Employee Privacy in the Social Media Age

Presented by:
Amber Elias
Phone: (617) 532-9323
Email: aelias@fisherphillips.com

Employee Privacy

- Workspace Searches
- Employee Monitoring
- Off-duty Conduct

Guiding Principles

- Is the search or monitoring necessary for the specific business purpose involved?
- Is the search or monitoring narrowly tailored to quickly and accurately discover the information at issue?
- Does the search or monitoring target ***only*** the relevant employee(s)?

Guiding Principles

- Does the company have a policy?
- Was the employee notified of the policy?
- Has the policy been consistently implemented and enforced?

Workspace Searches: When to Search

Start with Guiding Principle:

Is it necessary for the specific business purpose involved?

Workspace Searches: What to Search

Next Guiding Principle:

Is the search narrowly tailored to quickly and accurately discover the information at issue?

- Too broad – sweeps in information employees reasonably expected to be private
- Too narrow—misses key info, defeats the purpose of the search

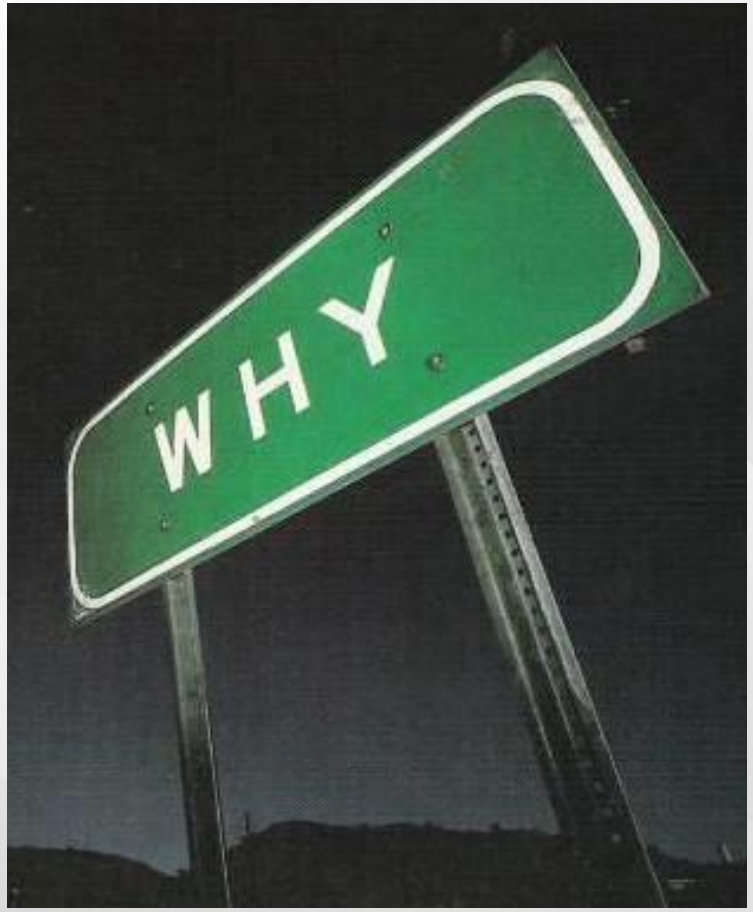
Workspace Searches: What to Search

- Cubicles and offices
- Company computers
- Lockers
- Desks
- Company email
- Company instant messaging programs
- Company cell phones and PDAs
- Company laptops

Workspace Searches: What Not To Search

- Employees' purses and wallets
- Employees' personal cell phones or PDAs
- Employees' personal laptops
- Employees' personal email accounts

Monitoring



What is the business purpose?

- Protecting confidential information
- Protecting business reputation
- Tracking attendance and working time
- Preventing civil or criminal lawsuits

Steps To Take Before Monitoring

- Determine what information is confidential and limit access
- Have employees sign confidentiality agreements
- Secure the physical network and other network technology by restricting access
- Limit access through security protocols such as password or access privileges and individual drive locations
- Install filters & firewalls restricting internet access

Steps To Take Before Monitoring

Consider federal and state laws:

- Stored Communications Act
- Computer Fraud and Abuse Act
- Wiretap Act
- Electronic Communications Privacy Act
- State laws

Monitoring – Company Email and Computer Use

No Expectation of Privacy

- Tell employees that they will be monitored, how they are to be monitored, and what is to be monitored.
    - Put it in writing and make it clear and as extensive as possible
- Reinforce the issue that there is no expectation of privacy on the employee's part often
    - Acknowledge on a pop-up screen each time he or she logs into the computer

Monitoring – Company Email and Computer Use

Consistent Enforcement

Policies must be enforced regularly and consistently

If not:

- Discrimination / Retaliation
- Lose support for argument that all efforts have been taken to keep the Company's confidential information confidential

Monitoring - Telephone

What is the business purpose?

- productivity, quality control, customer relations

Business calls v. personal calls

Consent – state law ordinarily dictates whether the consent of participants is requires

Monitoring – Video Surveillance

What is the business purpose?

- deter theft/unlawful conduct, maintain security, monitor productivity

Location of Video - no bathrooms or locker rooms

Audio transmission – may violate federal/state wiretap laws

Monitoring – Social Media

What is the business purpose?

- Checking backgrounds in hiring process
- Protecting confidential information
- Protecting business reputation
- Tracking attendance and working time
- Preventing civil or criminal lawsuits

Monitoring – Social Media

Be careful when monitoring - you may regret what you learn:

- Race
- Religion
- Age
- Genetic Information
- Disability Information
- Sexual Orientation

Monitoring – Social Media

Tips for Managers

- Don’t become “friends” with employees
- Don’t reveal anything you wouldn’t say or post in public
- Don’t engage in fraud (“fake” friend requests or passwords)
- Use privacy controls to manage flow of information
- Remember web content can be false

Monitoring – Social Media

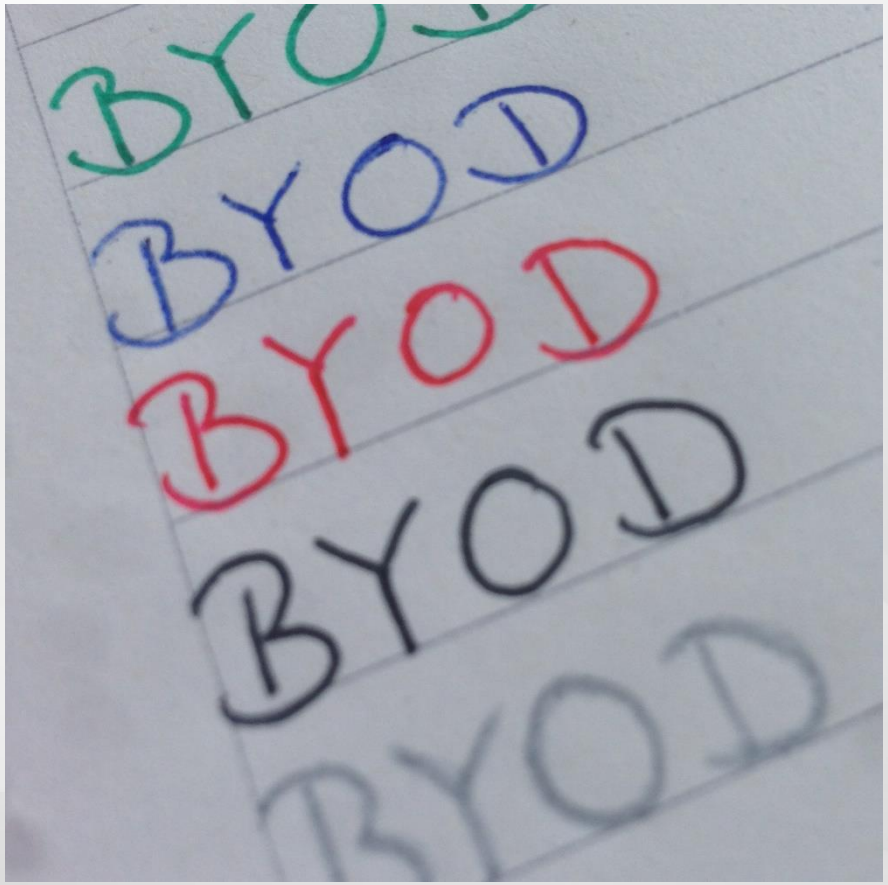
- Do not try to obtain employees' social media passwords
- Consistently monitor the COMPANY'S online presence
- Set up an alert service to track posts about the company
  - Helps track what employees are saying
  - And what the public is saying

Monitoring – Social Media

NLRB Protections:

If employees are discussing terms and/or conditions of employment, e.g., wages, discipline may be impermissible in certain circumstances as the employees may be engaging in "protected activity."

Monitoring – Bring Your Own Device



Benefits of BYOD

Employer:

- Cost shifting
- Increased productivity through access to resources
- Increase employee satisfaction

Employee:

- Carry one device, not two
- Flexibility of work – time and location
- Satisfaction

Monitoring – Bring Your Own Device

Risks of BYOD

Security

- data breach/loss
- malware & viruses
- lost/stolen devices

Litigation

- e-discovery
- control
- preservation

Monitoring – Bring Your Own Device

BYOD Policy

- language reducing any expectation of privacy and monitoring if being done
- advise that access is a privilege and what acceptable use is
- what to do if device is lost or stolen
- security requirements
- preservation requirements

Monitoring – Bring Your Own Device

BYOD Policy

Connect BYOD policy to other policies:

- harassment
- trade secrets/confidentiality
- social media

Monitoring/Discipline: Off-Duty Conduct

Can an employer monitor or discipline employees for conduct that occurs when an employee is off-duty and off-premises?

Monitoring/Discipline: 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.

Discipline: Illegal Off-Duty Conduct

- If employer learns that a worker has engaged in illegal off-duty conduct, can the employer ask the worker about it?
- In many states, and according to EEOC, answer is “no,” unless the off-duty illegality has some concrete impact on the employee’s work or the employer’s business.
- E.g. – drunk driving conviction of bus driver or embezzlement conviction of bank employee

Discipline: Legal Off-Duty Conduct

At-will Employment

Employer can terminate an employee at any time, for any reason, no reason or even bad reason, as long as it is not an unlawful reason.

Discipline: Protected Off-Duty Conduct

State Law

Expansive laws protecting spectrum of conduct

- 17 states have "tobacco only" statutes: CT, DC, IN, KY, LA, ME, MS, NH, NJ, NM, OK, OR, SC, SD, VA, WV and WY
- 8 states protect use of lawful products (i.e. tobacco, alcohol): IL, MN, MO, MT, NV, NC, TN and WI
- 4 states offer statutory protection to those who engage in lawful activities: CA, CO, NY and ND

Discipline: Off-Duty Conduct

Marijuana Laws

- Medical or recreational marijuana legal in 25 states and DC
- 8 contain provisions prohibiting adverse action against worker for participating in program
- *Coats v. Dish Network, LLC* (June 15, 2015) – Lawful activity state (CO). Colorado Supreme Court held law did not protect off-duty marijuana use because nothing illegal under federal law can be legal under the statute.

Guidelines

- Recognize that this area is growing and that the law and trends are still developing
- Always check state law before taking action
- All discipline must be handled in a consistent, non-discriminatory and non-retaliatory manner
- ***THINK FIRST--ACT SECOND!***

Final Questions?

Presented by:
Amber Elias
Phone: (617) 532-9323
Email: aelias@fisherphillips.com

Thank You

Presented by:
Amber Elias
Phone: (617) 532-9323
Email: aelias@fisherphillips.com

How Can your HRG Assist

Seminar: Social Media in the Workplace

- Provide Social Media Guidelines
- Review internal and external Risks
- Include the Paychex Social Media policy in your employee handbook

- **Update Current Handbook to include**
  - Workplace Search Policy
  - Social Media Policy
  - Internet and Computer Policy

Your Paychex HR Generalist Team

Donna Denoyelle - 603.471.2590, x5228427, ddenoyelle@paychex.com

Maria Dongas – 603.471.2590, x5228499, mdongas@paychex.com

Karen Fernekees – 603.471.2590, x5228467, kfernekees@paychex.com

Tanya Derouin– 207.784.0178 x5228470, tderouin@paychex.com

Angela Freitas – 207.871.8646, afreitas@paychex.com

Jackie Hoyt – 603.471.2590 x5228463, jhoyt@paychex.com

Sheila Soule – 603.471.2590 x5228492, ssoule@paychex.com