

Employment Law for BUSINESS *sixth edition*

Dawn D. BENNETT-ALEXANDER and Laura P. HARTMAN

McGraw-Hill Irwin

Copyright © 2009 by The McGraw-Hill Companies, Inc. All rights reserved.

Are There Guarantees in Life?

- The right “to be let alone”
- Privacy as a fundamental right
- Employer need for private information
- Global marketplace
- Protecting employees’ personal information

LO1

13 - 2

Myths about Employee Privacy Rights

- Employees have an absolute right to privacy in their workplace
- It is a breach of an employee’s right to privacy for an employer to ask with whom the employee lives
- In the private sector, the Constitution protects employees’ right to be free from unreasonable searches and seizures
- Without constitutional protection, employees in the private sector are left with no protection against invasions of privacy
- Once an employee gives information to an employer, the employer may use it for whatever purpose it desires

13 - 3

Background

L02

- Privacy may be protected by: Constitution (federal or state), federal and/or state statutes, common law
- Fundamental rights guaranteed by the Constitution
 - The right to be free from unreasonable searches and seizures
- Argument: The employee is trying to hide something
- Access to employee information

13-4

Public Sector Employee Privacy

L03

- The Fourth Amendment
 - Protection against unreasonable search and seizure
 - Violation if the search is:
 - Unreasonable
 - Unjustified at its inception
 - Impermissible in scope
 - Search warrant
 - Drug testing
 - Search of employer-owned property
 - False imprisonment

13-5

Public Sector Employee Privacy (continued)

- The 5th and 14th amendments
 - Strict scrutiny
 - Compelling state interest
 - Rationally related to a valid state interest
 - Is the right fundamental?
 - Implicit in the concept of ordered liberty
 - Deeply rooted in this Nation's history and tradition
 - No general right of the individual to be left alone

13-6

The Privacy Act

- Regulates the release of personal information about federal employees by federal agencies
- Basic principles:
 - Employee access to their files
 - Mechanism to correct or amend information
 - Employer protection of information
 - Maintenance of information
- The right to privacy is not absolute
- Guiding factors
- Employee relief

13-7

Privacy Protection Study Commission

- Privacy Act not extended to private sector
- Commission recommendations
- Commission policy goals
- Five basic employee procedural rights:
 - Notice
 - Authorization
 - Access
 - Correction
 - Confidentiality

13-8

Federal Wiretapping—Title III

- Federal Wiretapping – Title III
 - Governs the interception of oral, wire, and electronic communications
 - Interception by state and local law enforcement
- ECPA
 - Covers all forms of digital communication
 - Prohibits unauthorized eavesdropping
 - Prohibits unauthorized access to messages

13-9

Private Sector Employee Privacy

LO4

- Bases for right to privacy in the private sector
 - Common law tort claims
- Statutory claims
- Tort law protections/common law
- Intrusion into seclusion

LO5

Tort

A legal wrong, for which the law offers a remedy.

13 - 10

Private Sector Employee Privacy (continued)

- Public disclosure of private facts
 - Intentional or negligent public disclosure of private matters
 - Such disclosure would be objectionable to a reasonable person of ordinary sensitivities
- Publication in a false light
 - Public disclosure of facts that place the employee in a false light
- Breach of contract
- Defamation
 - Libel vs. slander
 - Compelled self-disclosure

13 - 11

Regulation of Employee's Off-Work Activities

LO6

- Employers may regulate off-work or otherwise private activities of their employees where they believe that the off-work conduct affects the employee's performance at the workplace
- Smoking
- Weight
- Marital status
- Romantic involvement
- Political status
- Lifestyle discrimination
- Enforcement

13 - 12

Employer's Information-Gathering Process/Justified Use/Disclosure of Information

- **Process** of information gathering
 - Harassment
 - Improper filing
 - Dissemination of the information
- Function creep
- Collection and retrieval of information
- Limitation of questions to potential employee
- Proper storage of information
- References

13 - 13

Electronic Monitoring or Surveillance of Employee Activities

- Written policies concerning e-mail and Internet use
- Bloggers beware
- New technologies
 - Issues that intersect law and ethics
 - The nature/capabilities
 - Information gathering
 - Technology and traditional workplace challenges
 - Informal intrusions

L07

13 - 14

Forms of Monitoring

- Surveillance by glitch
 - Information uncovered by mistake
- Surveillance by default
 - All information sent through a system is caught and cataloged
- Surveillance by design
 - Entire purpose is to collect information and the user is aware of this purpose
- Surveillance by possession
 - Employee information contained in a database or some other list

13 - 15

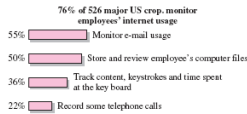
How Does Monitoring Work?

- Silentranner
- Global positioning
- Websense/Websense reporter
- MIMESweeper
- Reasons to monitor:
 - Avoid legal liability
 - Prevent employee theft
- Protection from overt intrusions
 - Prior consent
 - Business extension

13 – 16

Percentage of Large U.S. Companies That Monitor Employee E-mail

Exhibit 13.7 Percentage of Large U.S. Companies That Monitor Employee E-mail



76% of 526 major US corporations monitor employees' Internet usage.
 55% monitor e-mail usage
 50% store and review employees' computer files.
 36% track content, keystrokes and time spent at the keyboard
 22% record some telephone calls

Source: Adapted by authors from data from the American Management Association, "2005 Electronic Monitoring & Surveillance Survey," May 18, 2005, http://www.amanet.org/research/pdfs/EM1_summary05.pdf.

13 – 17

Business Justifications for Monitoring Employees' Technology Use

LOB

- Reasons to limit workplace Internet use:
 - Wasted time
 - Overlogged networks
 - Inappropriate material seepage into the workplace
- Areas of employer potential liability:
 - Defamation
 - Copyright infringement
 - Sexual harassment
 - Discrimination
 - Obscenity
- Impression when an employee visits various sites
- Formal policies or programs regulating employee Internet use

13 – 18

The Case of Employee E-mail

- Employers' needs vs. employees' right to privacy
- The employer's interception must not exceed the scope of the employee's consent
- Employers must specifically inform employees of the extent and circumstances under which e-mail communications are monitored
- State imposed notice requirements

13 - 19

Developing Computer Usage Policies

LO9

- Policies should be both written and communicated to the employee, and then adhered to
- Suggested guidelines
 - Appropriate areas
 - Employee access to information gathered
 - Ban on continuous monitoring and secret monitoring
 - Only job relevant information collected
 - Only for business interest

13 - 20

Waivers of Privacy Rights

- An employer may request that an employee waive her or his privacy rights as a condition of employment
 - **Requiring** a waiver is a questionable approach
- Requirements:
 - The waiver should be accompanied by an offer of employment
 - The waiver must be knowingly and intelligently given
 - The waiver must be clear and unmistakable
 - The waiver must be in writing
 - The waiver must be voluntary

13 - 21

Privacy Rights Since September 11, 2001

- USA PATRIOT Act
- The government is now allowed to monitor anyone on the Internet simply by contending that the information is “relevant” to an ongoing criminal investigation
- By September 2002, 58 new regulations responding to terrorism
- Employer response to governmental request for information

13 - 22

Summary

1. Conduct an information audit for the purpose of determining those areas of the company’s practices and procedures that have the **potential for invasion**.
2. In connection with sensitive areas where the company maintains no formal policy, **develop a policy** to ensure appropriate treatment of data.
3. The information collected should be kept in one of several files maintained on each employee: personnel file, medical file, evaluation file, confidential file.
4. Information should be gathered from **reliable sources**, rather than sources of questionable repute, such as hearsay, lie detector tests, and subjective indicators.
5. **Publicize privacy policies and procedures**, and **educate employees** regarding their rights as well as their responsibilities.

13 - 23
