Fourth Amendment
Applicability:
Expectations of Privacy

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

- Describe current test for determining whether Fourth Amendment applies to searches or seizures of digital devices or evidence

- Outline factors weighed in determining whether persons have reasonable expectations of privacy in digital devices

- Describe arguments regarding whether persons have reasonable expectations of privacy in deleted files
Overview

How and when does the FA *apply*, if at all, to computer technology?

“Inside the box” – standalones / data

“Outside the box” – networked devices / data & communications
Applicability & Satisfaction

**Does 4th Apply?**

1. Need gov't activity: "search" or "seizure"

2. Search must intrude upon person's reasonable expectation of privacy

If 1 and 2, then search must be justified as reasonable
selected issues:

A. Expectation of Privacy Analysis

B. Private Searches and Seizures
Expectation of Privacy Analysis

In General

Search: must have legitimate expectation of privacy invaded by gov't

two prongs

1. individual has subjective expectation of privacy

2. society recognizes that expectation as reasonable

If either prong missing, no protected interest
“Inside the Box”

- Repair shop searches
- Shared computers
- Personal computers connected to networks
- Workplace searches
- Consent searches
- Border searches
- Searches incident to arrest
- Inventory searches
- Probable cause-based vehicle searches
“Outside the Box”

- Detecting Internet “DRAS” information
- Obtaining “PCTDD”
- Getting subscriber account records
- Acquiring messages from service providers
- Examining contents of private web sites
- Obtaining cell phone site location data
- Tracking via GPS devices
- Searching on peer-to-peer (P2P) networks
Whether REP: **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
if no monitoring policy & no routine access by others to computer, may have REP in files

[ex] 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 Def’s computer 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/I* every time employee accessed computer  
   
   *Bailey*
“Operational realities” of the workplace

Another ex:

- Y pastor of small church
- Only other employees: custodian and secretary/administrator
- Church provided Y computer and private office
- No official policy regarding computer use or access
- Not networked to any other computer
- Kept in private office, with special lock
• Y kept two of three keys; administrator kept third locked in her credenza

• Admin only opened door for custodian and visiting pastors; but no one was permitted entry w/o Y’s permission

• Admin not permitted to log on to Y’s computer when he was not physically present

• Admin received call from church’s ISP; spam had been linked to church’s IP

• Admin ran “spybot” program on Y’s computer; found “some very questionable” web site addresses

• Contacted staff parish relations chair and IT person to have the computer examined
• Per district superintendent, chair of staff parish relations contacted police, unlocked Y’s office, and signed consent to search office and computer

• After searching the office and computer, an officer interviewed Y and essentially got Y to concede that he did not have a “right to privacy” on the computer and they could look at anything on it because it wasn’t Y’s computer

Did Y have a legitimate expectation of privacy in his office or computer?

State v. Young, 974 So. 2d 601 (Fla. 1st DCA 2008)
Joint Users

“no generic expectation of privacy for shared usage on computers”

[ex] student -- no standing to suppress session logs (indicating when he used computer), & hard drives of university-owned computer in computer lab.

Password-Protected Files

creator “affirmatively” intends to exclude joint user & others from files

--- does NOT assume risk joint user would permit S/
**Information Obtained from Third Parties**

**In general**

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
Repair shop case

- Took computer to Circuit City for installation of optical drive / DVD burner
- Videos were viewed; police informed; computer seized, then SW obtained for search

- Voluntary exposure; Assumption of risk
- Abandonment of privacy interest
- Plain view

**No F/A protection against**

1. **information from computer technicians**
   - have conveyed info to another person

2. **Email recovered from third party**
   - like letter, no REP once message received

3. **Internet chat rooms**
   - runs risk of speaking w/ undercover agent
How about your OWN computer used in your work?

- B, city treasurer -- shared work space with city clerk in open area of city hall
  
  * public could view but excluded; other workers routinely used space to access fax machine, use copier
  
  * only one Gov't 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
* clerk had problems with city computer, complained to cop (former computer sales)

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

* Guess what he found

Did B have a R.E.P. in his own computer?

*U.S. v. Barrows*, 481 F.3d 1246 (10th Cir. 2007)
Connecting your computer to a network

- University network admin found student-user who had hacked Qualcomm and also gained unauthorized access to university’s network

- Traced intrusion to university housing; remotely searched the computer to verify identification and continuing risk to university server

- Gov’t didn’t dispute student’s subjective expectation of privacy in his computer and dorm room

- Ct held student had a legitimate, objectively reasonable expectation of privacy in his personal computer

so, principal question:

Was defendant’s objectively reasonable expectation of privacy in his computer eliminated when he attached it to the university network?
Factors & Conclusion

- No announced monitoring policy on the network
- To contrary, policy stressed that, with few exceptions, files would be accessed only by authorized users
- No policy allowing university to actively monitor or audit computer usage
- Computer was in dorm room and protected by a screensaver password

“When examined in their entirety, university policies do not eliminate Heckenkamp’s expectation of privacy in his computer.”

_U.S. v. Heckenkamp_, 482 F.3d 1142 (9th Cir. 2007)
After reviewing federal cases on REP in workplace computers, Ct concluded “that defendant had no reasonable expectation of privacy in the personal information stored in his workplace computer.”

But then went on to say that “Even if defendant had a subjective expectation of privacy because he used a confidential password, that expectation was unreasonable under the facts of this case.”

“We conclude … that neither the law nor society recognize as legitimate defendant’s subjective expectation of privacy in a workplace computer he used to commit a crime.”

Deleted Files: What happens when user "deletes" a file?

* goes to **recycle bin**

* to attempt to permanently delete data, **empty recycle bin**

* data may remain on hard drive

  -- file marked as not needed, space available to store other files

  -- erasure when computer overwrites w/ another file

  -- fragments may be retrievable if entire file not overwritten

* word processing programs -- might have **saved portions** or versions

* may be on **hard drive until reformatted** -- even then, may still partially recover files, depending on how drive reformatted
Views on Admissibility of “Deleted” Data

A. Gov’t claim: files abandoned
   
   rejected as a false analogy: instead, like throwing in can inside house

B. Def Claim: Deleted Files Outside Scope of Warrant

   -- “deletion” creates legally different REP

   Rejected

   1. Same as “pasting together scraps of a torn-up ransom note.”
   2. Mere hope or attempt at secrecy not legally protected.
   3. No 2d warrant needed to scientifically test legally seized physical evidence.
Questions?

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