Search and Seizure Developments involving digital evidence

Thomas K. Clancy
Director

National Center for Justice and the Rule of Law

The University of Mississippi School of Law

Amendment IV

Reasonableness clause:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,

Warrant clause:

and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Digital Evidence Searches and Seizures

1. **Is the Fourth Amendment applicable?**
2. **Is it satisfied?**
   - **two approaches to digital evidence**

conceptual difficulties of applying traditional doctrines to digital evidence

Applicability

Does the 4th Apply ?

part A: need gov't activity:
"Search" or "Seizure"

part B: that activity must intrude upon a
protected interest

Reasonable expectation of privacy test

1. person exhibits **actual, subjective expectation of privacy**

2. society recognizes that expectation as
Justified / Reasonable / Legitimate

Smith v. Maryland, 442 U.S. 735, 740 (1979)

If either prong missing, no protected interest

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

vol. exposure to public eliminates F/A protection
Katz

voluntary disclosure

assume risk that third party will disclose information, item to gov't

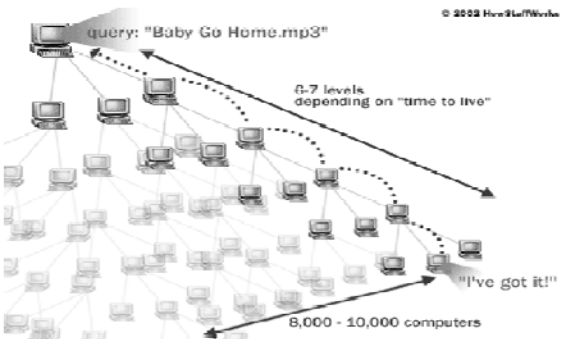
Peer-to-Peer (P2P) Networks

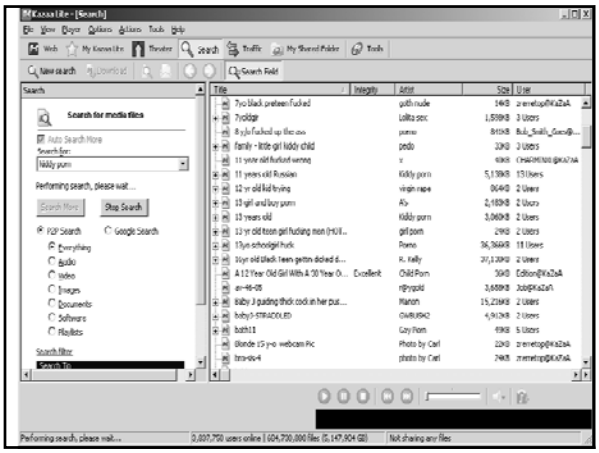
file-sharing technology --- creates virtual networks

criminal activity:

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

How Gnutella Works



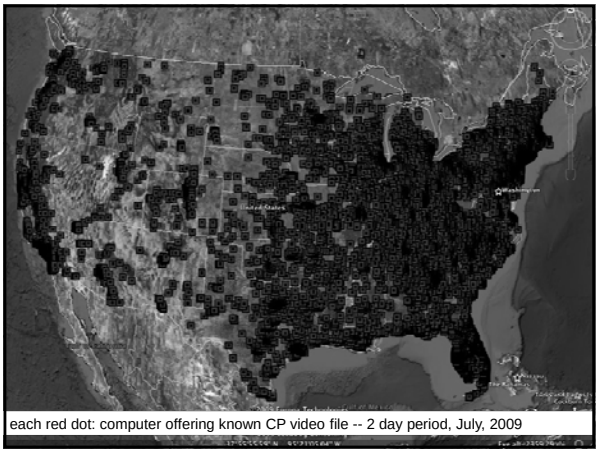


Law Enforcement Response

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?**



each red dot: computer offering known CP video file -- 2 day period, July, 2009

no REP in P2P

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

"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."

City of Ontario v. Quon, 130 S. Ct. 2619 (2010): ***some answers?***

- **cop sent text messages to wife, mistress via gov't issued pager**
- **agency reviewed printouts obtained from provider to determine if needed more capacity for police business**

issues:

***See* memo for full summary**

1. **Quon have REP in messages?**
2. **Wife / mistress have REP in messages?**
3. **Was search Reasonable ?**

police pager policies

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**

Quon: NO answers

- "case touches issues of far reaching significance"
- concern: "broad holding" on REP "might have implications for future cases that cannot be predicted"

Therefore:

1. assumed Quon / women had REP
2. search reasonable

dicta on REP analysis -- *possible* factors

- Duke's statements change in policy?
- did Duke have "fact or appearance" of authority to change / guarantee REP
- should public / private employees be treated differently
- gov't had interests to review messages:
  - performance evaluations
  - litigation on lawfulness of police actions
  - comply w / open records laws

- Rapid changes in communication
- many employers expect / tolerate personal use
- employer policies "especially" when "clearly communicated"
- some state statutes require employers to notify when monitoring electronic communications
- uncertain evolution of **workplace norms** / law's treatment

- **Cell phone / text messaging pervasive -- hence:**
  - **one view:**

    "essential means or necessary instruments for self-expression, even self-identification"
  - **another view:**

    due to ubiquity / affordability employees can buy own

Scalia, concurring

- **Applicability discussion "unnecessary" & "exaggerated"**
- **rejects "implication" about electronic privacy that Ct should decide less –**

  The-times-they-are-a-changin' is a feeble excuse for disregard of duty.

- **courts/ litigants likely to use dicta as "heavy-handed hint about how they should proceed"**

The Court's standard

"is (to put it mildly) unlikely to yield objective answers"

Smiling Bob meets the 6th Circuit

Is email protected by Fourth Amendment?

Warshak #1,
532 F.3d 521 (6th Cir. 2008) (en banc)

QUESTION not ripe:

privacy expectations

- **"may well shift over time"**
- **"shifts from internet-service agreement to internet-service agreement"**
- **requires knowledge about ever-evolving technologies**

---

variety of agreements

Service providers ....

- **will "not ... read or disclose subscribers' e-mail to anyone except authorized users"**
- **"will not intentionally monitor or disclose any private email message" but "reserves the right" to do so in some cases**
- **right "to pre-screen, refuse or move any Content that is available via the Service"**
- **e-mails will be provided to government on request**
- **other individuals will have access to email / can use information**
- **no REP in any communications**

U.S. v. Warshak (#2),
631 F.3d 266 (6th Cir. 2010)

SCA subpoena on less than probable cause violates 4th Amend

- analogy to letters / phone calls
- ISP = post office / telephone company

- subscriber agreement: limited access only to protect ISP

- not holding: subscriber agreement will *never* be broad enough to snuff out REP .... if ISP intends to "audit, inspect, and monitor" emails, might be enough

Digital Evidence Searches and Seizures

Satisfaction issues

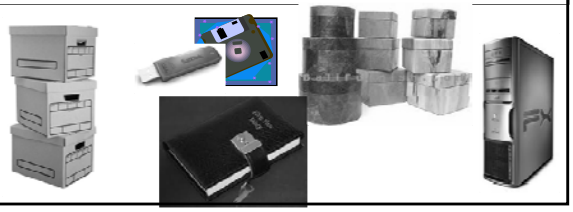
conceptual difficulties of applying traditional doctrines to digital evidence

where you come out is function of where you go in

Are computers containers or something "Special?"

view #1: Data are Documents / Container Analogy

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



Plain view & computers

contents of unopened files

View #1

data analogous to document search: can look at all data to ascertain value

View2 "special approach"

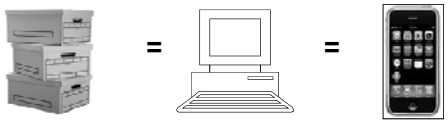
imposes limitations on search to restrict application of plain view doctrine

View #1: Analogy to filing cabinets/containers

RATIONALE: Computer is a Container

- **cannot anticipate exact form of "records"**

"no principled distinction" between digital & paper records



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

- two views: apply to ***all*** digital devices

Can police search Cell Phone incident to arrest?

- **YES: are containers – based on "binding" SCT precedent**
  People v. Diaz, 244 P.3d 501 (Cal. 2011)
- **NO: are <u>not</u> containers and persons have "higher level of privacy" in info "they contain"**
  State v. Smith, 920 N.E.2d 949 (Ohio 2009)

example of special approach

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

FACTS: warrant for 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."

some "special" approach limits on scope of search

- **warrant sets out S/ limitations**
  - **restrict by file name, extension, date range**
- **Warrant sets out S/ methodology**
  - **key word s/ for relevant terms**
  - **ENCASE, FTL, etc**
  - **explicit protocols**
- **need 2nd warrant for intermingled documents**
- **use third party to sort**
  - **taint teams, special masters, magistrate review**

U.S. v. Comprehensive Drug Testing, 579 F.3d 989 (9th Cir. 2009)

- **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**

en banc decision

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 personnel, must agree in warrant application that 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

CDT -- rehearing en banc #2

new opinion: **621 F.3d 1162 (9th Cir. 2010)**

5 rules of en banc #1 now in concurring opinion

majority: views digital evidence as special category

- **rejects plain view**
- **requires prior approval in warrant for execution procedures**

CDT -- rehearing en banc #2

goals:

maintain privacy of intermingled materials

Avoid general searches

_____

"obvious case of deliberate overreaching by the gov't ... to seize data as to which it lacked PC"

rejection of special execution rules:

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

Rejects view -- Govt must describe search methodology

"We have simply held that officers must describe with particularity the *objects of their search."*

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)

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"

VS

officials & judges must assure S/ minimizes unwarranted intrusions upon privacy

Supreme Court rejects ranking containers

at one point, tried to distinguish among containers:

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

REJECTED

- 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."

"Special approach" is inconsistent with Supreme Court cases

1. U.S. v. Grubbs, 547 U.S. 90 (2006)
2. Dalia v. U.S., 441 U.S. 238 (1979)

   both reject implicit warrant issuance requirements

3. Andresen v. Maryland, 427 U.S. 463 (1976)

   permits broad document search

4. U.S. v. Ross, 456 U.S. 798 (1982)

   rejects distinctions between containers

2011 Supreme Court term

United States v. Jones

issues:

- Is installation of GPS device a seizure?
- 24 hour tracking for 30 days a search?

Jones possible outcomes:

1. **Warrantless installation of GPS device *is* an illegal seizure**
   - **avoids "search" issue on warrantless surveillance**
2. **tracking for 30 days is *not* a search**
   - **merely follows precedent**
3. **Cert. improvidently granted**
   - **had warrant !**

Extended discussions and citations on subject:

www.NCJRL.org

- **Clancy, Fourth Amendment: Its History and Interpretation – semi-annual supplement**
- **Clancy, The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer, 75 Miss. L.J. 193 (2005)**