

Tweets & Terminations: Social Media in the Workplace



Presented by:

Thomas M.J. Hathaway

for

MSHPM Webinar

CLARK HILL

Discussion Points

- **Social media in the workplace**
 - Reasons to allow
 - Reasons to prohibit
- **Social media and employment laws**
 - State and Federal laws, rules and regulations
 - Examples of employment decisions and attendant legal risks
- **Best Practices**
 - Social Media policies
- **Questions**



Social Media in the Workplace



CLARK HILL

Social Media in the Workplace

- **54 percent of U.S. companies say they've banned workers from using social networking sites while on the job**
- **19 percent of companies allow social networking use only for business purposes**
- **16 percent of companies allow limited personal use of social networking sites**
- **Only 10 percent of the 1,400 CIOs interviewed said that their companies allow employees full access to social networks during work hours**
- **Consider whether desirable or feasible to limit for business use only**
- **Decision driven by corporate culture and company's objectives and beliefs**

Reasons to Prohibit Access to Social Media

- **Diverts employees' attention away from work priorities**
- **Hurts bottom line.**
 - Employee productivity dropped 1.5 percent in companies that allowed full access to Facebook
 - 77 percent of workers who have a Facebook account use it during work hours.
 - “Some” employees use the social networking site as much as two hours a day at work. It did not say how many workers fit into that category, but did note that one in 33 workers surveyed use Facebook only while at work.
 - And of those using Facebook at work, 87 percent said they had no clear business reason for accessing the network.

Reasons to Allow Access to Social Media

- **Effective business tool**
- **Professional networking**
- **Marketing**
- **Product/service feedback**
- **Greater interactivity between customers and businesses**
- **Employee recruitment**
- **Community outreach**
- **Reach out to masses**

Social Media and Employment Laws



CLARK HILL

Legal Risks for Employers Based on Employee Use of Social Media

- **Employee's direct use of social media**
 - Customer relations
 - Damage to reputation of company
 - Defamation
 - Trade secret disclosure
 - Disclosure of private customer data
 - Harassment claims
 - Tortious interference
 - Fraud
 - Threats
 - First Amendment issues
 - Discovery during litigation
 - Securities issues
 - FTC Guidelines Regarding Testimonials

Legal Risk to Employers Based on Adverse Employment Decisions

- **Employer's employment decisions based on employee's direct use of social media**
 - Off-duty conduct laws
 - Federal and State EEO laws
 - Retaliation
 - Whistleblowers' claims
 - SOX claims
 - National Labor Relations claims
 - Invasion of Privacy
 - Stored Communications Act, Wiretap Act and Electronic Monitoring Statutes

The Challenge for Employers

- Facebook and MySpace less than 7 years old
- No published cases regarding monitoring by employers
- Very few cases addressing employee terminations for content of blogs, Facebook or MySpace postings
- Themes in available decisions: Employer beware! Access of password-protected blogs could lead to liability

Off-Duty Conduct

- **Many states prohibit discipline/discharge for off-duty conduct**
 - Smoking
 - Alcohol
 - Recreational activities
 - Political practices

- **Review State's off-duty conduct laws before discipline/discharge**

Retaliation Claims

- ***Williams v Singing River Hospital System***
 - African-American employee reported a former co-worker who showed her a YouTube video entitled “Fry that Chicken”
 - Alleged race discrimination and retaliation
 - Claim dismissed because adverse action occurred before she complained about video

- ***Navab-Safavi v Broadcasting Board of Governors***
 - Independent contractor sued after contract not renewed
 - Alleged race and national origin discrimination and retaliation
 - Contractor – U.S. citizen born in Iran
 - Terminated after video protesting Iraq war posted on YouTube
 - Court denied motion to dismiss for inability to recover monetary damages under the Bivens test or on the basis of qualified immunity

Public Employers Retaliation and First Amendment Claims

- ***Richerson v Beckon***
 - Retaliation claim for exercising First Amendment rights
 - Posted blog about another District employee
- ***Spanierman v Hughes***
 - Retaliation claim for exercising First Amendment rights
 - Communicated with students through MySpace page
- **Both Cases**
 - Dismissed
 - Different result if posts involve matters of “public concern”

Sarbanes-Oxley Act Claims

- **Protects employees of publicly-traded companies who**
 - Report a violation of a rule or regulation of the Securities and Exchange commission or
 - Report a violation of any federal law relating to fraud against shareholders

Discrimination Based on EEO Laws

- **EEO Laws**
 - Title VII – protects race, color, religion, sex or national origin
 - Elliott-Larsen Civil Rights Act – protects race, color, religion, sex, national origin
 - Americans with Disabilities Act
 - Age Discrimination in Employment Act
 - Some states – sexual orientation
- **Applications**
 - Video resumes
 - EEOC Guidance regarding Electronic Resumes with Video Clips
- ***Marshall v Mayor & Alderman of Savannah*, affirming dismissal of sex discrimination claim by probationary firefighter fired after posting racy photos**
- ***Mai-Trang v Starbucks*, dismissing discrimination claim where employee fired after employee posted threats against company on employee's MySpace page**
- ***Jackson v Planko*, claim dismissed where employer believed employee was a threat to safety of other employees due to support of gun rights and visits to gun websites in violation of policy**

Employee E-Mails with Lawyer on Company Laptop

- ***Stengart v Loving Care Agency Inc*, March 30, 2010**
 - New Jersey Supreme Court
 - Health care service executive who used a company laptop to exchange messages with her attorney on a password protected e-mail account had reasonable expectation of privacy that was violated when her employer retrieved and read the messages from the computer's hard drive.
 - Written policy on computer use “not entirely clear”
 - No mention of personal email accounts like the Yahoo account used
 - “Even a more clearly written company manual” would not have justified company's intrusion into executive's communications with lawyer
 - Rejected employer's argument that it had a right to search company-owned equipment for information about executive after she left the company and accused the firm of unlawful discrimination
 - Company violated right to privacy – Employer's right to review emails has limits and does not trump attorney-client privilege

No Expectation of Privacy Using Employer's Email

- ***Scott v Beth Israel Medical Center*, 2007 NY MISC LEXIS 7114**
 - Breach of employment contract for failure to pay \$14,000,000 severance
 - Employee communicated with his attorney regarding the litigation over the employer's email system
 - Employer's Email policy - no expectation of privacy
 - Court held – Plaintiff's use of employer's email system to communicate with his attorney in violation of email policy rendered any communication NOT made in confidence destroying any attorney-client privilege

Social Media and the National Labor Relations Act

- *Register Guard*, employer's email system is company property and employers are free to enforce "business only" email policies
- *Konop v Hawaiian Airlines*, employees comments on secure website critical of employer, officers and union constituted protected union organizing activity. Ninth Circuit rejected employer's argument that protection lost because comments contained "malicious, defamatory and insulting material known to be false."
- *Endicott Interconnect Techs v NLRB*, employee's postings on a newspapers internet forum protecting layoffs not an unfair labor practice. Employee's comments constituted "a sharp, public, disparaging attacks upon the qualify of the company's product and its business policies" not protected by NLRA.
- Sears Social Media Policy prohibiting "disparagement of company's or competitors' products, services, executive leadership, employees, strategy, and business prospects, held by the NLRB Office of General Counsel could not be reasonably construed to chill Section 7 protected activity

State Causes of Action

- Defamation
- Intentional infliction of emotional distress
- False imprisonment
- Assault
- Invasion of privacy
 - Employee's efforts to privacy
 - Employer's efforts to gain access
- ***Moreno v Hanford Sentinel***, Court rejected invasion of privacy claim of college student who ranted online against her hometown. Ranting republished in a newspaper. Led to family business being run out of town. MySpace rant public and thus could not support a privacy claim.
- ***Yath v Fairview Clinic***, patient brought invasion of privacy claims concerning internet posting of information from the patient's medical file on a MySpace page. Court held wrongful access of patient information not foreseeable and not involve in creating webpage that contained patient information

Federal Limitations on Employer Monitoring of Electronic Communications

- **Electronic Communications Privacy Act 18 USC 2510**
 - A person “may not intentionally . . . intercept any wire, oral or electronic communication”
 - Only covers “interception”
 - Viewing Facebook and MySpace pages likely not “interception”
- **Stored Communications Act 18 USC 2701**
 - Allows employer access to stored communications (voice mail or email) with employee’s consent
 - Protects only communications in which the employee had a reasonable expectation of privacy not those readily accessible to the general public
 - Only protects information contained in “electronic storage”
 - Where employer makes clear that certain communications are not protected or public postings on social media, likely not protected under the SCA

Intellectual Property Issues

- **Trade secrets and confidential information**
 - Employees inadvertently or purposely post trade secrets or other confidential information
 - Eli Lilly & Co.
 - Mark Jen, Google
- **Loss of trade secret protected status and ability to obtain patent protection**
- **Copyright infringement from photos, news articles or music**
- **Trademark issues**

Examples of Employment Decisions with Attendant Risk

Pietrylo v Hillstone Restaurant Group, 2009 U.S. Dist. LEXIS 88702
(D.M.J. Sept., 29, 2009)

- Restaurant employee created MySpace page for fellow employees to “vent” about the restaurant; invitation-only user group with a personal and password protected web page. Posts complained about the restaurant, customers and supervisors. A supervisor obtained a user name and password from a hostess who felt coerced into providing the information. Plaintiff was discharged for violating policy requiring professionalism and a positive attitude.
- Jury awarded \$3,403 plus punitive damages of \$13,612

Examples of Employment Decisions with Attendant Risk

Quon v Arch Wireless, 529 F.3d 892 (9th Cir. 2008), cert granted,
City of Ontario v Quon, U.S. No. 08-1332 (12/14/09)

- Police department paid for and provided cell phones to police officers for use in the course and scope of their employment.
- Arch Wireless provided the service. Text messages were transmitted over their network and backup copies were kept. The City was the subscriber to the services and had a policy of monitoring e-mail and other forms of communication, banning personal use of systems, but not explicitly covering text messaging in the policies.
- The City's computer policy provided that there was no expectation of privacy.
- Claim that there was an informal policy not to monitor unless the employee refused to pay for excessive personal use. Quon paid overage fees for exceeding text messaging limits to avoid auditing for personal messages.
- The City obtained copies of Quon's text messages from Arch Wireless, without employee consent, because it deemed itself a subscriber under the Stored Communications Act.
- The Ninth Circuit found in favor of Quon and that the City violated the Stored Communications Act, the Fourth Amendment and the California constitutional right to privacy.

Examples of Employment Decisions with Attendant Risk

Konop v Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002)

- Company accessed an employee's secure website using other employees' login information (with their permission) even though the site's terms prohibited access by management and prohibited authorized users from allowing others to access the site.
- The website contained vigorous criticisms of the airlines' management and labor concessions. the company disciplined the pilot.
- Court found the airline violated the Stored Communications Act and that an exception to the Act (where permission to view is granted by a "user") did not apply because the authorized employees had not actually "used" the site themselves.

Examples of Employment Decisions with Attendant Risk

Pure Power Boot Camp v Warrior Fitness Boot Camp, 587 F.Supp.2d 548 (S.D.M.I. 2008)

- Employee planned to leave his job to start his own company. When he resigned, his employer was able to access his personal email accounts which he had logged onto while at work, using a password that automatically popped up.
- Company found damaging evidence related to the employee's pre-resignation activities.
- Court found that the company's email policy was not specific enough to put employee on notice that personal email viewed over the company's computers would be accessed by the company. The Court also determined that employees leaving of his password on the computer did not create an implied consent to view his personal email accounts.
- Court ruled the employer's conduct violated the Stored Communications Act and ruled that the damaging emails obtained in violation of federal law could not be used against the employee even though they would have been discoverable in the ordinary course of litigation.

Best Practices and Policies



CLARK HILL

Social Media Policies Are Essential

- **Social media, and the use by employees, customers, vendors and the public, will continue to grow**
- **Social Media policies are essential**
 - 76% of companies have work e-mail policies (2006 Employment Law Alliance Survey)
 - 50% of employers have a formal blog policy in place (2006 American Management Association Survey)
- **Revise email/internet policy or create stand alone social media policy**

Maintain and Regularly Communicate Policy

- **General Information**
 - Must be formal and written
 - Obtain signed acknowledgment of receipt of policy
- **No Expectation of Privacy**
 - Establish that electronic equipment and communications, documents, information is company property
 - Establish that employees should have no expectation of privacy
 - Establish that employee's use of the system indicates their consent to monitoring and waives all privacy rights
 - Establish security measures that employees are expected to observe
 - Specifically preserve the right to monitor and review all messages and content without additional notice

Maintain and Regularly Communicate Policy

- **Prohibited Activities**

- Set limits or prohibit personal use of email, voice mail, instant messaging, blogging, social networking, etc
- Prohibit viewing, downloading or displaying pornographic or offensive material
- Prohibit the viewing, downloading or display of illegal, defamatory material
- Require explicit approval for downloading of games, programs or information
- Prohibit use of computer system to harass, insult or intimidate another
- Require outside files be scanned for viruses before downloading or opening
- Establish that violations of the policy may result in disciplinary action up to and including termination

Maintain and Regularly Communicate Policy

- **Security**
 - Establish security features for the transport and maintenance of electronic equipment outside the workplace
 - Control use of employee equipment which could be used for union organizing, by restricting to business-only purposes

Best Practices Regarding all Electronic Communications Policies

- **Train your employees, contractors, and anyone who uses your IT systems**
- **Do Not Circumvent Access Restrictions**
- **Have non decision-makers screen out information regarding protected status**
- **Know state laws governing privacy and lawful off-duty activity**
 - 31 states currently have lifestyle discrimination laws protecting lawful off-duty activity

Electronic Signatures

- **Electronic signature is legally recognized in Michigan**
 - Uniform Electronic Transactions Act enacted in Michigan. *MCL 450.831*
 - Electronic signature means an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
 - If the law requires a record to be in writing, an electronic record satisfies
 - If the law requires a signature, an electronic signature satisfies
 - An electronic signature is attributable to a person if it is the act of the person as may be shown in any manner, including a showing of the efficacy of any security procedure
 - Programs for creating and reviewing digital signatures

- **Authentication – Safe Guards**
 - I am the person whose signature appears below
 - I have reviewed the policy
 - I understand the policy
 - I agree to its terms

Thank You



Thomas MJ Hathaway
thathaway@clarkhill.com
(313-965-8233)

Note

This document is not intended to give legal advice. It is comprised of general information. Employers facing specific issues should seek the assistance of an attorney