EMPLOYMENT LAW | CIVIL & BUSINESS LITIGATION

www.WhitneyLawGroup.com

Marblehead MA | Burlington MA | Portsmouth NH | New York NY

WHITNEY LAW GROUP, LLC

EMPLOYMENT LAW | CIVIL & BUSINESS LITIGATION
www.WhitneyLawGroup.com
Marblehead MA | Burlington MA | Portsmouth NH | New York NY

PRIVACY/CONFIDENTIALITY IN THE WORKPLACE

NBI Seminar Manchester, NH
November 20, 2019

Topics to Cover

- Employee Privacy “101”
- Sources of privacy law
- Monitoring by Ers
- Scary stats about EE activities
- Risks of email, texting, BYOD, social media, internet
- GPS tracking
- E-mail and internet monitoring
- Video surveillance
- Monitoring of phone calls and voicemail
- Best practices to protect confidential information, trade secrets, IP
- Key take-away points

Technology Issues

- Increased use of technology in the workplace has created new concerns for both ERs and EEs in the areas of privacy and confidentiality:
  - E-Mail
  - Texting
  - The Internet / social media
  - Wireless devices
  - GPS
  - Video and audio surveillance
  - Data storage devices and cloud storage

EE Privacy "101"

- Conflict exists between EE's right to privacy and the ER's right to monitor use of its equipment and investigate misconduct
- NH law protects EE from surveillance, but contains carve-outs for ERs
- Only protected in "private place": "a place where one may reasonably expect to be safe from surveillance including public restrooms, locker rooms, the interior of one's dwelling place, or any place where a person's private body parts including genitalia, buttocks, or female breasts may be exposed."
- ER can conduct surveillance in a "private place" for variety of reasons, including illegal activity, violation of regulations, fraudulent activity, etc.

Pertinent Sources of Law

- 4th Amendment
  - Protection against searches and seizures
- Federal law prohibits interception of electronic communications
  - Business exception
- State wiretap law prohibits monitoring of conversations without consent of all parties
  - Some states are more lenient (e.g., NY)
  - This arises frequently in HR situations
- NH privacy law – no private right of action
  - Administered and enforced by AG

NH Privacy Laws re: Social Media and E-Mail

- ER cannot require EE or applicant to:
  - Disclose login info for a personal account
  - Add a person to an EE/applicant's list of contacts associated with personal account
  - Reduce the privacy settings of a personal account to permit 3rd party to view the contents
- ER can't discipline or threaten to discipline an EE for failing to do any of the above

So what can an ER do?

- Adopt policies concerning use of equipment, including email, internet, social media
- Monitor use of equipment and software
- Obtain information about EE from public domain
- Insist on limited access to personal accounts for purpose of investigating employee misconduct
- Demand that EE provide login info for access to:
  - Account or service provided because of employment
  - Electronic communication device or online account paid for by ER

Why Monitor?

- Protection of IP
- Legal liability and compliance
  - Investigating harassment/wrongdoing
- Ensure proper use of company assets
- Prevention of theft
- Job performance / productivity
  - Maximize ROI
  - Most expensive recurrent cost on budget

Scary Statistics

- EEs waste up to 2 hours per day on non-business activities
- 50% of EE do personal web surfing
- 70% of adult-oriented web traffic is between 9am-5pm

Monitoring Survey

- Internet connections = 61.6%
- Email = 46.9%
- Video record of job performance = 11.7%
- Telephone conversations = 8.5%
- Voicemails = 7.6%
- Computer files = 3.63%

(AMA Survey)

Data Theft Study

- nearly 60% of employees who leave job take company data
- 79% of those who took data said that they did it despite knowing the employer prohibited taking
- 67% said that they took data in order to leverage their new job
- types of data taken
  - 65% took email lists
  - 45% nonfinancial business information
  - 39% customer contact lists
  - 35% employee records
  - 16% financial information
- 24% said that they continued to have system access after last day of work

Lessons from SCOTUS Sexting Case

- *Quon v City of Ontario*
- Implement broad policy that covers technologies used by EEs
- Communicate policy clearly
- Any ER search should be based upon legitimate business reasons
- Conduct search as narrowly as possible
  - Minimize intrusiveness

More lessons …

- Technology use policy language is vital
  - Define technologies covered
  - Broad language
  - State no expectation of privacy in use of company systems
  - Advise that deleted information is accessible
  - Address temporary internet files
  - Centralize modification of policy (for consistency)

Communicating With Lawyers Using Company Computers

- Does an EE waive the A/C privilege when sending emails using ER's equipment?
  - Using company email?
  - Using company internet and personal email?
- Law is still developing on this issue

GPS Monitoring

- Increased use by ERs
  - Route efficiency
  - Improve safety and deter theft

- Also raises privacy concerns
- *Vitka v. City of Bridgeport* (1/10)
  - CT Court upheld municipality's right to monitor movement of fire marshal

E-Mail: efficient tool, but not without risk

- Poses significant hazards
- Discovery tool for lawyers
  - Informal nature of communications
  - Often creates great evidence
  - E-mail never dies!!!!!!!
  - Consider electronic retention policies
- Potential for misuse
  - Harassment, "Spoofing"
  - Proprietary information may be lost

Texting, a new nightmare

- The ubiquity of texting is overtaking some forms of business communication
- Many employees prefer it over email, especially millennials
- Creating new problems
- Harder to monitor than email
- Often commingled with employees' personal texts
- Creates serious risks of goodwill impairment

Bring Your Own Device (BYOD)

- BYOD refers to an EE's use of personal devices to conduct business on behalf of an ER
- Interop survey found 95% of respondents indicated that their organizations have embraced BYOD, but only one-third of these companies have BYOD policies in place

Social Media

- LinkedIn, Twitter, and other social media platforms creates more confusion about employee privacy rights
- Employers can control social media connections for certain key business relationships
- Contracts are key here
- Ownership of social media accounts are vital to address as well

Internet Use and Misuse

- Allows for the exchange of information at little cost
- Provides significant resource to EE
- Pitfalls:
  - Hostile work environment
  - Decreased productivity from inappropriate or personal use
  - Copyright infringement
- Consider tracking or blocking software
- Adopt policy

Video Surveillance

- Generally okay in "open" areas
  - Hallways, lobbies, EE cafeterias, open offices, warehouses, any areas open to the public
  - Okay with hidden or visible camera, with or without notice
- Prohibited where EE has reasonable expectation of privacy
  - EE dressing rooms, bathrooms, desks, lockers
- Think carefully about video surveillance –touchy issue
- Audio/video may be prohibited by wiretap statute

Tips for handling monitoring oral communications:

- Limit monitoring activities to situations where there is an important business purpose.
- Inform EEs in advance and in writing that the company will monitor telephone calls and electronic communications, such as voice mail, e-mail and the Internet.
- Provide a mechanism for notifying the non-EE party to the communication that the call may be monitored for quality control purposes.

Monitoring Oral Communications (cont'd)

- Only monitor personal calls long enough to determine that the call is personal and not of a business nature.
- Do not monitor purely personal calls.
- If personal information is learned through monitoring, the personal information should not be disclosed to others, unless there is a compelling business need to do so. Even then, the information should be disclosed only on a need-to-know basis.

The tools for a CI protection program will include:

- Computer safeguards
- Security measures regarding the use and disposition of all electronic technologies (USB drives, flash cards, smartphones, FTP sites, social media sites, etc.);
- Restrictions on and protocols for access to and use of facilities (electronic and physical) that store confidential information; Companies should restrict access to those people who need to know the subject confidences, and not grant access to all employees or vendors.

The tools for a CI protection program will include (cont.):

- Policies for the use of company property, computer hardware and software; confidential software and database contents can be protected by a password protected pop-up form that notifies employees and others that they are dealing with protectable trade secrets;
- Protocols for accessing, handling, marking, storing, retaining, and shredding paper documents (such as “confidential” legends, use of locked file cabinets, adoption of a “clean desk” policy);
- Protocols for sharing information with third parties; including restricting the scope of the third-parties who will be granted access to the trade secrets;

The tools for a CI protection program will include (cont.):

- Implementing procedures for ensuring employee awareness of all policies and procedures, including through new employee orientations and on-boarding procedures, the use of employee handbooks, discussions of the policies at meetings, ongoing trainings, and scheduled computer pop-up reminders;
- Protocols and checklists used when an employee resigns or has been terminated covering exit interviews, shutting down computer accounts, terminating cell phone accounts, eliminating facility access, examining all items taken by the employee, including by computer forensics.
- Post-departure reviews of possible security breaches; and restrictive covenants entered with employees and others.

The tools for a CI protection program will include (cont.):

- Use of basic types of restrictive covenants include the following
  - Noncompete agreements;
  - Garden leave clauses;
  - Forfeiture-for-competition agreements;
  - Compensation-for-competition agreements;
  - Nondisclosure, or confidentiality, agreements;
  - Nonsolicitation and no-service agreements;
  - Antipiracy, no-raid, and no-hire agreements;
  - Invention assignment agreements; and
  - Return of property agreements and data device inspection agreements and policies regarding employee use of social media.

- Each of these protective measures serves a specific purpose. Which to use, when to use them, how to properly craft them, and how to enforce them are determined by a combination of the needs of the company, the corporate business needs, and the skill, knowledge, and experience of the attorney working with the company. Proper attention to each of these issues in advance will save much-needed time and unnecessary expense later.

Corporate security expert Bo Dietl (l.) watches as Roger Eaton, president of KFC USA, places Colonel Harland Sanders' handwritten Original Recipe into KFC headquarters' newly modernized vault Monday. (Bohannon/AP)

WHITNEY LAW GROUP, LLC

COCA COLA VAULT: WHERE IS THE SECRET FORMULA KEPT?

Avatar **ALEKSANDAR MISHKOV**
/ published 2 years ago

15,255 **FOOD/DRINK** **HISTORY**

WHITNEY LAW GROUP, LLC

Termination Concerns

- Property return
- Leaving “naked”
- Reminder of contractual obligations
- Delinking of social media contacts
- If concerned about EE, use forensics, preserve PC and server

Take-Aways

- Policies are critical
  - Set expectations
  - Be clear
- Only monitor what you own or can access publicly
- Monitor narrowly
  - E.g., business hour usage
- Monitor only to consider legitimate business issue
- Unionized workforce – address in CBA
  - E.g., GPS likely mandatory bargaining item
- Public sector ERs have more legal issues to consider

EMPLOYMENT LAW | CIVIL & BUSINESS LITIGATION
www.WhitneyLawGroup.com
Marblehead MA | Burlington MA | Portsmouth NH | New York NY

THANK YOU!