

**THE BIGGEST EMPLOYMENT
LIABILITY ISSUE
PRIVACY AND ELECTRONIC
COMMUNICATION
(DIFFICULT SITUATIONS IN THE
ELECTRONIC WORKPLACE)**

by
Bob Gregg
Boardman Clark Law Firm

**The Growth Area in Business
and Liability**

- Technology improves our ability to enable people in the workplace.
- Technology improves the scope of business, communication and recordkeeping.
- Technology has created an explosion of legal issues and organizational liability.

Agenda

- Introduction
- Electronic Discovery
- Handling Difficult Situations between Employees
 - Complaints
 - Rumors
 - Improper use and harassment
- Privacy and Confidentiality
 - Employee right to control the system
- Off the Job (?) Use
 - What is off the job, FMLA, negligence, social media
- Conclusion

Discussion Example

You and two other managers have been emailing regarding your frustration with a new employee. You all agree she's capable of doing an adequate job but has a bad attitude. She doesn't seem to have the motivation. She's also not very bright and has been very slow at learning. She doesn't appear to listen when talked to. She seems to have an "I don't care" attitude. She is absent a lot! The latest email had a touch of frustrated sarcastic humor. "She's used every excuse in the book to be absent. I bet next she'll claim to be pregnant and we'll be stuck with FMLA!"

Electronic Discovery Rules

Electronically Stored Information (ESI)

"Writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained."

**Rediscover Verbal
Communication**

Your email is "evidence"

Don't Speculate

Don't brainstorm serious topics by email.

- "String emails" on serious topics can become problematic

- Email blowups
- Email wars

- Not just the Email**
- Reports
 - Graphics
 - Electronic files
 - Charts
 - Records
 - Contracts
 - Drafts and redrafts
 - Calendars
 - Network access records
 - "Documents of any kind"

- Not just the Computer**
- Computer use (Intranet and Internet)
 - Telephones
 - Cell phones
 - Text messages
 - Tapes, CDs, disks
 - Locaters/global positioning
 - Electronic calendars
 - Message systems

Busted by your Blackberry?

Your "personal" devices may not be personal.

Bring Your Own Device to Work (BYOD)

Opens your personal life to discovery

May give employer the right to monitor, control and delete your personal information

Rule 26(a) requires that employers disclose, at the beginning of litigation and prior to any discovery by plaintiffs, a copy of, or a description by category and location of, any documents (paper or electronic) that may support its claims or defenses.

**Rule 26F
Preservation**

- Freeze the system on “notice”
- To archive, or not?

Failure to Preserve is “Spoilation”

Sanctions for Spoilation

- You pay to have it restored.
- You pay penalties.
- The Court “suppresses” your evidence.
- Presumption of guilt.
- **You lose!** Court grants summary judgment due to your bad faith.

**Difficult Situations Among
Employees**

Dick, who is recently divorced, and Jane, who is married, both work in the same area of the building. Recently they have been frequently spotted going to lunch together or having a drink after work. Their co-workers also report that on breaks the two tend to seclude themselves from others, talk quietly and smile a lot. Email rumors are now circulating about Dick and Jane's "affair," and several employees have expressed indignation about "that couple's behavior."

- Office gossip email magnifies the impact.

Duty of Care for the Workplace Environment

Duty to Act

Where is "the line?"

- Committed criminal acts
- Is an alcoholic
- Is drug dependent
- Has and/or is spreading a serious contagious disease
- Committed professional malpractice
- Committed infidelity in one's marriage or serious relationship
- Received a promotion or other job benefits by sex, bribery or other illicit ways
- Comments that reveal medical information without consent
- Divulging negative employment information (discipline, performance evaluations, reasons for discharge) to those who do not have a need to know.
- Comments or speculation over sexuality--or lack thereof--or sexual orientation.

- Discrimination
- Defamation
- Invasion of Privacy
- Negligent Supervision

Mark has a network of friends who exchange humor by email. They send him some pretty good ethnic and sex jokes. Mark knows some of his co-workers would get a kick out of these, so he forwards them to their work PCs. Of course, Mark is very careful; he would never send a joke or video clip to anyone he thought might not like that sort of humor.

Harassment

Duty of equality to employees, customers, public, etc.

- It was just a joke
- The email is your ad

- Have a Policy on
“Inappropriate Use”**
- Enforce it
 - Educate your workforce

- Duty of Care**
- To monitor
 - To report illegal usage
 - Pornography
 - Identity theft
 - Computer fraud

Electronics Communication Act

- Have effective use and monitoring policies
- Right to intercept and inspect authorization

Privacy

The balance between the organization's right to control and the individual's privacy.

- Monitoring
- Electronic surveillance and security
- Social media monitoring
- Bioscanning

Privacy

1. Not job related

Privacy

1. Not Job Related
2. Expectation

Policy

- No privacy statement
- Organization's ownership
- Interception and monetary
- User's authorization

Don't Undermine the Policy!

- *Quon v. City of Ontario* (U.S. Supreme Court, 2010)

Privacy

1. Not job related
2. Expectation
3. Confidentiality and Security

Information Security

Federal Fact Act

- Requires electronic obliteration of personally identifiable information when discarded.

State Laws

- Invasion of privacy, defamation, theft of trade secrets and negligent supervision (Wis. Stats. 968.31, Interception and Disclosure of Wire, Electronic or Oral Communications).

BYOD

- Does information on personal device void a confidentiality agreement?
- Whose property is it?
- Social networking for work puts customer information out on personal device

Trade Secret Act

- Covers access by "improper means" and "misappropriation"
- Employer gave permission. Access and retention is not improper or misappropriation

- Policy on proper access
- Security agreement
- Ability to delete (if possible)

Confidentiality

- The most common breach of privacy
- Careless use of personal information

Sometimes it is the intent to be "helpful" which does the harm.

- Have clear confidentiality policies
- Identify those who "touch" confidentiality
- Give training

Off the Job?

- Or still on the hook for liability?

Wage and Hour Considerations

- Electronic communications make it difficult to be "off the clock."

Family and Medical Leave Act

- Electronic work can create eligibility
- Electronic contract during leave can violate FMLA
- Work from home can mean the leave did not count as FMLA and must be paid

Employee Negligence

- Work product
- Security breaches (family members)

- Have clear policies on work from home
- Approval of all hours
- Reporting and tracking of hours

Safety

- OSHA Distracted Driving Rules
- A policy is essential

The Social Network and Privacy

- Not job related
- Expectations of privacy

Off-work social networking is generally not "private" except for secured access sites

Secured sites are private

Relationship to the workplace may allow employers to act on inappropriate off-work social media behavior.

Richardson v. Beckmann (9th Cir., 2009)

Off-Duty Conduct

Does the employee's off-duty conduct have a connection to the workplace?

- Injury to the employer's business or operations;
- Inability to report for work.
- Unsuitability for continued employment.
- Other employee(s) refusal to work with the off-duty offender, or danger to other employees.

Duty of Loyalty

but

- First Amendment (for public employees)
- Concerted activity

*In re American Medical Response
of Conn.* (NLRB, Oct. 2010)

- Concerted activity
- Overbroad policy

Balance of legally or
constitutionally protected
speech of “public concern”
vs.
harassment, bullying, personal
vendettas, undermining the
public trust

Policy and Practice

Electronic Communication Policies

- Computer use
- Personal use guidelines
- Right to inspect
- Security

Collateral Policies

- Cell phones and other electronic devices
- Harassment
- Illegal activities
- Access to and confidentiality of information

Do monitor

Do act to correct misuse

Do train staff
about proper use

Security and confidentiality

Do have an
Information Retention Plan
for discovery obligations


