Surveillance in the Academic Community

Matthew Deffebach
College and University Professional Association for Human Resources
Paul Simon was wrong . . .

It’s not just you and Julio down
Today's Lesson:

• Privacy—the clash of issues
• Sources of Protection
• Public Sector
• Private Sector (and public)
• State Issues

Monitoring Considerations-Why?

Why monitor e-mail, internet, telephones, etc. and watch employees?
- Embezzlement/Misappropriation
- Harassment/Discrimination-Constructive Knowledge Problems
- Efficiency and Loss of Productivity
- Corruption of data/loss of resources

The General Rules of the Road

A. Statutory: ECPA and Omnibus Safe Streets Act…the Wiretap Statutes
B. Common Law.
Result: a Clash

SOURCES OF PRIVACY LAWS

Constitutional Law | Statutes | Regulations

Common Law | Company Policy/Contracts | Reasonable Expectation of Privacy
Public vs. Private

Public Sector Employees

• Generally afforded greater protection than private employees

• Constitution protects against “state action”

• Individual privacy protected under First, Fourth, Fifth, and Fourteenth Amendments
Fourth Amendment

- Protects against unconstitutional searches and seizures
- Employee must have “reasonable expectation of privacy”
- Expectation of privacy generally less in business than in home

Vega-Rodriguez v. Puerto Rico Telephone Co.
110 F.3d 174 (1st Cir. 1997)

- Employees of quasi-public phone company challenged video surveillance at work
- Court held employers have legitimate in efficiently run workplace
- No expectation of privacy in open areas so long as viewer’s presence is lawful
Vega-Rodriguez v. Puerto Rico Telephone Co.  
110 F.3d 174 (1st Cir. 1997)

- No general right to be free from video surveillance at work
- Surveillance was not too intrusive
  - recorded only “plainly visible” images
  - no sound recorded

Thompson v. Johnson County Community College  

- College placed video surveillance in locker area used by security officers to store personal items
  - Occasionally a changing area
  - Also contained equipment for heating/air conditioning
- Cameras resulted from reports of theft and weapons on campus
- Recorded only video – no sound
**Thompson v. Johnson County Community College**


- Cameras recorded only between 10:30 p.m. and 6:30 a.m.
- Court: silent video surveillance subject to 4th Amendment
- However, no reasonable expectation

---

**Thompson v. Johnson County Community College**


- Locker area was not enclosed
- Anyone could view locker room activities by walking through area
- Area not reserved for security officers’ exclusive use
- Search was reasonable investigation of alleged workplace misconduct
United States v. Simons, 206 F.3d 392 (4th Cir. 2/28/00).

- To establish a violation of Fourth Amendment rights, the employee “must first prove that he had a legitimate expectation of privacy in the place searched or the item seized.”

- “Government employees may have a legitimate expectation of privacy in their offices or in parts of their offices such as their desks or file cabinets. . . . However, office practices, procedures, or regulations may reduce legitimate privacy expectations.”

- The court found that, “[i]n light of the Internet policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet.”

How not to get burned:

1. What is the reason for the surveillance? (balance against privacy interest)

2. What notice was provided?

3. What is the expectation of privacy? How open is the area?
All employee wants: little honesty

Private (and public) Sector Employees

• No “state action” protection
• Typically, left with protection through the following:
  – Federal statutes and regulations
  – State statutes and regulations
  – Common law, including tort of invasion of privacy
  – Company policies
Federal Statutes Affecting E-mail Surveillance

Statutory:

The Electronic Communications Privacy Act ("ECPA") prohibits the unauthorized "interception" of communications in transfer and unauthorized access of stored communications.
The KEY exception…..Consent !!!!

2511 (2) (d):

It shall not be unlawful under this chapter for a person *not acting under color of law* to intercept a wire, oral, or electronic communication where such person is a party to the communication or where *one of the parties to the communication has given prior consent to such interception* unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

?? What type- implied v. expressed ?

?? One time ?
New Problems
A. New Technology
   1. Picture Phones
      * harassment and privacy issues
      * misappropriation/trade secrets
      * Consider policies or complete bans (Intel and General Motors ban from research facilities):
         a. Identify issues
         b. Need for policy changes
   2. Instant Messaging
      * 2004 Survey 31% of employees use IM (admitting even making disparaging remarks or discussing confidential information)
      * Not recorded on employer's server, but “float freely” and may be tracked by administrator and software exists to store and archive
      * Consider “intercept” problem if monitor without consent
      * 2004 Survey only 20% of companies with e-mail policy addressed IM
3. Cost of E-Production-Zubulake issues

(a) When does employer know/should know of potential litigation to prevent spoliation of evidence?

(i) At time of EEOC charge and even before when anticipate

Spoliation is the destruction of evidence or failure to preserve evidence in pending or foreseeable litigation. Employers face sanctions as well as dangerous spoliation instructions to the jury (inference that the evidence would have been favorable to plaintiff)

Good news dear, these same rules apply when monitoring phones, voice-mail, etc.

So, give notice, get consent, and monitor for business purposes only.
Security officers also sued under Title I, Electronic Communications Privacy Act.

Court held that Title I does not prohibit silent video surveillance – it is the interception of an oral communication that subjects the interceptor to liability.
Lessons Learned:

1. For phone systems, same rules for e-mail compliance apply

2. For video, same notice/expectation of privacy rules apply as discussed with public sector

3. For most forms of privacy challenges, the recipe for success:
   
   notice+consent+no reasonable expectation of privacy.

Too Much? Remember, your job could be worse.
THANK YOU!

Matt Deffebach
(713) 547-2064
deffebam@haynesboone.com