IMLA Annual ConferenceOctober 31, 2007



Sherlock Holmes in the 21st Century Municipal Workplace

Monitoring & Surveillance of Public Employees in an Electronic Age

Attorney Daniel D. Crean

Public Workplace Surveillance Issues

- Workplace Privacy
- Public Employee Constitutional Protections
  - First and Fourth Amendment
  - "Due Process"
- Statutes/Ordinances/Charters
  - ECPA, Fair Credit Reporting Acts, Wiretapping, Eavesdropping, Computer Privacy, General Privacy, Motor Vehicle Record Laws, Whistleblower Protection
- Open Records Laws

Workplace Surveillance: Why Do It?

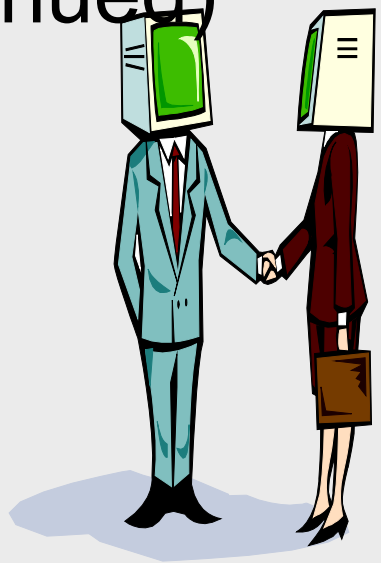
- In 2001, employees stole $15.243 billion in inventory
- In 2002 report:
  - 9 of 10 respondents were victims of computer security breaches (with 8 of 10 suffering $ losses)
  - 2 most expensive categories of theft were intellectual property ($170,827,000) and financial fraud ($115,753,000)
- Estimated 70 to 80% of all computer
- crime is committed by employees
- against their employers

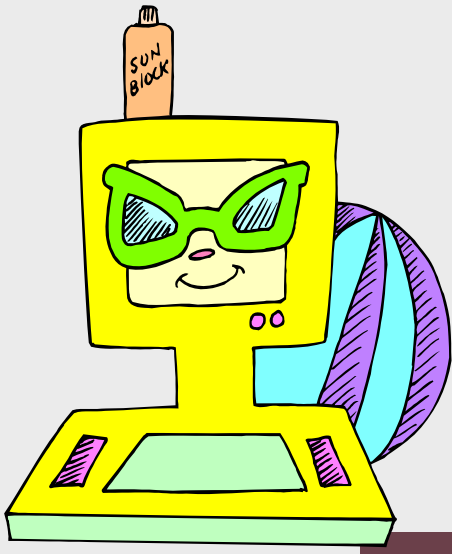


  - Source: Lane, *The Naked Employee*

The Need for Surveillance (continued)

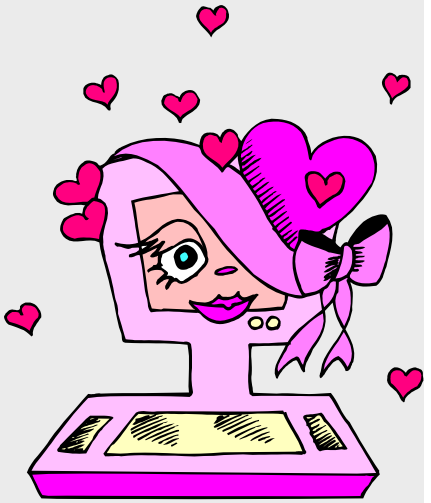
- Telephone chitchat
  - By late 1950s >75% of homes had phones but “domestic” calls to work were not commonplace
  - Now computer communication between office & home [& elsewhere!] is commonplace
- Computers & software make game playing easier to do [and easier to do unobserved]
  - Apreo (producer of *AntiGame) claims that workplace games cost employers >$50 billion per year*





Yet more interesting numbers . . .

- Currently approximately 15,000 sexual harassment complaints are filed annually with EEOC, with awards to successful claimants averaging > $500,000
- Computers (internet and intranet) are major elements in harassment complaints, particularly those involving hostile environment
- Revenge, Terrorism: Disaffected employees, customers, random acts
  - Can be physical or electronic





Email - some statistics

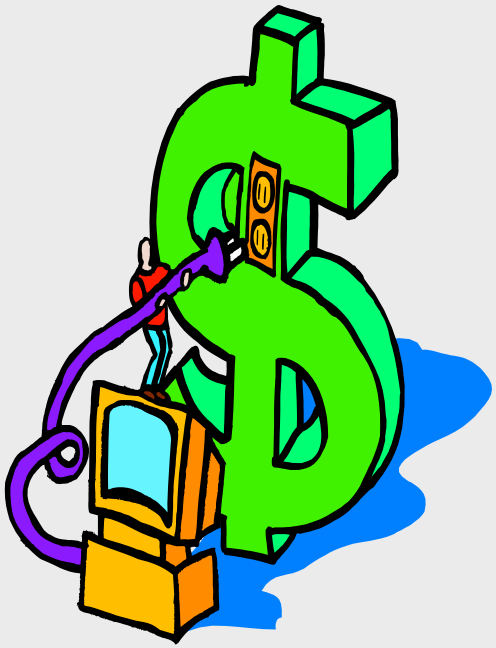
- Average corporate worker in May 2007
  - Handles 142 emails/day (700/week, 35,000/year)
- By 2010, expected to grow to 57,000 annually

What percentage of these are work-related?

What percentage of these contain:

- Harassment?
- Smoking Gun?
  - Inadvertent or intentional disclosure of confidential info?
- Embarrassment?

For what percentage of these should brain have been engaged before hitting send?



Why monitor & record electronic information?

- Federal Discovery Rules (and some state rules) require production of email, electronic documents, etc.
- How to produce? But even more, how do you know what you've got without reading it all?
- Need to retain in anticipation of litigation.
- Non-spoliation policies and actions



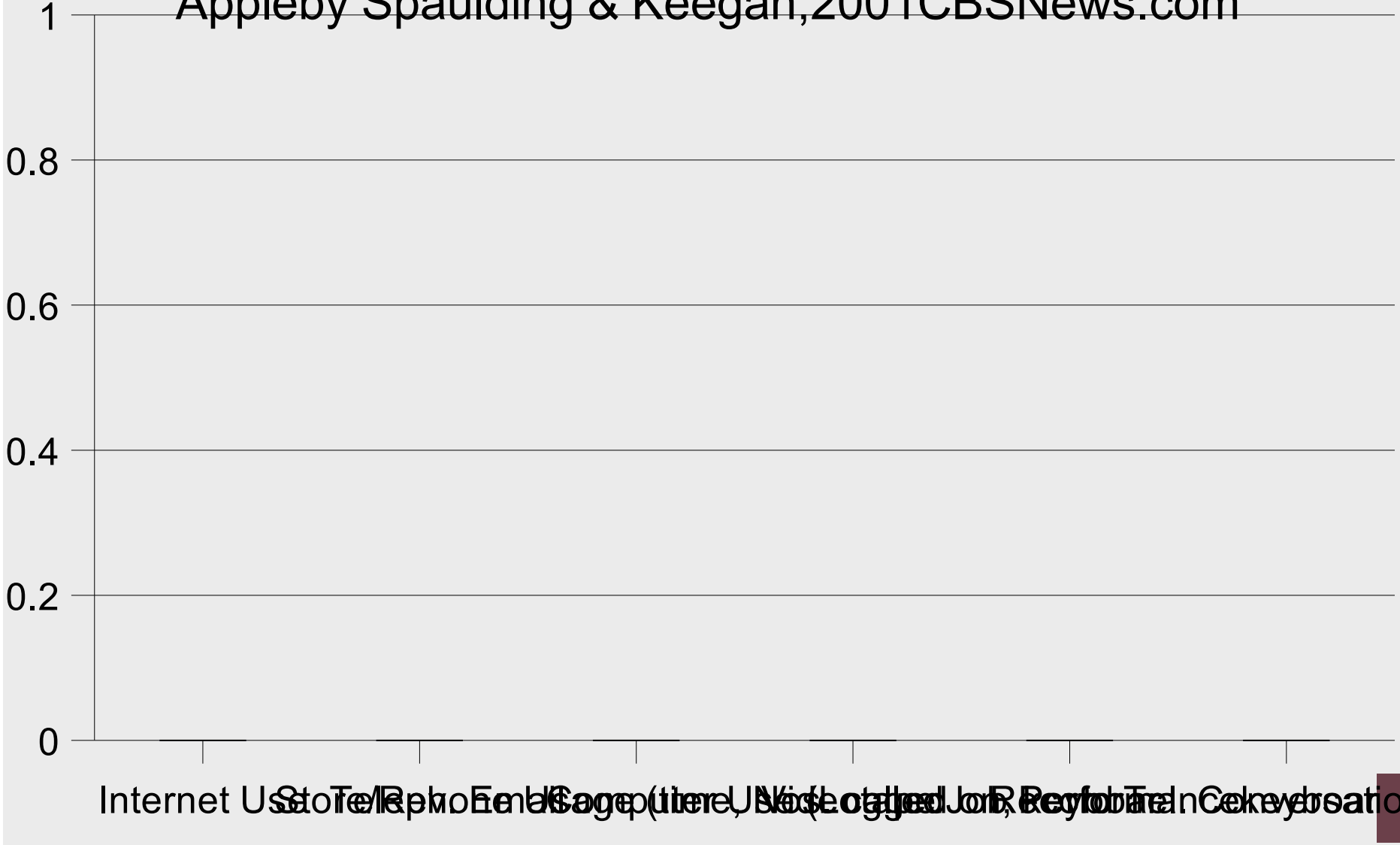
So, what are employers doing in response?



- According to some, taking reasonable action to retake control of the workplace
- According to others, technology makes it possible to gather enormous amounts of data on employees, far beyond what is needed
- So, how much surveillance/monitoring is too much?
- Enhanced and increased scrutiny may →
  - Conflict with Privacy & Constitutional Protections

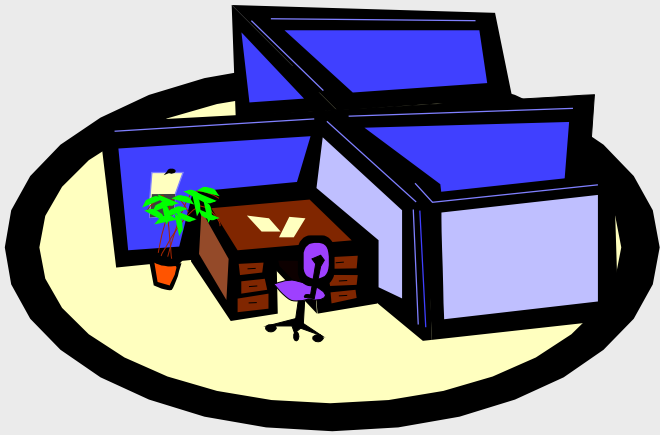
Private Sector Employee Monitoring

Source: Appleby Spaulding & Keegan,2001CBSNews.com



Workplace Privacy

- Sources
- Nature, Scope and Extent
- Practice and Practical Concerns





Workplace Privacy

- Workplace privacy exists in both public & private sectors by virtue of court decision, state constitution, state statutes

- Privacy also protected by other statutes not expressly protecting workplace privacy
  - Discrimination
  - Medical Information
  - Wiretapping and similar laws

- Public sector employees also receive protections under US and State Constitutions

Common Law Privacy

- The right to privacy (including workplace privacy in some states) includes protection from:
  - ➢ Intrusion on physical/mental solitude
  - ➢ Public disclosure of private facts
  - ➢ Publicity depicting person falsely
  - ➢ Appropriation of person's name/image

  - ➢ Traditional formulation based on Restatement of Torts

Public Employers & Privacy: Limits Imposed on Search/Seizure



Searches and seizures by government employers or supervisors of the private property of their employees are subject to Fourth Amendment restraints.

An expectation of privacy in one's workplace is based upon societal expectations that have deep roots in the history of the Amendment. However, operational realities of the workplace may make some public employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official.

O'Connor et al. v. Ortega, **480 U.S. 709 (1987)**

Factors in Validity of Searches

- Employee Abandonment of Privacy
- Property or Possessory Interest in Area Searched
- Existence & Clarity of Search Authorizing Policies
- Purpose of the Search: Criminal - Civil
- Special Factors
  - Nature of the Workplace
  - Need for Discipline/Security

And, not specifically a topic for today, but . . .Don’t Forget Employee Free Speech!



Justifications for reducing expectations of privacy in an electronic workplace

Computer/system integrity
- Viruses, unauthorized use of software, piracy, licensing

System capacity
- E-mail and junk mail storage, employee time in storing/retrieving documents

- Inappropriate e-mail and web site access
  - Pornography, harassment, offensive content
- Intellectual property protection
  - Copyright
- Governmental integrity
  - Confidentiality
  - Investigations

Electronic Privacy:Monitoring/Surveillance



State and Federal Laws governing electronic surveillance may limit free hand of employers to monitor employee use of computers and telephones and visual monitoring of the workplace.

- FEDERAL ECPA does not apply to local government
- State Wiretapping and Eavesdropping laws may apply
- State Violation of Privacy laws may also apply

Generally, laws are based on expectations of privacy.

That expectation is controlled by policy & practice.

Monitoring v. Intercepting



- Monitoring (or Auditing) -
  - Checking e-mail after it has been sent/received
  - May be less susceptible to challenge
    - It is not “active”
    - It is like looking at an employee’s work product in a file cabinet
- Intercepting (or Filtering)
  - E-mail checked during transmission
  - May be subject to greater restriction
    - Results from active “listening” to actual communication - more akin to wiretapping
    - May still be defensible if done reasonably and pursuant to policy that has reasonable purpose

One Sample of Computer Surveillance

- **WinWhatWhere Investigator: Computer** activity monitor
- . . . “the most advanced and detailed computer activity monitor available. Since inventing the genre in 1993, WinWhatWhere has been the innovative leader in computer monitoring **software**.”

- Investigator raises the bar again with **Web Cam** Capture, Hide & Seek, Key Phrase Alerts, and Timed Events. These new features make Investigator the most comprehensive monitoring program available today.
- F**eatures** :- Keystroke logging - Screen capture - Internet Activity- Window Content -Chat Room - Hide & Seek (Moves/renames itself) - Remote installation - Key Phrase Alerts - Web Cam Capture - Timed Events - Send data to remote location - File Activity Monitor
- - Built-in Network support- And more...

Another Sample

Scalable Software markets “Survey” and says:

Despite marketing claims, Software Asset Management products are . . . not designed . . . to optimize the use of your software investments. They fail to capture comprehensive and detailed . . . usage intelligence and communicate this to the business in a commercially meaningful way. . . many companies are overpaying simply because they have little or no idea how their software is being used, let alone if it is being used at all and usually agree to costs based simply on what is installed.

The product “details the time the employee spends using Windows applications, e-mail and the Internet, and provides the employee with easy-to-understand reports so the he/she can better manage their time.”

Thus, instead of monitoring keystrokes it monitors time spent interacting with installed programs. There are no legal barriers, as the information gathered is not “in transit” within meaning ECPA.

(The Naked Employee)

To lessen issues with employee privacy & monitoring laws

- Policy adoption has the purpose of
  - Furthering effective and productive use
  - Educating employees
  - Protecting against misuse
  - Protecting against liability
    - For improper use (e.g., harassment)
    - For improper regulation of employee use
- A key element in policy adoption is elimination of, or at least minimizing, employee expectation of privacy

Policies & Practices

- Policies and Practices Can
  - Guide employees away from improper conduct
  - Even prevent some problems
  - Create basis for communicating with & explaining restrictions to employees
  - Provide a basis for discipline
  - Provide a defense

Questions?Contact information:dcrean@nhprimex.org

THANK YOU