LIEBERT CASSIDY WHITMORE

EMPLOYMENT LAW | LABOR RELATIONS | EDUCATION LAW | MANAGEMENT TRAINING

# Privacy Issues in Our Technological World

www.LCWlegal.com

*Presented by:*

*Pilar Morin*

# Agenda

- Defining Tools/Technology
- Legal Framework
- Case Studies

# Technologies That Give Rise to Privacy Concerns In the Workplace

- Email
- Blogging
- Instant Messaging
- Video Sharing
- Social Networking
- Twitter
- GPS
- Biometrics
- Telematics
- Video Surveillance

# “Getting Dooced”

- Being terminated for blogging about the employer
- In a survey of 294 large United States companies, 7.1 percent reported terminating an employee for blogging-related conduct.

# Background Checks Online

- Prospective employer may legally use Internet tools because most of the time:
  - Information obtained online is publicly available
  - It is posted by the job applicant (ex. MySpace or Facebook)

# Legal Framework: Sources of the Right to Privacy

# Categories of Privacy Interests

- Informational Privacy:
  Confidentiality of personal matters

- Autonomy Privacy:
  Freedom over personal conduct

# Sources of the Right to Privacy

- U.S. & California Constitutions
- U.S. & California Statutes
- Common Law

# Sources of the Right to Privacy

- United States Constitution
  - No express right to privacy in text of United States Constitution
  - First, Fourth, and Fourteenth Amendments imply a right to privacy

# Sources of the Right to Privacy

- United States Constitution
  - *Katz v. United States*, 389 U.S. 347 (1967)
    - Fourth Amendment protects “reasonable expectation” of privacy
  - *O’Connor v. Ortega*, 480 U.S. 709 (1987)
    - Public sector employees may have reasonable expectation of privacy in the workplace unless expectation reduced by putting employee on notice of reduced expectation of privacy

# Sources of the Right to Privacy

"All people are by nature free and independent and have inalienable rights. Among these are …*privacy."* (emphasis added)

Article I, Section 1, of the California Constitution

# Standard of Review

## Balancing Test:

Employee's Reasonable Expectation of Privacy

vs.

Employer's Legitimate Business Needs

# When Does an Employee Have a Reasonable Expectation of Privacy

- Objective standard
- Recognized by social norms as private
- Realities of the workplace

# Legitimate Business Needs

- Productivity
- Efficiency
- Supervision
- Control
- Prevent improper or illegal use
- Prevent liability

# Federal Statutes Protecting Electronic Communication

- Electronic Communications Privacy Act, 18 U.S.C. § § 2510-20, 2701-11
  - Amended the Wiretap Act (protects electronic communications during transmission, and before the electronic communication is opened and stored)
  - Prohibits:
    - Intentional interception of electronic communications
    - Disclosure or use of intercepted electronic communication

# Federal Statutes Protecting Electronic Communication

- Electronic Communications Privacy Act, 18 U.S.C. § § 2510-20, 2701-11
  - Exceptions under the Act:
    - Consent [18 U.S.C. § 2511(2)(c)]
    - Provider exception [18 U.S.C. § 2511(2)(a)(i)]
    - Publicly accessible [18 U.S.C. § 2511(2)(g)(i)]

# Stored Communications Act ("SCA") 18 U.S.C. § 2701

- Prohibits intentional and unauthorized access of wire or electronic communications while in electronic storage
- Does not apply to:
  - Provider of wire or electronic communications service
  - User of that service

# California Statutes Protecting Computer Resources

- Penal Code Section 502 protects computer systems, data, the privacy of individuals and “the well-being of financial institutions, business concerns, governmental agencies, and others."
- It prohibits unauthorized use, copying, damage, interference, and access to lawfully created computer data and computer systems
- Provides both criminal and civil remedies
- Excludes conduct taken during scope of employment

# California Privacy Act ("CPA") Penal Code § 631

- Prohibits willful attempt to learn the contents or meaning of communications in transit over a wire (wiretapping or eavesdropping)
  - Consent exception goes beyond Federal Wiretap Act; requires the consent of "all parties to the communication"
  - Consent can be implied by notice, i.e. customer lines

# Evidence Code § 917(b)

"A communication between [lawyer and client; physician and patient; psychotherapist and patient; clergy and penitent; husband and wife; sexual assault counselor and victim] does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access…"

# Gov't Code § 6250 et. seq.
# The Public Records Act

- "Any writing containing information relating to the conduct of the public's business" (GC §252(e))
- Excludes: "personnel, medical or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy." (GC §6254(c))

# Rules of Civil Procedure

- Require disclosure of Electronically Stored Information (ESI)
- Federal: Without awaiting a discovery request party must disclose category and location of potential ESI re: claims and defenses
- Disclosure includes back-up tapes, employee PCs, and Blackberry devices as well as electronic records of conversations through voice mail or instant messaging

# Case Studies

# Case Study

John is a janitor at Western Unified School District. He is assigned to clean and maintain several high schools in the District. The District has learned that John is boasting in a public chat room that he has had sexual relations, during work hours, with various women at the different sites he has worked. None of the women are students.

John’s chat room confessions take place after work on his private computer. The HR Director investigates by going onto the public chat room to monitor the live chat, where John identifies himself as a District employee and provides details about “the jobs.” The HR Director confirms John’s confessions are true.

John claims the District has violated the Electronic Communications Privacy Act and the Stored Communications Act. Does he have a case?

**NO**

# Case Study

What if John created a web page for classified employees in the District who are employed as janitors to organize. He uses the website to provide the janitors with union information. But, the web site also allows the janitors to “talk shop” and socialize.

**May the District view and monitor it?**

Would it make a difference if John posted the information on a blog, located in a private web and the HR Director falsely used the identity of another District janitor to get access?

**YES**

# Case Study

A female member of the high school drill team claims that a male coach sent inappropriate text messages to a former member of the drill team. That student has moved out of state and cannot be located by the school to confirm the allegation. The District issued the coach a cellular telephone.

May the District contact its cellular telephone provider to get copies of the coach's text message transcripts since the District owns the cellular telephone and pays for the service?

**MAYBE**

# Case Study

The District is hiring new janitors. John recommends his cousin Cameron. The HR Director decides to use Google, MySpace, and Facebook to check out Cameron and other applicants.

The HR Director gathers the following facts from her Internet search:

- Cameron is female and Latina
- Cameron is single but has posted an add looking for a sperm donor as she wants to start a family right away
- Cameron is also President of an animal rights group

# Case Study

What if the HR Director conducts her internet search and instead finds:

- Cameron's MySpace page identifies herself as a member of a local gang known for car jacking and robberies
- Cameron is a convicted felon
- Cameron has a blog with her photograph which consists of racist hateful comments

# Case Study

The District wants to use GPS technology to track District janitors due to complaints that they are leaving job sites early after completing their regularly assigned work. The District hopes to increase efficiency by installing this technology in all District vehicles provided to janitors.

**Can the District do this?**

# Penal Code section 637.7

Prohibits the use of an electronic tracking device to determine the location or movement of a person

Exception: vehicle's owner, renter, or lessor may place the device on its own vehicle

# Business Justifications for Monitoring Employee Movements

- Employee Monitoring Through Global Positioning Systems (GPS)
  - Promotes safety and efficiency
  - Locate lost or injured personnel
  - Allows agency to track operations
  - Can establish/disprove agency liability
  - Locate stolen vehicles

# Video Surveillance in Facilities

- Potential Expectation of Privacy in Video Surveillance in the Workplace

  In *Hernandez v. Hillsides*, the California Supreme Court upheld video surveillance of a private office:

  •Employer: nonprofit residential facility for abused children

  •surveillance was narrowly tailored in place, time, and scope

  •Surveillance was prompted by legitimate business concerns of finding who was viewing pornography after hours in violation of  policies