Labor & Employment
Inner Workings

09.5698

Labor & Employment **Inner Workings**

Privacy Issues in the Employment Environment

FOLEY

FOLEY & LARDNER LLP

Background and General Privacy Issues

Sources of Privacy Protection

- U.S. Constitution
  - First Amendment;
  - Fourth Amendment; and
  - Fourteenth Amendment.
- State Constitutions
  - Some have broader privacy protections.
- Federal and State laws
- Regulations and Rules

Sources of Privacy Protection

- Self-Regulation
- Contracts
- Industry regulation
- Common law

Federal Privacy Statutes

- Children's Online Privacy Protection Act (COPPA)
- Gramm-Leach-Bliley
- FCRA/FACTA
- Right to Financial Privacy Act
- Electronic Communications Privacy Act
- Health Insurance Portability and Accountability Act
- CAN-SPAM and telephone marketing restrictions

Common Areas of State Regulation

- Identity Theft Laws
- Restrictions on use of Social Security numbers
- Spam
- Internet Privacy
- Telephone/Fax Marketing Laws
- State Wiretapping Laws
- Computer Crime Laws
- Notice of Security Breach Laws
- Medical Privacy
- Financial Privacy

Electronic Communications

A History of Wiretapping

- *Katz* was one of the first cases to recognize a privacy right in wire communications
- Title III of the Omnibus Crime Control and Safe Streets Act resulted
- This ultimately became the ECPA

Electronic Communications Privacy Act (18 U.S.C. § 2510 *et seq.)*

- There are two portions of the ECPA
  - The Wiretap Act (Title I-interception);
  - The Stored Communications Act (Title II-dissemination or review).
- This is a temporal distinction
- There are also certain additional restrictions on public providers

Electronic Communications Privacy Act (18 U.S.C. § 2510 *et seq.)*

- Wiretap Act and Councilman.
  - Prohibits “interception” of “electronic communications”.
    - "electronic communication" "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photooptical system that affects interstate or foreign commerce,"
  - Does not include electronic storage as does the definition of “wire communications” or the storage definition of the Stored Communications Act

Electronic Communications Privacy Act

18 U.S.C. § 2510 *et seq.*

- What is Storage?
- There is a split in how courts address whether a communication is in storage
  - Is it in an in-box?
  - Is it in memory—RAM?
  - Is it in memory on the wire?

Electronic Communications Privacy Act (18 U.S.C. § 2510 *et seq.)*

- Applies mostly for businesses in the employee context
- Two potential exceptions:
  - protect the provider, another provider, or a user, from fraudulent, unlawful or abusive use of such service; or
  - a person employed or authorized, or whose facilities are used, to forward such communication to its destination

Other Employee Concerns

- Other issues to consider when you are drafting your policy
  - Does the absence of a policy create a reasonable expectation of privacy?
  - What role does password protection play?
  - What role do physical characteristics of an office play?
  - Is ownership of equipment determinative?

Quon v. Arch Wireless

- The case involves 4 plaintiffs—two members of a SWAT team, a dispatcher and Jeff Quon's wife
- The role of the policy in the case is important to note

Quon v. Arch Wireless

- Technology at issue was a text message capable pager that was supported by a third-party
- Both Quon and Trujillo had the same pager

Quon v. Arch Wireless

- What issues were presented in the case:
  - Was Arch (provider) an ECS (electronic communication service) v. a RCS (remote computer service)? Both an RCS and an release private information with consent of addressee, but only an RCS can release information with consent of subscriber. Since Arch was ECS, could not disclose contents to subscriber (police department) without consent of recipient.
  - What protections do employees have in text messaging?
  - What role does an employee monitoring policy play in setting the employee's expectation of privacy?
  - What role does "operational reality" play?
  - What impact do public records laws have?

Quon v. Arch Wireless

- ECS v. RCS
  - This issue was relevant because under 2702 a "subscriber" cannot get content without consent of a recipient.
- Employee policies
  - A general employee policy was in place, but was not consistently applied in the case.
- Operational reality
  - Here the Department had varied its announced policy by conduct.
- The role of personal use
- Public records laws

Quon v. Arch Wireless

9th Circuit Held:

- Arch Wireless was an ECS and violated the Stored Communications Act by releasing the text messages
- Plaintiffs had a reasonable expectation of privacy under the 4th Amendment with respect to the content of the messages
- The search was not reasonable
- City and Department are not protected by immunity

Quon v. Arch Wireless

- What are the takeaways:
  - Review your policy, particularly if it is "general"; ensure that it covers new technology;
  - Apply the policy consistently without exceptions;
  - Courts will look behind your policy;
  - Ownership is not determinative; and
  - Public records laws may not be determinative

Technology Issues and Implied Consent

- There are other cases that discuss how specific your policy must be

Other Employee Concerns

- Communications with individuals within some privilege or duty of confidentiality
- Videotaping.
- Is there a right of privacy in a company cell phone?
- Off-Duty Conduct (e.g., California Labor Code 96(k))

What About State Law?

- *Quon* did not address California law as the issue was waived on appeal
- In other cases, California's wiretap law has been applied to certain forms of communications

State Wiretap Laws

- Most states have a wiretap law that covers electronic communications as well

- E.g., California Penal Code 632, California Invasion of Privacy Act – may not eavesdrop or record confidential communication, confidential if objectively reasonable expectation that the conversation is not being recorded (and *Flanagan* case states applied to a case involving employees and supervisors in anticipation of litigation)

A Few Words About Videotaping

- Generally – difficult to predict what is acceptable, no "bright line" and can vary by state. General principles of privacy apply and are illustrative.
- Hernandez v. Hillsides (California Supreme Court, August 2009), state constitutional and common law claims, with limited off-hour hidden surveillance cameras in office: Key concepts included:
  - 1) nature of any intrusion based on reasonable expectation of privacy;
  - 2) offensiveness or seriousness of intrusion, including any justification and other relevant interests.
  - Comes down essentially to balancing test, weighing intrusion against defendant's justifications and countervailing interests, based on specific facts.

- Court held that although some expectation of privacy in shared or solo office (including expecting secret video equipment would not record activity) so that first element satisfied, but here intrusion was not highly offensive or sufficiently serious (narrowly tailored, and plaintiffs not at risk of being monitored or recorded during regular work hours) so second element not satisfied
- Privacy in workplace is diminished, but not lacking altogether (e.g., Sanders case, surreptitious recording by reporter among cubicles violated privacy)
- Factors include identity of person (stranger versus colleague), location (enclosed versus public and open), degree of intrusion (minor versus significant), reason for intrusion. Examples cited on both ends of spectrum (e.g., dressing rooms and locker rooms protected, versus lunch meeting in crowded outdoor patio and common exposed area—although, again, very fact dependent)
- Court mentioned no policy or warning of this

State Electronic Monitoring Laws

- Two party consent states present unique issues
- These states include:
  - California
  - Connecticut
  - Florida
  - Illinois
  - Maryland
  - Massachusetts
  - Michigan
  - Montana
  - Nevada
  - New Hampshire
  - Pennsylvania
  - Washington

Identity Theft

State Computer Crime Laws

- Alabama
- Arizona
- Arkansas
- California
- Colorado
- Connecticut
- Delaware
- Florida
- Georgia
- Hawaii
- Idaho
- Illinois
- Iowa
- Kansas
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- Texas
- Vermont
- Virginia
- Washington
- West Virginia
- Wisconsin
- Wyoming

Most States Have Identity Theft Laws

- Alabama
- Alaska
- Arizona
- Arkansas
- California
- Colorado
- Connecticut
- Delaware
- Florida
- Georgia
- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Texas
- Utah
- Vermont
- Virginia
- Washington
- Washington D.C.
- West Virginia
- Wisconsin
- Wyoming

Importance of State Identity Theft Laws

- Many regulate the improper collection of personally identifiable information
- Some require financial gain, while others do not
- Some provide civil remedies

- E.g., California Civil Code §1798.82 requires that an employer whose computer data contains employees' "personal information" (names, coupled with Social security numbers, driver's license or state identification card number, or financial account numbers) must promptly notify any employee whose "personal information" is acquired by an unauthorized person, unless notification would impede a criminal investigation.

The Law of Pretexting—State Laws

- California
- Florida
- Georgia
- Illinois
- Maryland
- Michigan
- Montana
- New York
- North Carolina

GINA

The Genetic Information Nondiscrimination Act of 2008 (GINA)

- GINA Provisions:
  - Generally: Prohibits employers and group health plans from discriminating based upon "genetic information" and strictly limits the collection of such information.
  - Acts As a Floor of Protection But Does Not Preempt Higher Regulation Under State Law
    - 34 States Have Their Own Genetic Information Laws
  - GINA's Effective Dates
    - Employers – 18 months after signing (November 21, 2009)
    - Group Health Plans/Insurers – one year after signing (May 21, 2009)

The Genetic Information Nondiscrimination Act of 2008 (GINA)

- Important Definitions In GINA
  - "Genetic Information": information about
    - An individual's "genetic tests" (*i.e.*, analysis of DNA, RNA, chromosomes, proteins or metabolites that detects genotypes or chromosomal changes)
    - Genetic tests of the individual's family members
    - The "manifestation of a disease or disorder" in the individual's family members (not limited to hereditary conditions or to biological relatives)
  - "Family Members" include
    - Dependents
    - "Any other individual who is a [first-fourth degree] relative of the individual or such individuals dependent"
    - Applies to spouses, adopted children

The Genetic Information Nondiscrimination Act of 2008 (GINA)

- Effect on Employers
  - Restrictions
    - Prohibits discrimination on basis of genetic information
    - Restricts employer's Acquisition of Genetic Information
    - Requires Employers To Expressly Maintain Confidentiality of Genetic Information
    - Applies Broadly:
      - Private Sector Employers
      - Public Sector Employers
      - Employment Agencies
      - Labor Organizations
      - Training Programs

The Genetic Information Nondiscrimination Act of 2008 (GINA)

- Employment Discrimination Prohibited
  - GINA incorporates by reference sections of other federal nondiscrimination laws, including Title VII of the Civil Rights Act of 1964, concerning coverage, confidentiality, enforcement and remedies.
  - Cannot act to deny an individual an employment opportunity or adversely affect the individual's status as an employee based on genetic information
  - Cannot retaliate for filing a claim of genetic information discrimination

The Genetic Information Nondiscrimination Act of 2008 (GINA)

- Cannot Discriminate based on genetic information when hiring/firing an individual
- Cannot Discriminate based on genetic information regarding compensation, terms, conditions and privileges of employment
- Employment Agencies cannot fail or refuse to refer an individual based upon genetic information and cannot encourage a prospective employer to discriminate based upon genetic information
- Labor Organizations cannot exclude or expel a member based upon genetic information and cannot encourage an employer to discriminate based upon genetic information
- Training Programs cannot refuse admission to, or employment in any program established to provide apprenticeship, training or retraining based upon genetic information

The Genetic Information Nondiscrimination Act of 2008 (GINA)

- GINA Restricts Employers Acquisition of Genetic Info
  - Prohibits Employers from requesting or purchasing genetic information related to an employee or family members
    - Exceptions:
      - Inadvertent Requests of Genetic Information ("water cooler problem"/ "Casual conversations")
      - Employee Wellness Programs
        - » Requirements (health benefits offered to employees as group, individual voluntarily provides written authorization, individualizes results of genetic services provided, employer receives info about such services only in aggregate without disclosure of individual's identity)
      - Requests for Family Medical Leave (employer may request family medical history to comply with FMLA)

The Genetic Information Nondiscrimination Act of 2008 (GINA)

- GINA Restricts Employers Acquisition of Genetic Info
  - Exceptions (cont.):
    - Purchase of Commercially and Publically Available Documents (*e.g.*, newspapers, magazines that contain information – obituaries -- does not apply to purchase of medial databases or court records)
    - Genetic Monitoring of Biological Effect of Workplace Toxins (written notice provided by employer, employee provides written authorization, employee told of results, monitoring complies with fed/state genetic monitoring regs such as OSHA, employer receives info in aggregate)
    - Law Enforcement Purposes (narrow exception – employer conducts DNA tests for law enforcement purposes as a forensic lab)
  - Even if Genetic Info Is Legally Acquired – cannot use it for discriminatory purposes or in violation of GINA's Confidentiality Provisions

The Genetic Information Nondiscrimination Act of 2008 (GINA)

- Employer Confidentiality Requirements
  - Genetic information if legally acquired must be maintained as a confidential medical record under the Americans with Disabilities Act ("ADA").
  - In addition to ADA requirements, GINA limits the disclosure of genetic information to instances which fit the following:
    - Disclosure to individual to whom info relates if requested by individual
    - To occupational or health researcher if research in compliance with regulations under 45 C.F.R. 46 (human research subjects)
    - In response to a court order

The Genetic Information Nondiscrimination Act of 2008 (GINA)

- Employer Confidentiality Requirements (Cont.)
  - To government officials investigating in compliance with GINA
  - Disclosures under the FMLA (Section 103) or similar state act
  - To federal, state or local public health agency only with regard to contagious disease presenting an imminent hazard of death or life threatening illness and the individual is notified
  - GINA does not prohibit authorized disclosures or use under HIPAA
  - GINA is not violated by the use or disclosure of medical information that is not genetic information about a manifested disease, disorder or pathological condition even if the condition has a genetic basis

The Genetic Information Nondiscrimination Act of 2008 (GINA)

- Remedies Against Employers
  - Same enforcement Under Title VII of Civil Rights Act
    - Lawsuits
    - Government enforcement actions by EEOC
  - GINA does *not* create a cause of action for disparate impact claims on the basis of genetic information (Genetic Nondiscrimination Study Commission – 6 years)
  - EEOC to provide final regulations within next year

Social Networks, Blogs and Employer Provided Resources

Concerns with the Resources

- Cognizant of Issues Including Privacy, Passwords, Off-Duty and Authorization, and Fact-Dependent Inquiries and Developing Law
- E-mail
  - Treated informally
  - Data security
  - Inappropriate content
- Blackberry's and PDA's
  - Treated informally like e-mail
  - Data security
  - Safety concerns
  - Off-the-clock work
  - Productivity/attention

Employer-Provided Resources

- Emerging technologies that can lead to privacy issues in the workplace
  - Cell phones
  - E-Mail
  - Instant Messaging (IM and Pagers)
  - Blackberry's and PDA's
  - Internet access (Blogs, Web-Surfing, Social Networking Sites)

Concerns with the Resources

- Texting/IM or Pagers
  - More informal than e-mail
  - Data security
  - Systems security
  - Safety concerns
  - Off-the-clock work
  - Productivity/attention

5 Major Employee Rights

- The right of free speech
- The right of privacy
- The right to respond to defamation
- The right to protest employer action
  - Illegal action and whistleblowing
  - Wages, hours and working conditions
- The right to be judged by performance

5 Major Employee Duties Limiting Unfettered Blogspeak

- Duty of care in hiring and retention
- Duty to provide a safe workplace
- Duty to provide an harassment-free workplace
- Duty to guard trade secrets and confidential information
- Duty to make judgments based on work-related information

Privacy Takeaways

- Assess what information is being collected
- Think through the types of data you are collecting
- Determine what laws apply to your company based upon the information it collects, where it does business and the identity of its customers

Privacy Takeaways

- Make sure that employees understand that they do not have an expectation of privacy in their use of your e-mail and electronic systems
- Consider what security systems you have in place and what securities measures you are requiring third parties to have
- Consider restrictions upon the use of removable media
- Make sure your privacy policy makes the necessary disclosures

Privacy Takeaways

- Reserve the right to modify your privacy policy
- Ensure that employees are aware of your policies
- Assess whether you have a responsibility to report a data security incident
- Consider what security systems you have in place and what securities measures you are requiring third parties to have
- Determine if you are sending or receiving data to countries that have higher privacy and security standards

Policies Should Address Blogging

- No unauthorized disclosure of trade secrets or other confidential, proprietary, non-public information allowed
- No unauthorized use of Company's name, logo, slogans, etc., allowed
- Do not allow blogging during work time
- Do not blog content that is disparaging, threatening, harassing, or inappropriate, about the Company or employees
- Employees should include disclaimers that the views expressed are solely those of the employees and not the Company
- Employees may be subject to discipline for violating the policy

Thank You!

John F. Birmingham Jr.
Foley & Lardner LLP
500 Woodward Ave
Suite 2800
Detroit, MI 48226
(313)234.7127
jbirmingham@foley.com

Andrew Serwin
Foley & Lardner LLP
402 West Broadway
Suite 2100
San Diego, CA 92101
(619)685.6428
aserwin@foley.com

John Yslas
Foley & Lardner LLP
555 South Flower Street
Suite 3500
Los Angeles, CA 90071
(213)972.4659
jyslas@foley.com