

Privacy In The Electronic Workplace

Whose Business Is It Anyway?

ALVARO HASANI, ESQ.
Phone: (908) 516-1058
Email: ahasani@fisherphillips.com

Today's Discussion

- Employer Rights — Workplace Searches, Monitoring and Surveillance
- Employee Privacy Rights — Source and Scope
- Impact of Technology



Whose Business Is It?

Employer's Right to Control and Protect Business

vs.

Employee's Interest in Privacy and Autonomy



Reasons for Workplace Search and Surveillance and Employee Monitoring

- Protect trade secrets and confidential information
- Increase productivity
- Prevent harassment/discrimination
- Investigate employee misconduct
- Track location of company equipment
- Improve workplace safety
- Monitor customer relations
- Protect company reputation
- Maintain computer network (prevent viruses, etc.)
- Minimize risk of data breaches
- Improve employee wellness

Statutory Protection for Employee Privacy

- Electronic Communications Privacy Act of 1996 (ECPA)
- Stored Communication Act (SCA)
- Fair Credit Reporting Act (FCRA)
- Americans with Disabilities Act (ADA)
- Family and Medical Leave Act (FMLA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Genetic Information Nondiscrimination Act (GINA)
- State off-duty conduct statutes

Common Law Invasion of Privacy

- Appropriation: the unauthorized use of a person's name or likeness to obtain some benefit
- Public disclosure of private facts: the dissemination of truthful private information which a reasonable person would find objectionable
- Intrusion: physical or electronic intrusion into one's private quarters

Intrusion

- Balance of Interests:
  - Did **employee** have a reasonable expectation of privacy?
  - Did **employer** have a legitimate business reason that outweighed the employee's privacy interest?

Balance of Interests

- Reduce Expectations of Privacy
  - Comprehensive Policies
    - "Business use only" / NLRB
  - Employee Acknowledgments

Balance of Interests

- Limit Intrusion
  - Is the search or monitoring necessary for the specific business purpose involved?
  - Is the search or monitoring designed to discover the information at issue?
  - Does the search or monitoring target only the relevant employee(s)?

Workplace Searches



Searching Employee's Company Computer

- Four-factor test to determine whether a reasonable expectation of privacy exists in the context of e-mail transmitted over and maintained on a company server:
  - whether the corporation maintains a policy limiting personal or other objectionable use;
  - whether the company monitors the use of the employee's computer or e-mail;
  - whether third parties have a right of access to the computer or e-mails; and
  - whether the corporation notifies the employee, or whether the employee was aware, of the use and monitoring policies.

Bingham v. Baycare Health System (M.D. Fla. 2016)

Searching Employee's Company Computer

Majority of courts have found that employees do not have a reasonable expectation of privacy in their work computers or in e-mails exchanged using a work account, especially when the employer retains a policy or otherwise notifies employees that their equipment or accounts are subject to monitoring

Searching Employee's Company Computer

Alamar Ranch, LLC v. County of Boise

No. CV-09-004-S-BLW, 2009 U.S. Dist. LEXIS 101866 (D. Idaho, Nov. 2, 2009)

"It is unreasonable for any employee in this technological age … to believe her communications via work-issued equipment and email addresses would be confidential and not subject to monitoring."

Searching Employee's Company Computer

- But what about attorney-client communications:
  - You have reason to believe that an employee is going to quit to go work for a competitor, and may be trying to take confidential information with him
  - You search the employee's company emails and recover deleted emails between the employee and his attorney discussing how to get out of his non-compete agreement

Searching Employee's Company Computer - Attorney Communications

Bingham v. Baycare Health System

Case No. 8:14-cv-73-T-23JSS (M.D. Fla. July 20, 2016)

- Plaintiff and his attorneys exchanged emails on Plaintiff's personal e-mail account, which contained a link to a cloud storage account where Plaintiff's attorneys had uploaded documents for Plaintiff's review. Plaintiff then forwarded certain e-mails from his personal e-mail account to his work e-mail account so that he could access the links from work. The forwarded e-mails contain discussions between Plaintiff and his attorneys, as well as links to documents
- The court found that the factors weighed in favor of finding that the Plaintiff had no reasonable expectation that the emails forwarded to his work e-mail were confidential and held, therefore, that they were not privileged

Searching Employee's Company Computer - Attorney Communications

Stengart v. Loving Care Agency

201 N.J. 300, 990 A.2d 650 (2010)

- Employer found .html files of Yahoo! account emails exchanged between a former employee and her attorney regarding the former employee's lawsuit against her Employer on her work computer
- Employee sent the emails from her personal, password protected email account
- Employee did not have express notice that messages sent or received on a personal, web-based email account are subject to monitoring if company equipment is used to access the account
- Emphasizing importance of privacy concerns inherent in attorney-client communications, the New Jersey Supreme Court held that such communications were privileged – even though on Employer's computer

Searching Employee's Company Computer - Attorney Communications

Holmes v. Petrovich Dev't. Co., LLC

191 Cal. App. 4th 1047, 119 Cal Rptr. 3d 878 (Cal. App. 2011)

- Employer found emails exchanged between employee and her attorney regarding suit against employer exchanged using the employer's email and computer systems
- California appellate court held that such communications were not protected by the privilege
- "Akin to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by others."

Stored Communications Act

- Federal statute prohibiting intentional, unauthorized access to a stored wire, oral, or electronic communication
- Creates privacy expectation in stored electronic communications



Stored Communications Act

- Facebook posts are protected “electronic communications” under the Stored Communications Act, so long as the posts are limited to friends and not on the person’s public Facebook pages.
- Even though Facebook posts are protected, an employer does not violate the Stored Communications Act if the employer receives the posts from someone authorized to obtain them.

Stored Communications Act

- Employer violates the Stored Communications Act if it obtains Facebook (or other electronic communications) by:
  - Using a password retrieved from the hard drive of the employee's employer-owned electronic device.
  - Accessing the account by using the employee's employer-owned device where the password populates automatically.
  - Creating a fictitious person on Facebook to friend the employee.
  - Pressuring co-workers into divulging the employee's Facebook posts.

Stored Communications Act

Pietrylo, et. al v. Hillstone Rest. Group

No. 06-5754, 2009 U.S. Dist. LEXIS 88702 (D. N.J., Sept. 25, 2009)

- Password-protected chat forum and blog for employees
- Management requested access to the blog
- Employees terminated based on content found on blog
- Dispute on whether access to social media site by supervisor was coerced
- Jury found in favor of employees and a violation of the Stored Communications Act

Stored Communications Act

Ehling v. Monmouth Ocean Hospital Service Corp.

- Employee's Facebook page was set for "Friends" only, which included some co-workers, but no managers
- One "Friend" captured screen shots of the plaintiff's wall and emailed them to managers
- Managers never asked for screen shots
- Employee terminated
- Court held that the Facebook wall posts were covered by the Stored Communications Act but … the SCA's authorized-user exception applied because a "friend" voluntarily emailed the screen shot to a manager without any request or coercion

Stored Communications Act

Pure Power Bootcamp, Inc. v. Warrior Fitness Boot Camp, LLC

759 F. Supp. 2d 417 (S.D.N.Y. 2010)

- Employer logged into employee's Hotmail account that employee had used during work hours and on work computer
- Employee left username and password on the workplace computer
- Court found violation of the Stored Communications Act

Social Media

- Non-private posts are fair game, but not risk-free
  - Pre-Employment Screening
    - Looking for red flags: Attitudes/behaviors that do not mesh with employer's core values, pose potential liability for employer, or indicate propensities for misbehavior
    - But Facebook profile/pictures may include significant information about protected characteristics
    - Important defense for failure to hire claim is ignorance of protected characteristics
  - Policy Violations
    - Unauthorized disclosures of confidential information
    - Disparaging the Company's services, products or customers and vendors
    - Harassment/discrimination
    - Misuse of employee work time
    - Workers' compensation or leave fraud

Social Media

National Labor Relations Act:

- §7 – “Employees shall have the right … to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection.”
- §8(a)(1) – “It shall be an unfair labor practice for an employer to interfere with, restrain, or coerce employees in the exercise of rights guaranteed in §7 of this act.”

Off-Duty Conduct

- Competing interests:
  - Employee's right to be free from employer's control while away from work and for conduct that does not impact job.
  - Employer's desire to enforce policies, minimize liability, protect assets and reputation.



Off-Duty Conduct

- Not all employee off-duty misconduct may be subject to discipline
- Best approach is to:
  - Regulate off-duty conduct when there is a legitimate operational or business need
  - Analyze the connection between the conduct and the employee's job
  - Use balanced judgment on a case-by-case basis

Off-Duty Conduct

- Typical off-duty misconduct for which discipline may be appropriate
  - Moonlighting
  - Breach of confidentiality
  - Insubordination
  - Fraternization
  - Statutory Discrimination

- Duty to investigate and remedy off-duty conduct
  - *Espinoza v. County of* Orange, 26 AD Cases, 2012 WL 420149 (Cal. App. 4 Dist. 2012); *Blakey v. Continental Airlines, Inc.*, 164 NJ 38 (2000)

Off-Duty Conduct

- Illegal Activity/Arrests
  - Nature of arrest
    - Misdemeanor/felony
  - Duties of job and ability to perform
    - Loss of license?
  - Future liability of employer
    - Negligent retention
  - Conduct own investigation
  - Consider other policies that may impact
    - Attendance or failure to report

Employee Monitoring

- E-mail
- Social media
- Key logging
- Telephone
- GPS technology
- Biometrics

Key Logging

- General Capabilities:
  - Capture any passwords entered by users on the device
  - Take screen captures of the device at periodic intervals
  - Record the urls that were visited via web browsers, and possibly take screen captures of the web pages viewed
  - Record a list of the applications run by users on the device
  - Capture logs of all instant messaging (IM) sessions
  - Capture copies of sent emails
- Invisible and designed to prevent tampering

Key Logging

- Benefits:
  - Can be used to maintain productivity
  - Can protect valuable bandwidth
  - Can help to ensure optimum use of networked resources by monitoring employee activity online
- Risks:
  - SCA
  - ECPA
  - State Wiretap Acts

Key Logging

- Best practices:
  - Install only on employer-owned devices
  - Obtain employee consent
  - Draft policies notifying employees that workstations are monitored and obtain employee acknowledgement of policies
  - Don’t allow anyone to access passwords for an employee’s private accounts recovered through the keylogger

Telephone Monitoring

- Federal Wiretap Act/Florida Security of Communications Act
  - Prohibits the intentional interception (or attempted interception), disclosure, or use of any wire, oral or electronic communication
- Exceptions
  - Consent
  - Business extension exception

Telephone Monitoring

- Consent
  - One party consent under federal law
  - One party consent under NY, NJ law
  - All party consent under Florida law
  - May be express or implied
- Business Extension Exception
  - Employers acting in the “ordinary course of business” may electronically monitor, using a telephone extension, any business-related communication, without the employee’s knowledge or consent
  - Employers may not, however, monitor communications of a purely personal nature

GPS Technology

- What is “GPS?”:
  - “Global Positioning System”
  - GPS navigation utilizes a system of satellites orbiting the earth; GPS satellites receive signals from the ground, triangulate the signals location and send location information back to the receiver
  - Allows employers to know the location of a company vehicle or specific employee

GPS Technology

- Common Monitoring Techniques
  - Placing a GPS tracker on a company-issued vehicle
  - Issuing company-owned smart-phones with GPS tracking capabilities
  - Placing trackers on personally-owned vehicles used in work-related activities

GPS Technology

U.S. v. Jones

132 S. Ct. 945 (2012)

- Right to privacy in aggregate of locations:
  - Give notice of GPS tracking to employees
  - Limit the use of GPS trackers to company-owned property
  - Use GPS tracking for a specific purpose
  - Only collect/store information that impacts job performance

Biometrics

- Hand scanners
- Fingerprint scanners
- Iris scanners
- Retinal scanners
- Face recognition
- Voice recognition
- Vein recognition
- Fitness trackers (Fitbit, Nike+FuelBank, Jawbone UP)



Biometrics

- Employer uses:
  - Establish records of employee hours
  - Provide security
  - Restrict access
  - Promoting health - biometric screening

Biometrics

- Wearables:
  - Google Glass
  - Fitbit, Jawbone
  - Apple Watch
- Employee Privacy Concerns

Biometrics

EEOC v. Consol Energy, Inc.

(N.D. W. Va. 2016)

- Company implemented biometric hand scanner for clocking in and out
- Long-term employee refused to use new system because he believed it was “Mark of the Beast”
- Requested religious accommodation to avoid damnation
- Company refused and threatened discipline, and employee resigned
- After jury trial, awarded more than $600,000

Biometrics

- Check all applicable privacy and other potentially relevant laws before implementing a system
- Consider employee morale
- Notify all employees, in writing, of intent to use a biometric system
- Explain purpose
- Get employee's written consent
- Implement strict security policies for secure storage and safeguarding of all biometric data
- Be ready to consider accommodation requests

Bring Your Own Device Policies

- Authorize your employees to use personal electronic devices in the workplace in order to conduct business for the employer
- Risks to consider:
  - Wage and hour claims
  - Confidential information/trade secrets loss
  - Third-party data breach
  - Invasion of employee privacy
  - Electronic discovery/litigation hold burdens



Bring Your Own Device Policies

- Include specific monitoring and no expectation of privacy provisions in your B.Y.O.D. policy and, importantly, require explicit employee consent to access and deletion of company information
- Define permitted and prohibited uses of B.Y.O.D. and consequences for violations – be consistent in enforcement
- Litigation Hold / Preservation
  - Include provisions in your B.Y.O.D. policy that notify employees of hold duties in personal devices
  - Explicitly discuss forensic imaging of devices in policy

Working on Personal Computers and Personal Electronic Devices

- Between the employer and employee, who:
  - Owns or **controls** the data on the personal device?
  - Has a right to inspect data on these devices?
  - Has an obligation to preserve data on these?

What Does “Control” Really Mean?

Puerto Rico Telephone Co., Inc., et al., v. San Juan Cable, LLC

2013 WL 5533711 (D. Puerto Rico Oct. 7, 2013)

- An employer failed to preserve emails from the **personal** email accounts of three managing officers
- A federal court found “control” by the employer
- The lost emails were in the employer’s control because it *“presumably knew its managing officers used their personal email accounts to engage in company business, and thus its duty to preserve extended to those personal email accounts.”*

What Does “Control” Really Mean?

Digital Vending Servs. Int’l v. Univ. of Phoenix, Inc.

2013 WL 5533233 (E.D. Va. Oct. 3, 2013)

- An employer failed to preserve a thumb drive owned and used by its managing director
- A federal court found “control” by the employer
- The employer *“had control over the thumb drive when it went missing”* because even though the managing director had personal possession of the thumb drive, his employer had the authority and ability to ask him to preserve the documents and things in his possession

Workplace Surveillance

- Cameras:
  - Video
  - Audio
- Limitations:
  - Location
  - NLRA:
    - Unfair Labor Practices
    - Collective Bargaining Obligations



THANK YOU

FOR THIS OPPORTUNITY

ALVARO HASANI, ESQ

ahasani@fisherphillips.com
(908) 516-1058