?

Cellular Telephones
Sample Tower/Sector
Disclosure of Cell Site Location Data

- May government obtain historical or prospective cell site location data from telecommunications providers without a probable cause warrant?

- A divisive issue for the courts.
Basic Approaches

- Some courts have held that disclosure orders can be lawfully issued on the same basis as a pen register order.

- Other courts have held that federal law does not permit the issuance of such orders without full warrant / wiretap protections.
Pen Register Statute and Stored Communications Act, considered together with the Communications Assistance for Law Enforcement Act (CALEA), permitted a court to authorize the disclosure of prospective cell site information.
Communications Assistance for Law Enforcement Act (CALEA)

- Purpose of CALEA is:
  - To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes…
“Permitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concerns especially when the phone is in a house or other place where privacy is reasonably expected.”
Fourth Amendment basis

- One court acknowledged that while there might not be any “legitimate expectation of privacy in the telephone numbers dialed from a particular telephone,” it does not necessarily follow that the user “abandons any expectation of privacy in his or her location by carrying a cell phone” that emits a signal.

- Question based on location may depend on whether the user is in an area (like the home) that could not be observed from public spaces.
“True GPS”

“Handset solution”
- The data is “inside the box”
- Involves search of the device
Peer-to-Peer (P2P) Networks

- Rapidly evolving file-sharing technology
- Virtual networks
- Popular for downloading music and movies
- Reduced reliance on search engines
- Increased efficiency of data transfer
Client-Server vs. Peer-to-Peer

The Client-Server Model

The Peer-to-Peer Model
Next Generation of P2P

- After litigation essentially destroyed “broker/server” model
- Most new systems used “decentralized” file sharing
- Allow exchange of any type of computer data
How Gnutella Works

query: "Baby Go Home.mp3"

6-7 levels depending on "time to live"

"I've got it!"

8,000 - 10,000 computers
Criminal Activity With P2P

- Copyright Infringement
- Computer Hacking
  - Worms
  - Viruses
  - Theft of private information
- Child Exploitation and Pornography
Considerations

- By default, Kazaa/Imesh/Grokster software share all downloaded files.
- Broadband use turned home computers into distributed super-networks for sharing files.
- Design of networks fault tolerant and load balancing.
Considerations

- Users on Internet voluntarily
- Users can decide, through settings in the software, how much or how little of their computers will be open to viewing by others on the Internet
Considerations

- Every download is exact duplicate of the original image
- Internet Protocol (IP) Address of individual user can be ascertained (identifying unique computer)
- Successful tracking of IP address reveals computer that had the file available for distribution
Law Enforcement Response

- Large scale investigations looking for child pornography
- Searches over file sharing networks for known child porn images
Queries

- Is it a “Search”?
- Does a computer user connected to the Internet via a peer-to-peer network have a reasonable expectation of privacy in her computer?
Questions?

Don Mason
Associate Director
National Center for Justice and the Rule of Law
662-915-6898
drmason@olemiss.edu
www.ncjrl.org