

# **Facebook, MySpace, Twitter, oh my! Regulating the Workplace in the World of Web 2.0**

*by  
Susan Keating Anderson*

In this day and age of Facebook, MySpace, Twitter, blogs, online forums, chatrooms and the global, technological interconnectivity of individuals, it seems very little, information is off-limits to anyone with access to the internet. From the perspective of an employer that is seeking background information on applicants for employment or looking to monitor its employees' compliance with workplace policies and/or restrictive covenants, the nearly-unfettered access provided by the internet is great, right? While it is true that employers now have much more access to information that could prove valuable to business operations, employers must be careful in the methods they employ to gain access to such information and the scope of the information targeted or, as may be the case, inadvertently disclosed.

## **I. Why should an employer care about social media?**

- A. Unless you have sequestered yourself from society, you are likely aware of the increasing prevalence of social media in the marketplace: Facebook, MySpace, and Twitter are probably the most widely recognized social media vehicles, but there are also countless number of online forums, chatrooms, and weblogs through which your employees may be communicating.
- B. In fact, social media has overtaken email as the most popular electronic method of communication.
  - 1. According to a Nielsen study, in 2009, U.S. Internet users spent about 16% of their time on social networking websites and about 12% of their time emailing. In 2010, internet users spent 23% of their internet time on social media sites and only 8% of their time emailing.
  - 2. Facebook now has 500 million users; on average, users of Facebook spend six hours a month on the site.
- C. Social media isn't just for kids anymore.
  - 1. Nielsen found that the number of Americans aged 50 or above are visiting social media sites is double that of the 18 years or younger group.
- D. Access is becoming easier.
  - 1. Americans are increasingly accessing email and social media sites through PDA and other smartphone devices.

## **II. What is a blog, anyway?**

- A. A blog is the fusion of the term “web log” which refers to a personal journal posted on the Internet.
- B. Usually open to public; third-parties can post comments.
- C. Can update users instantly through RSS feeds.
- D. Can link to other sources.
- E. According to Pew Internet & American Life, over 12 million Americans keep blogs and over 57 million read them.
- F. Purposes of blogs
  - 1. Publish ideas and content
  - 2. Build community
  - 3. Serve as experts/thought leaders in field
- G. Profile of a blogger
  - 1. 54% male compared to 46% female
  - 2. 54% under the age of 30
  - 3. 39% have a college/graduate degree
  - 4. 42% earn more than 50k annually
  - 5. 83% blog from home
  - 6. 75 blog from work

## **III. Pitfalls and concerns associated with social media use in the employment context.**

- A. Employers are increasingly turning to the internet for reasons such as:
  - 1. Background Checks for Applicants
  - 2. Monitoring Employee Use of Technology
  - 3. Monitoring Off-Duty Employee Conduct

4. Preventing Improper Endorsements
  5. Other Important Considerations
- B. Background checks
1. In a survey of 100 hiring managers at small, midsize and large companies, 75% use LinkedIn, 48% use Facebook, and 26% used Twitter to research candidates before making a job offer.
  2. While internet searches can be a useful tool for employers, employers must tread carefully if using the internet to perform background checks on prospective employees.
  3. The internet may contain a lot of information that is relevant to hiring decisions, but it also likely contains information that could form the basis of a challenge to a hiring decision (ie, a failure to hire claim).
  4. There are numerous federal and state laws that prohibit discrimination in employment decisions.
    - a. **Chapter 4112 of the Ohio Revised Code** prohibits discrimination on the basis of race, color, religion, sex, military status, national origin, disability, age, or ancestry of any person. An employer is prohibited from considering membership in these protected classes of an employee or applicant in any decision “to discharge without just cause, to refuse to hire, or otherwise to discriminate against that person with respect to hire, tenure, terms, conditions, or privileges of employment, or any matter directly or indirectly related to employment.
    - b. **Title VII of the Civil Rights Act of 1964** (“Title VII”) prohibits discrimination on the basis of race, color, religion, national origin, or sex.
    - c. **The Pregnancy Discrimination Act** amended Title VII to make it illegal to discriminate against a woman because of pregnancy, childbirth, or a medical condition related to either.
    - d. **The Age Discrimination in Employment Act of 1967** (“ADEA”) prohibits discrimination on the basis of age.
    - e. The **Americans with Disabilities Act of 1990** (“ADA”) prohibits discrimination against a qualified person with a disability.

- f. The **Genetic Information Nondiscrimination Act of 2008** (“GINA”) makes it illegal to discriminate against an employee or applicant because of their genetic information.
  5. It can be very easy to discover information protected by law when doing an online background check on an applicant. If information of this nature is discovered, and *even if it is not considered in the hiring decision*, the applicant has fodder to argue that the hiring decision was motivated by a discriminatory motive. Suddenly, you could be facing a failure to hire claim even if you did not use protected information in your hiring decision.
  6. Moreover, many sites may contain inaccurate information and/or information that can be easily confused as being associated with the applicant, i.e., John Doe of Cleveland, when it is actually associated with someone else, i.e., John Doe of Toledo.
- C. How to be careful when performing online background checks
1. In order to protect your company (and you, as Ohio law allows an individual supervisor to be sued personally for his or her discriminatory acts) certain safeguards should be implemented with respect to background checks, such as:
    - a. Get the consent of the applicant;
    - b. Have written policies that dictate the protocol to be used for the search;
    - c. Train the personnel who will be conducting the search on the protocol to be used;
    - d. Screen in a uniform manner – both by applicants and sites searched;
    - e. Use a non-decision maker to conduct the search;
    - f. Do not “friend” applicants on Facebook, MySpace, etc.; and
    - g. Base decision on only legitimate, non-discriminatory reasons.
  2. Note that if an employer hires a third-party to conduct the background check, certain notice and procedural rights are provided to applicants under the **Fair Credit Reporting Act** (“FCRA”). As the law presently stands, the FCRA generally doesn’t

cover information that would likely be found on social media sites; however, future legislative revisions to the FCRA could do so.

D. Monitoring Employee Use of Technology

1. Privacy Issues

a. Personal internet use by employees on the job is virtually inevitable. While it would be very difficult to enforce a complete ban on such use, employers should have policies in place addressing the parameters of such use and providing notice to the employee that the employer may and will monitor employees' use of the internet. Absent adequate policies, employers expose themselves to liability for an invasion of privacy claim.

2. Ohio law: Invasion of privacy tort claim

a. In *Housh v. Peth*, the Ohio Supreme Court established the **tort of invasion of privacy** as including "the wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities." 165 Ohio St. 35, par. 2 of the syllabus. This tort has been used by employees to bring invasion of privacy claims against their employers for things like accessing an emails sent through or held in a business email account, monitoring employee internet usage, and accessing employee blogs and social media postings.

b. Evidence that an employer informed the employee of its intent to monitor such activities helps defeat the contention that an employee had a reasonable expectation of privacy in his or her workplace internet use.

3. Privacy under the 4<sup>th</sup> Amendment to the United States Constitution

a. The U.S. Supreme Court recently addressed an employee's **reasonable expectation of privacy** under the 4th Amendment of the U.S. Constitution in text messages sent on employer-owned pagers in *City of Ontario v. Quon*.

b. The Court held that a Police Department's search of a police officer's text messages on a city-issued pager did not violate the police officer's Constitutional rights under the Fourth Amendment, which guarantees freedom from unreasonable searches and seizures.

- c. In *Quon*, the Police Department performed an audit of the police officer's text messages to determine whether police officers were exceeding their monthly usage of text messages for work-related or personal reasons. The Police Department's audit revealed that Quon was sending and receiving sexually explicit text messages while on duty and concluded that Quon violated the City's "Computer Usage, Internet and E-Mail Policy."
- d. In reaching its conclusion, the Court assumed that Quon had a **reasonable expectation of privacy** in his text messages and reasoned that because the City's search was "justified at its inception" and was not "excessively intrusive" the search was "reasonable under the circumstances" in both the government-employer and private-employer context.
- e. The Court was careful to draw a distinction between text messages and e-mails, seemingly inferring that employees may have a greater expectation of privacy in text messages than e-mails (i.e. e-mails, unlike text messages, are sent and received on an employer's server).
- f. Nonetheless, employers should consider revising any current policies regulating computer, internet and e-mail usage to include language notifying an employee that text messages sent and received on company-issued devices (e.g. Blackberry, iPhone, and other PDAs) are also included in the company's usage policy and are subject to work-related audits.
- g. An employer should also keep in mind that any search of an employee's text messages must be for a "legitimate work-related purpose".

#### E. Social Media

1. Approximately 25% of employees admit to visiting social media during work hours, approximately 10% of employers have terminated an employee for the content of their postings to a social networking site, and approximately 50% of employers now block Facebook, MySpace and Twitter.
2. Employers have the right to monitor and restrict employee use of social networking sites but they should have written policies in place to do so.
3. These policies should include provisions that:

- a. prohibit employer-related information of any kind (logos, business email address, etc.);
  - b. require disclaimers that the content of the site is the personal viewpoint of the employee;
  - c. protect confidential business information; and
  - d. inform employees that discipline can result.
4. Employers also must remember to tie in the social networking/social media policies to other policies including harassment/discrimination and acceptable use policies. Further, current acceptable use policies are likely out of date in light of the emerging technology and will need updated.

F. Employee texting

1. It is estimated that 4.1 billion text messages are sent each day in the U.S. – and not all of them are nice.
2. To address harassment by text or cyberspace, 46 states have enacted laws against cyberstalking.
  - a. Ohio law is among those states – **Section 2917.21 of the Ohio Revised Code prohibits telecommunications harassment.**
3. The law regarding what constitutes sexual harassment or other unlawful discriminatory conduct has not changed. However, the methods for making such inappropriate communications (texting, social networking sites) have changed.
4. Thus, employer must implement clear written policies that limit employee texting to matters of business necessity.
5. Some employers have chosen to ban texting altogether and prevent that service from being available on business-owned cell phones.
6. Employers must also institute procedures that enable the storage and retention of text messages from company-provided phones. In cases of sexual harassment, such messages constitute “electronic messages” that are considered evidence in harassment cases, and must be retained by the employer to support or refute the charge.

7. Employers must also communicate to its employees that inappropriate text messages are no different from inappropriate face-to-face comments.
  - a. Texting has the immediacy of a casual, spoken word but the permanency of an indelible document.
  - b. Employees understand the first. They don't always understand the second.
  - c. The permanency of text messages make textual harassment cases much easier to prove than cases based upon conversations or conduct.
8. Texting while driving is also an issue that exposes an employer to potential liability.
  - a. While Ohio does not yet ban texting, many municipalities, including Cleveland, do.
  - b. Employers should amend its existing acceptable use/technology-related policies to explicitly ban work-related texting while driving.
  - c. Otherwise, employers may face liability if an employee causes an accident while engaging in work-related texting.

G. Monitoring employee off-duty conduct

1. In addition to keeping track of what employees are doing during business time and with business-owned computers, phones, PDAs, and other property, employers are increasingly monitoring an employees' off-duty conduct through the use of social media.
2. There are certainly some legitimate reasons for an employer to want to do so. There have been widely-publicized cases of employees calling off work only to be found later through social media at parties, on a boat, or engaging in other such recreational activities during the hours in which the employees should have been at work.
3. Recently, the Facebook and MySpace postings of a police officer in New York resulted in the dismissal of charges against a criminal defendant.
  - a. At the criminal trial, evidence was presented that a few weeks before trial, the police officer's "mood" was identified as "devious" on his MySpace page.

- b. There was also evidence that the police officer's Facebook status had been identified as "watching Training Day to brush up on proper police procedure." Training Day is a movie that centers around the actions of a corrupt narcotics detective.
4. There are a plethora of legal implications when an employer seeks to monitor or access an employees' off duty technology use.
- a. As discussed above, such conduct by an employer can implicate an employee's right to privacy and, in the public sector, his or her constitutional rights to be free from unreasonable searches and seizures.
  - b. In addition, the **Federal Electronic Communications Privacy Act** ("ECPA") prohibits the unauthorized interception of wire, oral or electronic communication. 18 U.S.C. sec 2510 et seq.
    - i. Employers can defend against such claims under ECPA's consent or business extension exception.
  - c. Under the **Stored Communications Act**, it is illegal to "intentionally access a facility through which an electronic communication service is provided...and thereby obtain...access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. sec 2701-2711.
    - i. Similar to the ECPA, the SCA contains an exception from potential liability if the conduct if there is consent by the person using the service with respect.
    - ii. In a case decided in May 2010, a federal court issued an opinion that addressed social media sites in the context of the SCA. The Court held that some, but not necessarily all, of the content on such sites may be protected by the SCA. *Crispin v. Christian Audigier Inc.*, 2010 U.S. Dist. LEXIS 52832 (C.D. Calif. May 26, 2010).

#### H. Preventing improper endorsements

- 1. Recent revisions to the **FTC Endorsement and Testimonial Guides** ("Guides"), effective December 1, 2009, specifically address endorsements and testimonials in the social media world, including as they relate to employee endorsements.

- a. In the revised Guides and for purposes of this outline, the term “endorsement” refers to both endorsements and testimonials and is defined as “any advertising message...that consumers are likely to believe reflects the opinions, beliefs, findings or experiences of a party other than the sponsoring advertiser.”
2. The Guides set forth general principles and include examples of the application of those principles in varying scenarios. Overall, the Guides reflect three fundamental advertising principles:
  - a. Endorsements must be truthful and not misleading;
  - b. If the advertiser doesn’t have proof that the endorser’s experience represents what consumers will achieve by using the product, the advertisement must clearly and conspicuously disclose the generally expected results in the depicted circumstances; and
  - c. If there is a connection between the endorser and the marketer of the product that would affect how people evaluate the endorsement, it should be disclosed.
3. Employee endorsements
  - a. With respect to employee endorsements on blogs, message boards, and other websites, whether operated by the advertiser or not, such endorsements must clearly and conspicuously disclose the employee’s relationship to the members or readers of the sites.
  - b. The Guides recommend that any discussion by an employee endorsing his or her employer’s products or services on personal blogs, Facebook pages, or Twitter be accompanied by a disclosure that identifies the author’s relationship with the employer.
4. Company-operated social media networks
  - a. A company that operates a social media marketing network must have reasonable programs in place to train and monitor members of the network. The FTC recommends the following as core elements to such programs: an explanation to members of the parameters of permissible and impermissible product claims; a reasonable monitoring program; and follow-up on questionable practices.

5. Employer liability

- a. The Guides specify that advertisers are subject to liability for FTC violations arising from false or unsubstantiated statements made through endorsements.
- b. Advertisers are also subject to liability for failing to disclose material connections between the advertiser and endorser. Endorsers may also be subject to liability for their own statements, though the FTC has stressed that its enforcement efforts is focused upon the advertisers, not bloggers or other endorsers.
- c. Though many such endorsements can occur on personal blogs and webpages not operated or associated with the employer, an employer can still be held responsible for endorsements that violate the Guides.
- d. In gauging employer liability for noncompliance in such instances, the FTC will consider whether the employer has appropriate policies and internal procedures in place to address such conduct. The Guides do not prescribe specific requirements for such policies or procedures.

**IV. Other Important Considerations**

A. Fair Labor Standards Act Issues

1. Under the FLSA, nonexempt employees could be entitled to wages and overtime for time spent reviewing and responding to text messages, emails and other communications received through company-issued PDAs.

B. Social Media User and/or Term of Service Agreements

1. Employers must be aware that terms of service and/or user agreements for social media sites such as Facebook often contain prohibitions against the solicitation and use of login information by someone other than the owner of the account.
2. Likewise, most prohibit the accessing of an account that belongs to another person. Thus, even if an employer seeks and obtains the consent of an applicant or employee to access his or her Facebook page, an employer or the applicant could find itself in legal hot water for doing so in violation of the contractual terms of the sites.

- C. Trade secret and disparagement issues
  - 1. Increased employee use of social media sites may result in publication of confidential information or public, disparaging comments about employers, supervisors and co-workers.
  - 2. Employers must make sure that existing computer use, confidential and proprietary information, and anti-harassment policies specifically address social media and advise employees that if they use the company's e-mail address or name they must act in accordance with the company's professional standards.
  
- D. Monitoring for Breach of Restrictive Covenants
  - 1. Social media sites, particularly those related to business networking such as LinkedIn, can prove to be useful to determine if a current or former employee has or are breaching covenants not-to-compete or confidentiality restrictions. However, an employer must be careful not to engage in “pretexting” (posing as someone else) or other misleading investigation techniques to gain access to such sites.
  
- E. Online recommendations of employees
  - 1. Employers need to realize that an online recommendation on sites such as LinkedIn are no different than a formal written recommendation letter, and actually could be worse given the perpetuity of information available on the internet. If an employer gives a glowing, inaccurate recommendation of an employee, it may be used against the employer in a discrimination suit. For instance, an employee fired for performance reasons may point to LinkedIn recommendation by his supervisor as evidence that he was performing well.

#### QUESTIONS?

Susan Keating Anderson  
Walter & Haverfield LLP  
sanderson@walterhav.com  
216-928-2936