2011 Chicago Board Association Social Networking Presentation

Katheleen A. Ehrhart, Partner at Freeborn & Peters LLP

Freeborn & Peters LLP

I. Background: The Increased Access To And Use Of The Internet and High Tech Gadgetry

What Are We Talking About?: Social and Professional Networks

- Facebook
- MySpace
- Twitter
- LinkedIn

The Growing Prevalence Of These Sites

- There are more than 40 million active Facebook users
  - 50% off users log on to Facebook on any given day
  - More than 35 million update their status each day
- LinkedIn has more than 55 million users worldwide– half are in the U.S.
- By some estimates there are 27.3 million tweets a day that go through Twitter

Other Communication Avenues On The Rise

- Blogs
- Text messaging
  - Wireless carriers reported more than 740 billion text messages were sent in the first half of last year.
  - That's 4.1 billion messages a day

Litigation Information Websites

- The use of the internet has even expanded access to information about litigation
  - The federal court Pacer system provides information about every case filed in federal court and provides the ability to download pleadings
  - Approximately 30 states have some sort of similar on line system

The Impact Of This Increased Internet Activity On Employers

Potential Ramifications To Employer From Employee Use Of Internet Sites

- Waste and inefficiencies created by employees spending time on internet
- Potential liability for employees' behavior/statements
- Potential liability from monitoring employees' behavior/statements

Potential Liabilities For Employees' Behavior/Statements

- Discrimination suits
- Harassment/bullying by employee to employee
  - Employees discussing other employees
  - Online relationships between employees
  - Inappropriate comments, photos, videos posted/texted by employees

Potential Liabilities From Monitoring Employees' Behavior/Statements

- Suits claiming violation of Title VII, ADA, etc.
  - Discovery of information on line not otherwise known about employee followed by subsequent adverse employment decision
- Invasion of privacy suits from monitoring internet sites and blogs

General Legal Framework For Employer Monitoring Suits

- While little case law exists dealing with blogging and social networking, prior cases dealing with private communications over company systems provide guidance.
  - Employees using employer's systems and computers and software: generally subject to workplace consequences.
  - Employee using employer's hardware but communicates privately using non-employer approved software or channel employer does not control:
    - Law is mixed.
    - Courts generally try and balance employer's expectation of business efficiency with the employee's expectation of privacy.

Key Case: *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008)

- Involved city employer's decision to obtain and review private non-work related text messages police officers sent over a network of pagers provided by departments.
- Discovered personal, sexually explicit messages.
- Plaintiffs brought claims for invasion of privacy and unlawful search under the Fourth Amendment.

Quon Case: Ninth Circuit held messages were private and employer search was unlawful

- Like a telephone number or address info on a sealed envelope, the "To" and "From" portions of the message were not private.
- But plaintiffs had a reasonable expectation of privacy as to *the contents of the message*.
- City's policy of not auditing messages reinforced this expectation.
- Search was not reasonable in scope– there were less constraining methods that could have been used to determine if messages were work related or not.

The Future of *Quon*

- The U.S. Supreme Court granted certiori in December 2009
- So it appears they are set to weigh in on these issues which could change the legal landscape dramatically.

Messages To Employers From *Quon*

- Employee does not necessarily give up privacy expectations merely by making use of employer's computers, phones, or other devices.

- A message-- and potentially a statement posted on a networking site or blog-- may be protected if the employee can demonstrate an intention to keep the contents private *and* the court views that intention as reasonable.

How Can Information Posted On An Internet Site Possibly Be Considered Private?

- Networking site profiles/blogs have a very personal quality– generally created as an individual's personal account outside work hours on personal computer
  - Employer's computer or system only being used to access the profile.
- Many networking sites offer multiple levels of privacy; user can identify which individuals have or do not have access to certain content
- Sites also may have private chat or messaging functions that not everyone can see

What Is An Employer To Do?: Best Practices

What Is An Employer To Do: Best Practices

1) Adopt a clear policy on internet use.
2) Place employees on notice regarding potential monitoring.
3) Implement planned monitoring; informal actions contrary to policy can undercut policy.
4) Train employees on appropriate use of internet.

Provisions To Consider For Company Internet Use Policy

1) Eliminate employee expectation of privacy using company owned technologies.
2) Provide notice monitoring may occur.
3) Employees should include a disclaimer on their website that they do not speak for the employer, required if they mention employer on the site.
4) Information posted on any site cannot harass or attack another employee, customer, vendor, contractor, employer, affiliate, etc. in any way, particularly based on any protected characteristic.

Provisions To Consider For Company Policy On Internet Use

5) Do not provide company's confidential or proprietary information.
6) Information posted to any site should not violate any company policy, code of conduct.
7) Make clear company respects employees' rights to express personal opinions and does not retaliate or discriminate against employees who post messages for political, organizing or other lawful purposes.
8) Spell out consequences of violation of the policy.

Best Practices: Monitoring Of Employees

- Place employees on notice of monitoring:
  - Include in policy that company reserves the right to monitor comments or discussions about the company, employees, customers, etc. that employees post *anywhere* on the Internet.
  - Inform employees that searches/monitoring will be conducted.
  - Obtain release from employees for running searches.

Best Practices: Monitoring Of Employees

- Actually conduct planned monitoring:
  - Informal policies or conduct that run contrary to formal policy can undercut effectiveness of policy and lend credence to employee claim that he/she had an expectation of privacy.

Best Practices: Training

- Go over internet use policy and ramifications for violation of the policy.
- Identify designated person within company who can answer questions about the policy.
- Key messages for employees:
  - Employees should be aware of their association with the company when posting on sites.
  - Employees should respect their audience.

Best Practices: Training

- Key Messages For Employees:
  - When publishing a blog or making statements, employee should make clear what he/she says is representative only of the employee's views and opinions, not the company's.
  - Be mindful that what is published will be public for a long time.
  - Respect the privacy and opinion of others.
  - There can be consequences for what is published on the internet.

Use Of Networking Sites In Employment Decisions

- There are few restraints on conducting internet searches regarding job applications.
- Risk: prospective employer may learn information it is prohibited from asking about (i.e. age, disability, family, religion) followed by an adverse employment decision.
- To lessen risk, company should consider upfront release from candidates regarding internet searches.