

# **Social Media Everywhere – What Everyone Should Know**

**Strategic Solutions for Solo & Small Firms  
August 2011**

**Prepared and Presented by:  
Leonard B. Segal  
Oberman Thompson & Segal, LLC  
120 South Sixth Street, Suite 850  
Minneapolis, MN 55402  
(612) 217-6442  
lsegal@otslawyers.com**

**\*THESE MATERIALS ARE PROVIDED FOR EDUCATIONAL AND INFORMATIONAL PURPOSES ONLY. THEY ARE NOT INTENDED TO CONSTITUTE LEGAL ADVICE IN ANY PARTICULAR SITUATION.**

**TABLE OF CONTENTS**

**INTRODUCTION**.....1

**1. Applicant Screening**.....1

**A. To Peek or Not to Peek** .....1

**B. Transparency**.....2

**C. Legal Concerns in Hiring** .....2

**2. Legal Concerns When Disciplining or Terminating an Employee**.....3

**A. The National Labor Relations Act: Protected Concerted Activity**.....3

**B. Retaliation/Whistleblower Protection** .....4

**3. Drafting a Social Media Policy** .....4

**A. Employers Should Have a Written Policy** .....4

**B. Training & Education**.....5

**4. Electronic Discovery of Social Media Information**.....5

**5. Legal Ethics and Lawyers Using Social Media** .....6

**A. MRPC 1.6: Client Confidentiality** .....6

**B. MRPC 4.1: Truthfulness in Statements to Others** .....7

**C. MRPC 5.5: Unauthorized Practice of Law; Multijurisdictional Practice of Law**.....7

**D. Inadvertent Formation of Attorney-Client Relationship** .....7

**E. Attorney Investigations**.....8

**CONCLUSION** .....8

## INTRODUCTION

The use of social media has exploded in recent years, bringing with it a variety of challenges for employers ranging from whether to use social media when considering a potential new hire to whether to terminate an employee for negative social media postings. Certainly employers have legitimate business concerns when it comes to social media. For example, they want to protect their confidential information, not offend actual or potential customers, avoid negative publicity, and not violate somebody else's intellectual property rights. Those concerns need to be balanced, however, against the rights of employees. Where the line is, and what employers can and cannot do, is just beginning to develop.<sup>1</sup>

### 1. Applicant Screening

Employers increasingly are scouring the Internet for information about applicants that they can use to make hiring decisions. In a 2009 survey from CareerBuilder.com, 45% of employers used social media sites to research applicants, and another 11% planned to start doing so. <http://www.careerbuilder.com/Article/CB-1337-Interview-Tips-More-Employers-Screening-Candidates-via-Social-Networking-Sites/>. Of those hiring managers who have screened applicants using social networking profiles, 34% have used such content to reject applicants. Many employers were more concerned about the appearance of applicants' private lives and personal beliefs than they were about professional skills, and many were more likely to reject applicants who reported their drinking or drug use than applicants with poor communication skills.

[http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr459&sd=9%2f10%2f2008&ed=12%2f31%2f2008&siteid=cbpr&sc\\_cmp1=cb\\_pr459](http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr459&sd=9%2f10%2f2008&ed=12%2f31%2f2008&siteid=cbpr&sc_cmp1=cb_pr459).

#### A. To Peek or Not to Peek

Social media postings can reveal a lot of information about an individual. Many employers believe that with access to that information, they will be better equipped to determine whether an applicant is a "good fit" for the employer. The risk, of course, is that employers may use such private information to make judgments about an applicant that are stereotypical, unfair and potentially illegal.

Before reviewing social media sites as part of their applicant screening process, employers need to decide whether such a review makes sense at all from a legal, risk, and company culture standpoint. If it does, employers should identify exactly what information they are looking for, what information they will ignore, and how the information will be gathered and screened. One way to "ignore" information is to have the person conducting the background check not be involved in the employment selection process itself, with only certain information forwarded from the investigator to the decision makers. For example, an employer may decide that it wants the hiring decision makers to know about applicants who profess that they use

---

<sup>1</sup> This article focuses on the private employment context. There are a number of special considerations that public employers must address.

illegal drugs, who post discriminatory remarks, or who disclose their current employer's confidential information, but not information about those who have tattoos or a spouse of a different race. In deciding what information to review in the hiring process, employers should not forget about positive attributes of job applicants, such as participation in community or charitable activities. Those activities may not be highlighted or included on resumes.

## **B. Transparency**

Employers who seek information about job applicants on social networking sites should obtain that information honestly. They should not "hack" into someone's account or require applicants to disclose their passwords. Similarly, employers should not surreptitiously attempt to obtain access to information that the applicant has limited to friends by getting the information from an applicant's friend or by misleading the applicant about the real reason for seeking such access.

## **C. Legal Concerns in Hiring**

Obtaining information about applicants on social media sites exposes employers to many potential legal claims. For example:

### **1. Discrimination**

A search of social media sites may reveal information about an individual's race, religion, sexual orientation, marital status, national origin, age, veteran status, or other protected class status - information that employer's cannot consider when making a hiring decision. Even if an employer did not actually base a hiring decision on an applicant's protected class status, simply having that information exposes an employer to a potential lawsuit which it will then have to defend.

In addition to Title VII, the Age Discrimination in Employment Act, the Americans with Disabilities Act, the Minnesota Human Rights Act, and other well known anti-discrimination statutes, other laws may also be implicated. For example, the Genetic Information Nondiscrimination Act of 2008 ("GINA") prohibits employers from acquiring genetic information. 42 U.S.C. § 2000ff *et seq.*; 29 C.F.R. § 1635. GINA defines genetic information broadly to include, among others, information about the manifestation of a disease or disorder in an individual's family members, i.e., family medical history. It is not difficult to envision Facebook postings describing a parent's battle with Alzheimer's disease or an applicant's fundraising efforts for a cancer cure in memory of a parent. Although the definition of genetic information has an exception for "commercially and publicly available information," it is not clear that information on social networking sites fall within this exception. Employers become vulnerable to a lawsuit if they acquire such information as part of their background investigation and then fail to hire the applicant.

### **2. Off Duty Conduct Laws**

Many states have laws limiting an employer's right to regulate the off duty conduct or activities of employees. Minnesota, for example, prohibits employers from refusing to hire a job

applicant and from disciplining or discharging employees who engage in the use or enjoyment of lawful consumable products (including alcohol and tobacco) off premises during nonworking hours. Minn. Stat. § 181.938. If an employer sees a Facebook posting of an applicant smoking and drinking, and that applicant is rejected, the applicant may have a claim under Minnesota law. Other states have enacted broader laws to protect employees in their off-duty activities.

## **2. Legal Concerns When Disciplining or Terminating an Employee**

More and more employers are monitoring postings by their employees on blogs and social media sites. Even those employers who do not actively monitor such postings often learn of an employee's postings from other employees, friends, or customers. The instinct of many employers when an employee posts negative comments about the employer is to terminate the employee. Such employers would be wise, however, to take a step back and analyze the situation before making a decision. In addition to the legal concerns discussed above in the hiring context, a number of other protections may exist for employees.

### **A. The National Labor Relations Act: Protected Concerted Activity**

Social media postings may be protected by the National Labor Relations Act ("NLRA").<sup>2</sup> Among others, the NLRA protects the rights of employees to organize or form a union and to "engage in other concerted activities for the purpose of mutual aid and protection." 29 U.S.C. §§ 157-158. If an employee's posting was for the purpose of organizing a union or concerned a dispute between employees and the employer, then any discipline imposed on the employee could arguably be an unfair labor practice.

The National Labor Relations Board ("NLRB") has begun filing complaints against employers who have disciplined employees based on social media postings. The theory behind such complaints is that such discipline violates employees' rights to engage in protected concerted activity. Taken a step further, the concern is that employers' social media policies – including discipline and termination for social media postings – tends to chill employees in the exercise of their rights to discuss wages, working conditions and unionization. See <http://www.nytimes.com/2010/11/09/business/09facebook.html>.

In one recent case that generated quite a bit of media attention, the NLRB filed a complaint against American Medical Response ("AMR") alleging that AMR violated the NLRA by disciplining an employee for violating AMR's social media policy, which barred employees from depicting the company "in any way" on Facebook or other social media sites. The NLRB complaint alleged that AMR's Facebook rule was overbroad and improperly limited employees' rights to discuss working conditions among themselves. The NLRB also objected to another AMR policy prohibiting employees from making "disparaging" or "discriminatory" comments when discussing the company or the employee's superiors and co-workers.

AMR responded that it discharged the employee based upon multiple, serious complaints about her behavior. The employee's Facebook comment stated: "love how the company allows a

---

<sup>2</sup> Non-union employers often assume that the NLRA does not apply to them. That is an incorrect assumption, as the NLRA protects both union and non-union employees.

17 [lingo for a psychiatric patient] to become a supervisor.” The NLRB’s position was that the employee’s comment drew supportive responses from her coworkers and further discussion and negative commentary about the supervisor. The NLRB argued that she had a right to criticize her employer with coworkers using her own computer and on her own time. The AMR case was settled and no decision was issued.

Whether, or when, a social media posting will constitute protected concerted activity is not yet well defined. Employers should exercise caution when drafting their social media policy and when terminating or disciplining an employee based on Internet postings.

### **B. Retaliation/Whistleblower Protection**

It is also unlawful for employers to retaliate against an employee for opposing unlawful discrimination or for reporting to an employer or governmental agency, in good faith, an actual or suspected violation of law. *See e.g.*, 42 U.S.C. §2000e-3(a), Minn. Stat. §363A.15, Minn. Stat. §181.932, Subd. 1. If an employee opposes a discriminatory practice on a social media site, any adverse action against the employee could result in a retaliation claim. While a whistleblower claim may be more difficult, since generally a report must be made to the employer or a governmental agency, it is certainly not out of the question that such a claim could be brought, especially when company management receives the post or is monitoring such posts.

## **3. Drafting a Social Media Policy**

### **A. Employers Should Have a Written Policy**

Employers should have a social media policy that sets forth its position with regard to social media. Without a well written policy, consistent, fair and nondiscriminatory enforcement is difficult. A written policy should be consistent with and complement an employer’s Systems Usage (such as Internet, the computer system, e-mail, etc.) policies.

Although a social media policy should be tailored to the specific company, the following topics should be included in a well written social media policy:

- State what the employer’s expectations are, including whether employees are allowed to access social media sites while at the workplace or during work time.
- State that there is no expectation of privacy in the use of the company’s equipment and systems, which equipment and systems belong to the company, and the company has the right to access and monitor such equipment and systems.
- State whether and, if so, to what extent a company’s equipment or systems can be used for personal use.
- State whether employees can use personal devices at the workplace or on work time.
- State that employees may not disclose any of the company’s (or its customers’) confidential or trade secret information, logos, etc.
- State that employees are not allowed to make statements on behalf of the company unless they are specifically authorized to do so.

- State that the company may impose disciplinary action, up to and including termination, for violation of its social media policy.
- State that employees should exercise good judgment, as social media sites are not private.
- Include a general disclaimer that the social media policy will be interpreted in a manner that is consistent with all applicable laws.
- State that employees must comply with other company policies when using social media (such as anti-harassment and anti-violence policies).
- State whether the company will be monitoring social media sites (consider blocking software to restrict access to certain web sites)<sup>3</sup>

#### **B. Training & Education**

Just as employers should train their employees with regard to their anti-harassment, discrimination and other policies, employers would be well-served to educate employees regarding social media and related online behavior. Employer education about general online behavior will benefit employees who use social media sites. Discussing real-world examples of improper usage of social media sites and the harm caused thereby should prove to be an effective teaching technique.

#### **4. Electronic Discovery of Social Media Information**

In litigation, parties now frequently try to discover information contained in the other party's social media postings. Courts generally allow the discovery and introduction into evidence of such postings that are available to the general public for viewing on the Internet. Courts seem to be allowing some greater protection, on privacy grounds, against discovery of such postings when the postings are accessible only to friends or are password-protected. That protection, however, is not absolute.

Discovery of private data on social media sites raises complex questions under the federal Stored Communications Act, 18 U.S.C. §§ 2701-11. In a lengthy opinion, many of these issues are discussed in *Crispin v. Christian Audigier Inc.*, 717 F.Supp.2d 965 (C.D. Cal. 2010), a copyright case. The defendants sought information from Facebook and MySpace, including the plaintiff's subscriber information and all communications by the plaintiff referring to any of the defendants. The court ultimately disallowed discovery of private messaging content, i.e., private messages and comments visible to a restricted set of Facebook or MySpace users.

In *Romano v. Steelcase, Inc.*, 30 Misc.3d 426, 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010), a woman sued for personal injuries allegedly suffered when she fell from an office chair. The plaintiff claimed extensive physical injuries with a loss of enjoyment of life. Steelcase subpoenaed her Facebook and MySpace profiles, including those portions of her profile she

---

<sup>3</sup> Employers must be sure to comply with any applicable laws such as the federal Electronic Communications Privacy Act, the Minnesota Privacy Communications Act, the federal Wiretap Act, and the federal Stored Communications Act. Similarly, some states, such as Delaware and Connecticut, require employers to give employees notice before monitoring their e-mail or computer at work.

marked private using those sites' privacy settings. Steelcase argued that, based upon the public portions of her profile, reasonable grounds existed to believe that the woman had an active lifestyle and engaged in physical activities inconsistent with her claims in the litigation. The plaintiff countered that she had a reasonable expectation of privacy in her home computer. The court rejected plaintiff's argument, ruling that her argument would condone her attempt to hide relevant information behind self-regulated privacy settings. The court found that her public postings provided a reasonable basis to conclude that her private postings may contain relevant to the defense of the lawsuit. *See also Sedie v. U.S.*, No. C-68-04417EDL, 2010 WL 1644252 (N.D. Cal. Apr. 21, 2010) (plaintiff claimed her ability to paint adversely affected by accident, then discussed painting on MySpace site).

In *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430 (S.D. Ind. 2010), the court addressed a similar issue in a sexual harassment case. The employer sought the production of all of the employees' photographs, videos or other postings on Facebook or MySpace because, it argued, this social media content would bear upon the claimants' allegations that they suffered emotional injuries beyond "garden variety" emotional distress. The court allowed discovery of the social media content, but only those postings that revealed, referred or related to any emotions, feelings or mental state.

## **5. Legal Ethics and Lawyers Using Social Media**

A 2009 survey of nearly 1,500 lawyers concluded that more than 70% of lawyers are members of an online social network, up 25% from the previous year and up 30% among lawyers aged 46 and older. Baldas, "They Blog, They Tweet, They Friend," Nat'l L.J. (Dec. 21, 2009). Similarly, the ABA's 2010 Legal Technology Survey Report reported that 56% of attorneys in private practice have a presence on a social media site, up from 43% in 2009 and 15% in 2008. *See generally* Margaret M. DiBianca, Ethical Risks Arising from Lawyers' Use of (and Refusal to Use) Social Media, 12 Del. L. Rev. 179 (2011); Abigail S. Crouse & Michael C. Flom, Social Media for Lawyers, Bench & Bar of Minnesota (Nov. 2010).

While this article is not intended to be a comprehensive review of ethical issues for lawyers when using social media, the following highlights areas in which lawyers should proceed with caution:

### **A. MRPC 1.6: Client Confidentiality**

Social media users love to be social. Twitter, Facebook, and other users of social media sites enjoy telling their friends - and sometimes the world - where they have been and what they are doing. Lawyers are no exception.

Lawyers should be very careful not to reveal client confidences or secrets when using social media. *See DiBianca*, 12 Del. L. Rev. at 187-90. Specifically, lawyers must avoid posting items regarding their clients or matters on which they have worked or will work. Even discussing a particular motion without naming names could reveal confidential information, particularly if you had previously disclosed the client's identity to anyone with access to your

post. Mayle, Navigating the Ethical Pitfalls of Online Networking, ABA Young Lawyers Division, The 101 Practice Series: Breaking Down the Basics (2009). Such a disclosure of client confidences could lead to disciplinary action. Levin, More on the New Rules – Social Networks, CBA Record (Nov. 2009).

Further, the identity of clients and client matters should not be posted on social media sites without the informed consent of the client. If informed consent is not an option, keep the information generic and unrecognizable. This can be tricky. For example, people may ask lawyers to provide recommendations for them, and frequently those people work for clients that have engaged the lawyer's legal services. When a lawyer indicates that he or she has "done business with" a person, it may become apparent publicly that the lawyer represented Company X - even though Company X has not given the lawyer permission to reveal this information.

**B. MRPC 4.1: Truthfulness in Statements to Others**

Minnesota Rule of Professional Conduct 4.1 requires truthfulness in statements to others. To comply with MRPC 4.1, lawyers posting on social media sites should make certain their resume and background information is current and accurate. Similarly, lawyers should make sure that any statements they make on social media sites are not inaccurate or exaggerated.

**C. MRPC 5.5: Unauthorized Practice of Law; Multijurisdictional Practice of Law**

Another area of ethical concern arises when a lawyer provides advice in a state in which the lawyer is not licensed to practice law. See Joel M. Schwartz, Practicing Law Over the Internet: Sometimes Practice Doesn't Make Perfect, 14 Harv. J.L. & Tech. 657, 675-77 (2001). Lawyers posting on social media sites should make clear where they are and are not licensed, and what jurisdiction has issued any certifications they hold.

**D. Inadvertent Formation of Attorney-Client Relationship**

Lawyers need to be careful when responding to queries on social media sites. Not only has the attorney not conducted a conflict check to ensure that the lawyer does not have a conflict with the person posting the question (which would be especially difficult if the poster is anonymous), the lawyer has no way of knowing whether the poster is providing all relevant facts or is even who he/she claims to be.

Even when lawyers act professionally on social media sites, another ethical area of concern is the inadvertent formation of an attorney-client relationship by answering questions posted on such sites. Answering specific questions could be considered giving legal advice. Lawyers should distinguish between information and legal advice, and disclaim the creation of any attorney-client relationship or intent to give specific legal advice.

ABA Formal Opinion 10-457 (Aug. 5, 2010) provides some guidance to lawyers in handling interactions with others on social media sites. [http://www.americanbar.org/groups/professional\\_responsibility.html](http://www.americanbar.org/groups/professional_responsibility.html). Initially, offering

information on the firm's website or a social media site does not automatically convert the reader into a client. General information about the law in a narrative or FAQ format is permissible, but the information must meet the requirements of ABA Rules 7.1, 8.4(c) and 4.1(a), which prohibit false, fraudulent or misleading statements of law or fact.

**E. Attorney Investigations**

Just as employers use social media sites as an applicant screening tool, lawyers may use social media sites as part of their investigations in criminal and civil lawsuits. In certain instances, this might run afoul of ethical rules. In Pennsylvania, for example, a lawyer sought information on an adverse witness published by that witness on Facebook and MySpace but accessible only by the witness's friends. The lawyer hoped that these postings might include impeachment material. The lawyer wanted to hire an investigator to become a friend of the witness so that the investigator then would have access to these postings and could give them to the lawyer. This plan violated Pennsylvania's version of Model Rule 8.4 and was found to be deceptive because it would purposefully conceal the investigator's reason for friending the witness and induce the witness into friending the investigator. Philadelphia Opinion 2009-02 (Mar. 2009).

It is always wise to keep in mind that, just as the adverse witness has left an electronic communications trail, so has the lawyer. Do not do anything that you would not want disclosed to a judge, jury, opposing attorney, or the entire world.

**CONCLUSION**

Social media allows people to communicate with one another in ways that never before existed. As is often the case with new technology, it brings with it both the potential for positive value as well as the potential for abuse. The law in this area is truly in its infancy and will undoubtedly grow and develop in the years to come. Employers are well advised to stay up-to-date on the latest developments in this area.