Fourth Amendment considerations involving digital evidence

Thomas K. Clancy
Director
National Center for Justice and the Rule of Law
The University of Mississippi School of Law

---

the good old days

---

Data Generated in 2006

- 161 billion gigabytes
- 12 stacks of books reaching to the Sun
- 3 million times all the books ever written
- need 2+ billion iPods to hold it
the crime scene

“Cyber Crime”

- “Computer crime”
- “Network crime”
- “Computer-related crime”
- “Computer-facilitated crime”
- “High tech crime”
- “Internet crime” or “Online crime”
- “Information age crime”

Any crime in which a computer or other digital device plays a role, and thus involves digital evidence.

new crimes & new techniques

computer as Target
- unauthorized access, damage, theft
- spam, viruses, worm
- denial of service attacks

computer as Tool
- fraud
- threats, harassment
- child pornography

computer as Container
- from drug dealer records to how to commit murder
just a murder!

- studied currents
- researched bodies of water
  - including San Fran Bay
- how to make cement anchors
- tide charts

had 5 home computers

Digital Evidence

Information of probative value that is stored or transmitted in binary form and may be relied upon in court.

two types:
1. user created
2. computer created

Digital Evidence

User-created

- Text (documents, e-mail, chats, instant messages)
- Address books
- Bookmarks
- Databases
- Images (photos, drawings, diagrams)
- Video and sound (films, voice mail, .wav files)
- Web pages
- Hidden files
Digital Evidence

Computer-created
- Email headers
- Metadata
- Activity logs
- Browser cache, history, cookies
- Backup and registry files
- Configuration files
- Printer spool files
- Swap files and other “transient” data
- Surveillance tapes, recordings

meta data

“Information about the Data”

track changes function
digital camera images -- metadata
- date, time taken
- exposure information (lens, focal length, flash, F-stop, shutter speed)
- serial number
- description of photograph
- location where taken

sources of digital evidence

phones, PDAs
Digital surveillance

Chicago’s 911 Network

Houston police drone

Houston Police use DRONES to spy on AMERICANS - Local 2 news.flv
GPS devices

- how they work:
- benefits?

http://www.youtube.com/watch?v=dnpelpHmm8M
Challenges

- Criminals using technology
- Increasing ubiquity of digital devices
- “Convergence”
- Growth of data storage capacities
- Reduction in size of devices and media
- Crime “migration” to Internet

published search and seizure appellate ct. decisions

<table>
<thead>
<tr>
<th>Year</th>
<th>STATE</th>
<th>FEDERAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>13 (10)</td>
<td>19 (16)</td>
</tr>
<tr>
<td>2008</td>
<td>13 (10)</td>
<td>17 (13)</td>
</tr>
<tr>
<td>2007</td>
<td>9 (5)</td>
<td>14 (9)</td>
</tr>
<tr>
<td>2006</td>
<td>17 (9)</td>
<td>14 (8)</td>
</tr>
<tr>
<td>2005</td>
<td>13 (6)</td>
<td>20 (15)</td>
</tr>
<tr>
<td>2004</td>
<td>14 (11)</td>
<td>6 (4)</td>
</tr>
<tr>
<td>2003</td>
<td>7 (6)</td>
<td>6 (6)</td>
</tr>
<tr>
<td>Pre-2002</td>
<td>22 (12)</td>
<td>33 (18)</td>
</tr>
<tr>
<td><strong>total</strong></td>
<td><strong>117 (78)</strong></td>
<td><strong>136 (95)</strong></td>
</tr>
</tbody>
</table>

253 total
173 Child Porn
68 %

green - total cases
yellow - Child Porn
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 steps in digital investigation

Outside the box: network investigations
- Tracing electronic communications
- Identifying suspect and account

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

when does person have REP in data in computer?

Case law has examined 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?

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

obtaining evidence

Sender (AOL) → AOL Server
Temporary Storage

AOL Server
Temporary Storage

Earthlink Server
Temporary Storage

Recipient (Earthlink)

Sender (AOL) → Stored
Communications Act

AOL Server
Temporary Storage

Earthlink Server
Temporary Storage

Recipient (Earthlink)
Traditional F/A doctrine

No F/A Protection from 3rd Party Disclosures to Gov’t

Rationale: Risk Analysis -- Voluntary Exposure

misplaced belief to whom voluntarily confides will not reveal secret

Miller

such “risk” is “probably inherent in the conditions of human society’

Hoffa

voluntary disclosure

assume risk that third party will disclose information, item to gov’t
Peer-to-Peer (P2P) Networks

file-sharing technology --- creates virtual networks

criminal activity:

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

How Gnutella Works

6-7 levels depending on "time to live"

1.000 - 10,000 computers
Considerations

- User on Internet voluntarily
- User decides, through settings in software, how much of computer open to others on Internet
- Every download exact duplicate of original

Law Enforcement Response

search file sharing networks for known child porn images

Questions:

- “Search” w/ in meaning of 4th Amendment?
- Does user connected to Internet via P2P have reasonable expectation of privacy in files in shared folders?

Operation Fairplay
**no REP in P2P**

U.S. v. Ganoe, 538 F.3d 1117 (9th Cir. 2008)

**P2P network**

"To argue that Ganoe lacked the technical savvy or good sense to configure Lime Wire to prevent access to his child pornography files is like saying that he did not know enough to close his drapes."

**US v. King, 509 F.3d 1338 (11th Cir. 2007)**

Connected own laptop in his dorm room to military base network

Knew activities on network subject to monitoring

Airman looking for music found porn on King’s computer

After report, investigator located King’s computer on network

- Found porn file
- Additional CP files

REP?

Hard drive contents "akin to items stored in the unsecured areas of a multi-unit apartment building or put in dumpster accessible to the public"

**same principles applied --- No F/A protection against**

1. Disclosure of subscriber info by ISPs

2. Email recovered from recipient


3. Internet chat rooms

   **doctrines:**
   - Voluntary exposure
   - Assumption of risk

4. Posting info on a Website
application of principles to --

1. Virtual worlds
2. Cloud computing
3. Web based data storage

What are the relevant considerations?

Virtual worlds

- Create your own virtual space
- Chat and interact with your friends in rooms you create
- Express yourself by customizing your avatar and streaming personal videos and photos
- Add your room to your site by inviting your friends to chat and decorate

AVATAR - Graphical representation of you.
(note) - It's probably not a realistic depiction.
cop sent text messages to wife, mistress via gov’t issued pager
duty to review printouts obtained from provider to determine if
more capacity needed for police business

Issues:
1. Quon have REP in messages?
2. Wife / mistress have REP in messages?

City of Ontario v. Quon, 529 F.3d 892 (9th Cir. 2008), cert. granted __ S. Ct. __ (December 14, 2009) No. 08-1332.

Formal Written Policy
- explicitly said user had no REP
- could audit, monitor, or log all activity
- not for personal use
- Quon aware of and signed

Informal Policy
- Lt. Duke: you pay overages, will not audit
Should Q be treated differently than Wife / mistress?

Possible analogies as to the items:

- Its like letter in mail
- Its like numbers dialed on telephone
- Its like any info possessed by third party

The Problem:

- How to regulate searches for Data?

1. Does the 4th Apply?

2. Is it Satisfied?
   - "Unreasonable"
   - Warrant Clause requirements

3. Remedies?

What Is Reasonable?

The core 4th Amendment concept -- its meaning serves to regulate:

- Under what circumstances s/s may occur
- Scope of the intrusion
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

Document Searches

Andresen v. Maryland: warrant for --

specific docs re -- lot 13 T “together w/ other fruits, instrumentalities ... of crime"

- upheld s/ of law office
- cannot use complex scheme to avoid detection when police have PC suspect has evidence

Andresen:

- "Some innocuous documents will be examined, at least cursorily"
- officials & judges must assure s/ minimizes unwarranted intrusions upon privacy
View #1: Analogy to filing cabinets/ containers

Rationale: Computer is a Container
- cannot anticipate form of “records”
- “no principled distinction” between digital & paper record
- scope: includes all containers reasonably likely to have items described in warrant

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

Example of special approach

U.S. v. Payton, 573 F.3d 859 (9th Cir. 2008)

Facts: warrant for search of financial records in drug case – did not explicitly authorize s/ of computers

“It is true ... that pay/owe sheets indicating drug sales were physically capable of being kept on Payton’s computer.”

Held: s/ violated F/A

Contrary ruling “would eliminate any incentive for officers to seek explicit judicial authorization for searches of computers.”
Why Computers are “Special”

- vast array of information
  - documents
  - financial records
  - business records
  - e-mail
  - Internet access paths
  - deleted materials
- ability to sort, process, and transfer info
- means for communication via e-mail
- connects to Internet
- important privacy concerns

CAUTION: technology rapidly growing and changing

some underlying concerns with Wholesale Seizures

1. Potential disruption and invasion of business, professional practice, personal lives
2. General Warrants -- a principal vice the Fourth Amendment was supposed to prohibit!

Consequences of “special” approach

1. warrant sets out S/ limitations
   (ex) file names, extensions, date range
2. Warrant sets out S/ methodology
   (ex) key word s/ for relevant terms
3. May need use of technical S/ engines
   (ex) ENCASE, FTL, etc
4. May need 2nd warrant for intermingled documents
5. Limits what is in Plain View
situation: have properly seized large amount of media

What is the proper method to search?

Search protocols -- which are "Reasonable?" should one be required?

- possibilities:
  - new 9th circuit rule
  - special masters
  - taint teams
  - magistrate review
  - technological restrictions on scope of search
  - no special rules: just "reasonableness"

situation: have properly seized large amount of media

warrant for drug tests of 10 players

actual seizure was:

- 25 page list of all BB players, who were tested for drugs during 2003 season
- list of positive drug tests of 8 of 10 players sought
- medical records of individuals in 13 other sports, 3 businesses, and 3 sports competitions

1. Magistrates "should insist" gov't waive reliance upon plain view doctrine

2. Segregation and redaction must be either done by specialized personnel or an independent third party.

   -- if done by gov't computer personnel, must agree in warrant application that computer personnel will not disclose to investigators any info other than that which is target of warrant

3. Warrants/subpoenas must disclose actual risks of destruction of info and prior efforts to seize the info in other judicial fora
4. search protocol must be designed to uncover only info for which gov’t has probable cause and only that info may be examined by case agents

5. gov’t must destroy or, if recipient may lawfully possess it, return non-responsive data, keeping issuing magistrate informed about when it has done so and what it has kept

special masters

where large volume of data seized from D’s law office:

special master to decide what data responsive to SW or w/ in exception such as plain view


procedure

1. execution team composed of federal agents seizes or copies ALL computer media

2. agent not otherwise involved in investigation designed to review media to determine responsiveness to warrant

3. (AUSA not otherwise involved screens materials identified in step 2 for privileged materials)

4. (AUSA then meets and confers w/ DEF on privilege questions)

5. (if cannot agree, AUSA goes to CT for judicial determination of privilege)


procedure “reasonable” -- rejected special master alternative
other "special" rules

1. Must limit search to certain terms, dates, etc.
   
   E.g., People v. Carratu, 755 N.Y.S. 2d 800 (S. Ct. 2003)

2. Get a second warrant
   
   E.g., Carey

rejection of special execution rules:

U.S. v. Brooks, 427 F.3d 1245 (10th Cir. 2005)

... we disagree with Brooks that the government was required to describe its specific search methodology. This court has never required warrants to contain a particularized computer search strategy. We have simply held that officers must describe with particularity the objects of their search.

Is this also true of post search inquiries into "Reasonableness?"

U.S. v. Hill, 459 F.3d 966 (9th Cir. 2006)

must demonstrate factually need in each case

must explain why cannot describe objects of search more specifically

"seize the haystack to find the needle"

What's the remedy for overbroad seizure?
Technological premise of "Special Approach"

Papers:
no way to determine what to seize w/o some review of everything in cabinet

Computers: tools can refine S/ ----
tailor S/ by, inter alia:
* limit by date range
* key word S/
* limit by file type

premise: file name labels / extensions accurate

Different storage formats make info stored in file "easily ascertainable"

[ex] financial spreadsheets store info in different format than word processing programs

Conclusion:
If S/ warrant for financial records, cannot look at telephone lists, etc, absent showing other files have financial records

Carey example

warrant to S/ computer files for
names, telephone numbers, ledger receipts, addresses, other documentary evidence pertaining to sale and distribution of controlled substances

search execution:
files w/ sexually suggestive, obscene names
--- many w/ "teen" or "young" JPG extension

* 1st file opened: child porn
* more "jpg" files opened: child porn
**Tenth Circuit:**

Files w/ porn labeled "JPG" w/ sexually suggestive title

After 1st child porn file, Lewis aware:

* before opening files -- what label meant

* knew not going to find drug related activity

**Lewis ABANDONED permitted search**

---

**Critics of limits by file name / suffix**

Professional investigators: Must S/ all stored data

Conceal -- store in random order w/ deceptive file names

Cannot tell what storage medium contains by looking at names, suffix

**Courts:**

Like saying may not seize plastic bag w/ white powder labeled "flour" or "talcum powder"

Disguise easy: sexyeenyboppersxxx.jpg

-- renamed -- sundayschoollesson.doc

---

**Utility of Technological S/ Programs**

**Q#1: Technical Question:**

Can technological search programs reliably sort info?

* search engines -- none 100% reliable
  -- many investigators do not rely exclusively on

* electronic storage evolves
  -- gov't must keep pace or catch up
  -- previous quotes of professionals: need to examine to insure
Q#2: Constitutional Question

Even if S/ programs adequate to ID relevant materials, MUST they be employed?

Considerations:

* Technology a moving target
* Basis for in F/A?
  1. Does S/ have to be least intrusive or merely reasonable?
  2. Basis in F/A to specify S/ methods in advance?

Constitutional basis for mandating execution procedures?

1. *Andresen:* for document S/
   
   “Responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.”

2. *Plain language:* Warrant Clause requires --
   - Oath
   - Probable cause
   - Particular description of place to be S/

*Warrant Clause or Reasonableness Clause?*

*Dalia / Grubbs:*

Reject view: Warrants must specify manner of execution

Executing officers decide how to execute warrant

Nonetheless, “the manner in which a warrant is executed is subject to later judicial review as to its reasonableness.”

*U.S. v. Grubbs, 547 US 90 (2006)*
Intermingled Documents

Should amount of intermingled materials change analysis?

* Diaries often contain evidence unrelated to crime
* Filing cabinets often hold
  - paper, business related and otherwise
  - office supplies
  - personal items

Should filing cabinets, diaries, books, floppy drives, hard drives, and other storage devices have different rules?

Supreme Court rejects ranking containers

Tried to distinguish among containers:

* luggage -- high expectation of privacy
* other containers did not "deserve full protection of F/A"

REJECTED

- no basis in language of F/A: "protects people and their effects, whether they are 'personal' or 'impersonal'"
- "impossible to perceive any objective criteria" for viable distinction:

"What one person may put into a suitcase, another may put into a paper bag."

Some developing issues

Applying established rules to digital evidence containers

1. searches incident to arrest
2. border searches
Scope of consent search of cell phone ??

interviewed by police re - involvement w/ minor

- asked: had he been "calling her on telephone"
- asked: could cop see his cell phone
- L handed phone to police
- cop, after examining call info on phone, pressed "camera" button and observed CP

Lemon v. State, 298 S.W.3d 658 (Tx Ct App. 2009)

Lemon v. State, 298 S.W.3d 658 (Tx Ct App. 2009)

extended discussion in ---


www.NCJRL.org

pizza!