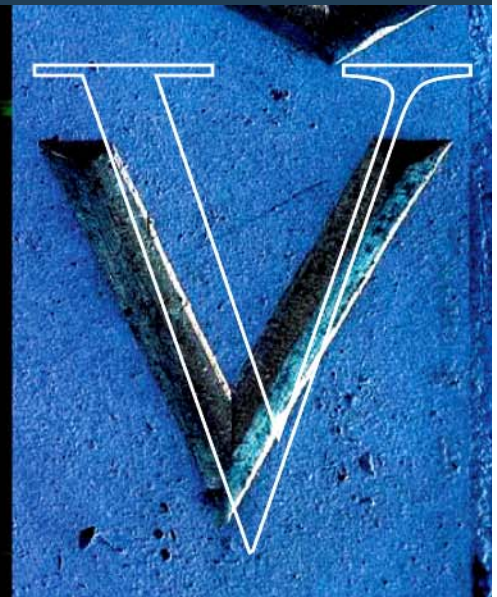
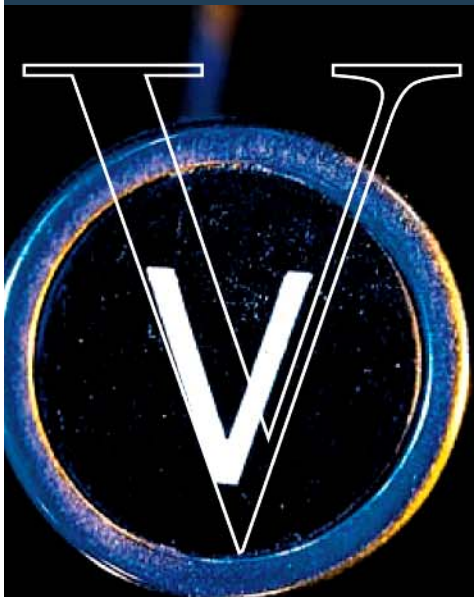


# VENABLE<sup>®</sup><sub>LLP</sub>

## Social Networking from 9-5: Unique Challenges Facing Employers

by James E. Fagan and Luisa M. Lopez

September 16, 2010



## Seminar Overview

- Tools of the Trade
- Why employees use social media
- Why you should be concerned that employees use social media
- Best practices for drafting and implementing a social media policy
- Questions



## Where are *your* employees these days?

- **Tools of the Trade** (i.e. Facebook, LinkedIn, Twitter, MySpace, Friendster, Skype, YouTube, Blogs, Instant Messaging, etc.)



## Increased popularity and users

- LinkedIn has over 65 million users
- Facebook has over 500 million users
- Twitter has about 106 million users (sending 55 million tweets daily)



## Did you know?

According to a 2009 survey conducted by Deloitte:

- 55% of employees admit to visiting social networking sites during work hours.
- 74% of managers surveyed believe social networking sites put the firms and their brand at risk.



## Did you know?

- 15% consider the risks of social networking sites at the boardroom level, but only 17% have risk mitigation policies or programs in place.
- 60% of managers believe they have the “right to know” what their employees are saying about the company on the employees’ personal (and private) social networking web pages.



## Why do you Need a Social Media Policy?

- Prevent loss of productivity
- Permit effective monitoring (compliance with laws)
- Protect the reputation and image of your company
- Protect against loss of confidential information and trade secrets
- Guard against suits for invasion of privacy, defamation, improper recruiting and improper discipline and termination
- Protection against discrimination, harassment and cyber-bullying



## Specific Areas Of Concern

- Apparent Authority
- Privacy
- Defamation and False information
- Confidential information and trade secrets
- Harassment and Discrimination
- Compliance with related state and federal laws
- Employer liability for criminal conduct
- Labor Law
- Ethics



## General Overview of an Effective Social Media Policy

- Must be clear and company specific
- Must be consistent with other company policies and procedures
  - Anti-discrimination
  - Anti-harassment
  - Computer, Internet, Email Systems
  - Employee Privacy
  - Confidentiality and Trade Secrets
  - References



## General Overview of an Effective Social Media Policy

- Focus on what can and cannot be done – i.e., the do's and don'ts
  - Can an employee access and use social media at work?
  - What are the restrictions on that access and usage?



## General Overview of an Effective Social Media Policy

- Monitoring
  - ***Give Notice***
  - Both on and off duty?
  - No legal obligation to monitor, but may want to monitor to address:
    - Loss of confidential information
    - Cyber-bullying, stalking
    - Discrimination and harassment
    - To better comply with legal restrictions such as wiretapping laws and the NLRA
    - Prevent defamation and improper recruiting and recommendations



## General Overview of an Effective Social Media Policy

- Include mandatory training
- Assign a compliance officer and a compliance framework
- Create a reporting procedure



## Limiting Apparent Authority and Protecting Corporate Identity

- The policy should make clear that employees may not:
  - Use the company’s name in the online identity (e.g. username, “handle”, or screen name)
  - Claim or imply authorization to speak as a company representative (i.e. blogs, comments)
  - Use the company’s intellectual property, logos, trademarks, and copyrights in any manner
  - Identify a client or co-worker in an online posting



## Reducing the Expectation Of Privacy

- The First Amendment does NOT protect an employee from being monitored, disciplined or terminated for violating a clear and reasonable social media policy
- Employees have NO absolute Constitutional right to privacy in the workplace (4<sup>th</sup> Amendment on searches and seizures does not apply)
- *But* you need a clear and reasonable policy that sets out expectations and restrictions on usage



## Reducing the Expectation Of Privacy

- Policy should reduce any expectation of privacy on the company's computers, email systems, blackberry, telephone/voicemail systems and any of the data on these systems by:
  - Making sure employees know that certain information exchanged on social networking sites can be monitored and accessed by the company
  - Expressly stating: no expectation of privacy, even with personal use and when telecommuting
  - Reserving right to remove content without notice
  - Reminding employees about privacy settings



## Potential Privacy Pitfalls

- **Make sure that policy complies with these associated laws:**
  - **Electronic Communications Privacy Act** (Wiretap – consent and business exceptions)
  - **Stored Communications Act** (improper access of electronically stored information)
  - **Federal Trade Commission Guidelines** (false advertising and misleading sales pitches)
  - **NLRA** (section 7 rights of employees for concerted activity)



## Potential Privacy Pitfalls

- **Some states have specific restrictions on monitoring and/or use of information**
- **A particular issue arises when monitoring and/or compliance is associated with off-duty conduct**
  - For example, posting information on Facebook from home account over the weekend
  - Policy needs to describe employer's interest in monitoring and regulating off-duty conduct if it presents a conflict of interest and is reasonably related to the job



# Prohibiting False And Disparaging Information

- ***Defamation/Disparagement***
  - Employees engaging in social networking and blogging for either personal or professional reasons **may not**:
    - Write about, post pictures of, or otherwise refer to any employee, vendor, supplier, business partner, or competitor without his or her permission (i.e. **Michigan nurse**)
    - Give a professional reference to a co-worker, former co-worker, client, vendor, customer or any other individual or company without first contacting human resources or appropriate company official (i.e. **Recommendations on Social Media**)



## Protecting your Company's Reputation

### What were they thinking? Real life examples

- **Dominos Pizza's YouTube Disaster**
- **KFC sinks with MySpace bath tub photos**
- **The Virgin Atlantic Airlines Facegroup**
  - 13 cabin crew members fired after sharing candid impressions of their employer and Virgin's airplanes
  - Insulting Virgin Atlantic passengers on Facebook
- **The Delta Airlines, Inc. Blog**
  - From "Queen of Sky: Diary of a Dysfunctional Flight Attendant" to "Diary of a Fired Flight Attendant."
  - "Racy" photos and commentary on blog



## Protecting Confidential Information And Trade Secrets

- Policy should prohibit employees from disclosing:
  - Clients, customers, partners, or suppliers by name
  - Company's confidential information and trade secrets
  - Information regarding company's clients, affiliates, partnerships
  - Policy should dovetail with any restrictive covenant language in employment agreements or handbook



## Preventing Unlawful Harassment And Discrimination

- Policy should emphasize that employees may not:
  - Post material that is abusive, offensive, insulting, humiliating, obscene, profane or otherwise inappropriate regarding the company, its employees, vendors, supplies, business partners, competitors, etc.
  - Post material that ***may be construed*** as discrimination or harassment based on race, ethnicity, color, national origin, religion, sex, sexual orientation, age, disability, or any other legally protected characteristic.



## Labor Law Concerns

- The NLRA applies to all employers
- Employees have § 7 rights to concerted activity
  - i.e., they can get together to discuss workplace activity related to their interests as employees
- NLRB opinion in SEARS case upheld social media policy that clearly defined prohibited activity because most of it did not interfere with protected activity



## Labor Law Concerns

- Permitted policy in SEARS case included prohibitions on:
  - Dissemination of company confidential information
  - Explicit sexual references
  - Obscenity or profanity
  - Reference to illegal drugs
  - *Disparagement of company products, executives, services, company leadership, business prospects, etc.*



## Preventing Liability For Criminal Conduct

- Cyber-stalking
- Cyber-bullying
- Sexting
- State laws and Federal laws that address computer usage and harassment such as Hate Crimes



## Ethical Concerns

- Violation of industry standards or licensure issues; e.g., medical, financial or legal worlds
- Violation of the attorney-client or work product privileges
- Unauthorized practice of law or medicine



# Social Media Recruiting and Hiring Considerations

## Hiring Practices

- Screen candidates in uniform manner
- Get written consent from job applicants
- Use Neutral Third Party to filter protected information (non-decision maker)
- Still need a legitimate, non-discriminatory reason for employment decision based on information found on social media



## Summary of Best Practices

- **Social Media is a useful but dangerous employment reality**
- **Employers need a clear and reasonable policy**
- **Notice to Employees with express or implied consent to monitoring and consequences**
- **Training of all employees**
- **Clear handling of enforcement, reporting and compliance issues**
- **Alignment of policy with all relevant policies and practices from recruitment to termination**



# Questions?



## Contact and next seminar information

### YOUR VENABLE TEAM

James E. Fagan, III Esq.  
jefagan@venable.com  
t 703-760-1656  
f 703-821-8949

Luisa M. Lopez, Esq.  
lmlopez@venable.com  
t 202.344.4506  
f 202.344.8300

Next M.E.E.T.S. Monthly Third Thursday  
Thursday October 21, 2010

*Highlights of Recent Supreme Court Decisions and  
Legislative Update on the Eve of Mid-term Elections*

[www.Venable.com](http://www.Venable.com)

