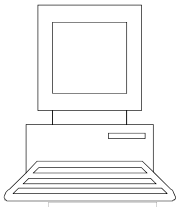
## Fourth Amendment Applicability

expectations of privacy *inside* the box

*Thomas K. Clancy*
Director

www.NCJRL.org

*"inside the box, outside the box"*



The Box

Outside the box: network investigations

## structure of 4th Amendment analysis

IN EVERY CASE, ....

*see* memo in tab#1 for outline

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?]

Applicability

## Does the 4th Apply ?

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

**part B:** that activity must intrude upon a **protected interest**

***this presentation is about Part B***

---

**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*

---

**protected interests**

***4th:***

**"The right of the people to be SECURE in their persons, houses, papers, and effects . . . ."**

**step #1: is object on list?**

**person, house, paper, or effect**

**step #2: quality protected?**

**does defendant have protected interest in that object implicated by gov't activity?**

**Privacy: main interest protected**

**"The *principal object of the Amendment is the protection of privacy . . . "***

**Soldal**

**Gov't Activity: "SEARCH"**

**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***

**partial list -- NO R.E.P.**

**Prison Cells**
**Handwriting**
**Facial Characteristics**
**Movements Outside**
**Open Fields**
**Bank Records**
**Trash**
**VIN numbers**
**Field testing of suspected drugs**

***NO PROTECTED INTEREST -- F/A does NOT apply --***

**How to find "legitimate" expectation of privacy?**

***look to:***

**1 real property law**

**2 personal property law**

**3 "understandings that are recognized or permitted in society"**

**California v. Ciraolo, 476 U.S. 207 (1986)**
**Rakas v. Illinois, 439 U.S. 128 (1978)**

**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?**

## Data on Work Computers – Governmental Employer

**Whether REP in gov't computers: case-by-case analysis**

**Factors:**

***context of employment relation**

*** access of other employees, public**

*** office policies, practices, or regulations**

**[ex] teacher -- no REP in computer owned by school district on desk in computer laboratory used to teach students about computers**

**Voyles**

## Monitoring policies

**if no monitoring policy & no routine access by others to computer, may have REP in files**

**[ex]** ***Leventhal:*** ***Def*** **had REP in computer in his office when**

- ***had exclusive use**
- *** no routine S/ practice**
- *** no notice of no REP in computer**

**despite**

- ***technical staff had access to computer**
- ***but maintenance normally announced**
- *** 1 unannounced visit to change name of server**
- *** occasional S/ of unattended computer for needed document does not defeat REP**

## Policies reserving right to Inspect / Audit defeat REP

1. **employee's written acknowledgement of agency policy, which**
   - *** prohibited personal use**
   - *** stated employees had no privacy rights**
   - *** stated employee consents to inspection / audit**

   ***Thorn***

2. **school dist. reserves right to "access all information stored on district computers"**

   ***Wasson***

**Data on Work Computers – Private Employer**

***analysis similar to public employer***

***NO REP in computer provided by employer when***

1. **employer reserves right to inspect**

   *Muick*

2. **company requires employee to assent to S/ every time employee accessed computer**

   *Bailey*

**Monitoring Policies continued . . . .**

*** D connected his computer (in his dorm room) to university network -- used it hack into corp. computer network.**

**Policy:**

**"In general, all computer and electronic files shall be free from access by any but the authorized users of those files. Exceptions to this basic principle shall be kept to a minimum and made only where essential to ... protect the integrity of the University and the rights and property of the state."**

**U.S. v. Heckenkamp, 483 F.3d 1142 (9th Cir. 2007)**

**Defendant used his own computer at work**

**US v. Barrows, 481 F.3d 1246 (10th Cir. 2007)**

**city treasurer -- shared work space with city clerk in open area of city hall**

*** public excluded but other workers routinely used space to access fax machine, use copier**

*** only one Govt computer shared with clerk**

*** brought in home computer and connected it to network**

***allowed clerk to use either computer to access city files**

*** left computer running continuously -- even weekends**

**Barrows .....**

*** clerk had problems with city computer, complained to cop (former computer sales)**

*** cop tinkered with city computer and then Barrow's to attempt to fix (he thought a file might be open on B's)**

***GUESS WHAT HE FOUND??**

**does Barrows have a REP in his *own* computer???**

**Traditional F/A doctrine**

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

**<u>Rationale:</u>** ***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***

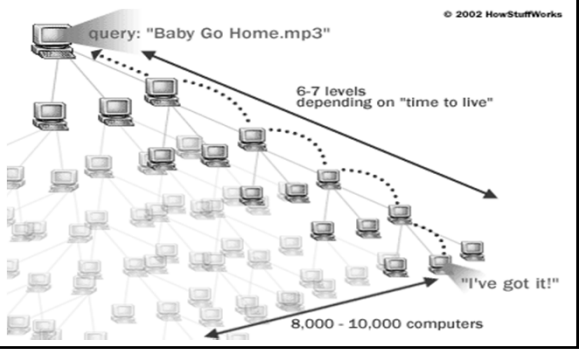
**Peer-to-Peer (P2P) Networks**

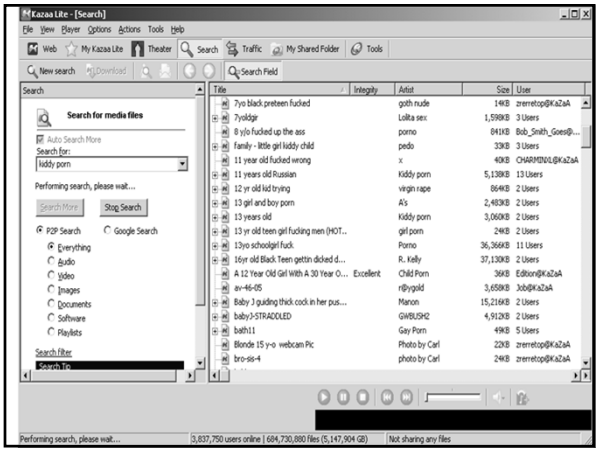
**file-sharing technology --- creates virtual networks**

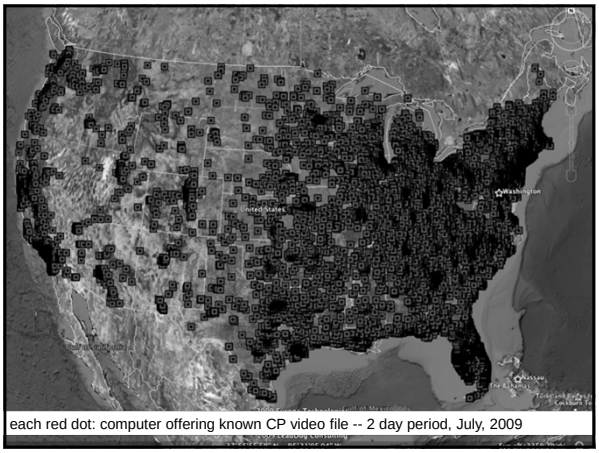

**criminal activity:**

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

**How Gnutella Works**




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

## 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)**

"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."**

## connecting computer to local network

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

- connected own laptop in dorm room to military base network
- investigator located 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"

## Extended discussions and citations on subject:

**Clancy,** The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer, 75 Miss. L.J. 193 (2005)

- Available at NCJRL.org

_____

more at:

**Clancy,** Fourth Amendment: Its History and Interpretation (2d Edition 2013)