EMPLOYER PITFALLS IN OUR SOCIAL MEDIA WORLD – LIFE WITH TWITTER AND FACEBOOK

I. INTRODUCTION

Whether employers like it or not, social networking sites such as Facebook, MySpace, and Twitter have infiltrated modern culture and impacted the workplace. Businesses that have embraced social networking recognize that this new platform allows them to connect with customers and talent cheaper and more comprehensively than "traditional" media. Those businesses also should recognize, however, that social networking can create public relations nightmares and, in some cases, legal liability.

This article discusses the benefits, challenges, and risks social media and social networking sites create for employers. It identifies the legal dimensions of employers' and employees' use of social media, and identifies areas of concern from a liability standpoint. The article also includes a sample employer policy which incorporates mechanisms to manage the risks associated with social media.

II. SOCIAL MEDIA BACKGROUND

A. Social Media

Social media consist of electronic communications that allow individuals to shift fluidly and flexibly between the roles of audience and author. Social media communications are created in a group/social way as opposed to being created by journalists, editors or media conglomerates. Social media is created using software which does not require extensive technological knowledge and is designed to facilitate rapid communication to a large audience.[1] Social media are said to support the democratization of knowledge and information by transforming people from content *consumers* into content *producers*.[2] Though there are many different forms of social media, each form has three primary components: (1) concept (the art, information, or theme being disseminated); (2) form of media (physical, electronic, or verbal means through which the concept is disseminated); and (3) social interface (degree of engagement -- intimate direct, community engagement, electronic broadcast -- with the audience).[3]

B. Social Media v. Industrial Media

Social media are distinct from industrial media such as newspapers, television, and film. Most obviously, social media are relatively inexpensive and accessible tools that enable anyone (even private individuals) to publish or access information. Industrial media, on the other hand, generally require significant resources (e.g., printing press, government-granted spectrum license) to publish information.

Other comparative properties of social and industrial media include:

---

[1] See Jospeh Thornley, What is "social media"?, available at http://propr.ca/2008/what-is-social-media/.
[2] Http://en.wikipedia.org/wiki/Social_media.
[3] Id.

- Reach - both industrial and social media technologies provide scale and enable anyone to reach a global audience.

- Recency - the time lag between communications produced by industrial media can be long (days, weeks, or even months) compared to social media (which can be capable of virtually instantaneous responses; only the participants determine any delay in response). As industrial media are currently adopting social media tools, social media and industrial media may begin to merge in this respect.

- Permanence - industrial media, once created, cannot be altered (once a magazine article is printed and distributed changes cannot be made to that same article) whereas social media can be altered almost instantaneously by comments or editing.[4]

C. Examples Of Social Networking Electronic Media

Well over one hundred social networking websites exist. Some of the more popular sites include MySpace and Facebook, site where users can add friends and send them messages, update personal profiles to notify friends about themselves, and join networks organized by city, workplace, school, and region. LinkedIn is a social networking site designed to allow registered users to develop a list of professional contacts.

[4] http://en.wikipedia.org/wiki/Social_media.

In blogs -- short for "web-logs" -- entries are periodically posted by users in journal style and often displayed in reverse chronological order. Some blogs provide commentary or news on a particular subject such as food, politics, or sports; and some function as personal online diaries. Blogs also have been used by employees, labor organizations, and employers during union organizing drives (including corporate campaigns), contract negotiations, and strike situations.

A typical blog combines text, images, and links to other blogs, web pages, and media related to its topic. One of the more pioneering blogs is that maintained by Sun Microsystems CEO Jonathan Schwartz (http://blogs.sun.com/jonathan/). Mr. Schwartz uses his blog to bring greater transparency into the corporate world (e.g., his public exchange with Securities and Exchange Commission Chairman Christopher Cox about corporations using websites and blogs to satisfy Regulation Fair Disclosure requirements). In a similarly creative vein, former employee Robert Scoble's blog provided Microsoft a vehicle to soften its corporate image. Mr. Scoble's blog, which is called "Scobleizer" and still is active today, promotes Microsoft products, but also praises competitors. In his role as the first "spokesblogger," Mr. Scoble "succeeded where small armies of more conventional public-relations types have been failing abjectly for years: he has made Microsoft, with its history of monopolistic bullying, appear marginally but noticeably less evil to the outside world . . . ."[5]

Twitter combines elements of blogging and social networking. It enables users to send and read messages, or micro-blogs, known as "tweets." Tweets are text-based posts of up to 140 characters displayed on the author's profile page and delivered to the author's subscribers a/k/a "followers."

III. SOCIAL MEDIA'S EFFECTS ON EMPLOYERS

According to a 2009 study conducted by Deloitte, LLP, 55 percent of employees visit social networking sites at least once per week and 20 percent admit to visiting social networking sites during work hours. Perhaps most significantly, 33 percent of employees do not consider the business implications of their internet postings on such sites. Given the number of people using social networking sites without considering what implications it has for their employer, businesses would do well to focus on the benefits and risks this trend presents.

A. Benefits To Employers

Marketing

Social media is an ideal marketing option for businesses because it is such a cost-effective way of getting a message out to a targeted audience. The most popular online social networking sites provide free personal accounts, from which a business can easily communicate with its stakeholders and audiences. The following icons are being seen more and more often on the websites and emails of businesses small and large:

[5] Robert Scoble, Microsoft's celebrity blogger, The Economist, Feb. 10, 2005, available at http://www.economist.com/people/displayStory.cfm?story_id=3644293.

Including links to a business's social networking accounts can help the business gain control of its brand name; provide additional links for search engine optimization; increase website hits; build better relationships with customers; and provide good public relations.[6]

Customer Feedback

Companies can actively use social media platforms to invite customers to serve as a virtual advisory board, complete with product designing and brainstorming sessions. Social media also facilitate customer reviews. Creating ways for customers to review brands makes good business sense -- a Bazaarvoice study found that 70% of customers who left reviews for products not only wanted to help improve those products, they also purchased more products more frequently than did non-reviewers. Customer reviews also are a way for customers to generate word-of-mouth buzz about products.[7]

Recruiting/Screening

Some employers now rely heavily on Twitter or LinkedIn to fill open positions because recruiting costs can be reduced (i.e., no need to pay a recruiter) and the avalanche of resumes now generated by job boards can be avoided. In addition to helping shape the applicant pool, social networking tools can be used to assess job candidates. According to a new study conducted for CareerBuilder.com, 45 percent of employers are using social networks to screen job candidates — more than double from a year earlier. While soliciting and screening candidates through social networking sites is inexpensive, as discussed more fully below, recruiting through social networks may create potential liability issues.

B. Risks To Employers

Public Relations Risks

Posts on social networking sites may worry employers because of the potential that such posts may embarrass the company. For example, in 2007, a Google employee posted an entry on Google's health advertising blog voicing her negative opinion of Michael Moore's healthcare movie "Sicko." This post received a lot of media attention and very negative feedback from some Google users, who construed the post to be a Google opinion because it was on the company's blog. In the end, Google apologized for the post and admitted that they "blew it."[8]

---

[6] Social Media: the future of small business marketing, available at www.constructaquote.com.
[7] Brian Solis, In Social Media, Collaboration is King, available at http://www.briansolis.com/2009/10/in-social-media-collaboration-is-king/#comment-9544.
[8] http://googleblog.blogspot.com/2007/07/google-and-health-care.html.

The Philadelphia Eagles NFL franchise similarly misstepped when it chose to terminate a game-day employee for calling Eagles management "retarded" after the team let long-term player Brian Dawkins sign with the Denver Broncos. Illustrating how employers must walk a fine line when facing such situations, the Eagles took tremendous public criticism for firing the employee. The negative publicity the Eagles received from that termination probably outweighed any negative publicity the team received from the comment's posting in the first place. If it did not, Dawkins giving his personal allotment of Eagles ticket to the ex-employee ensured that the Eagles would come out of the situation looking the least sympathetic.[9]

Employers overreaching is not limited to employee Facebook posts. The City of Bozeman, Montana, adopted a policy in June 2009 requiring all job applicants to "list any and all current personal or business websites, web pages or memberships on any Internet-based chat rooms, social clubs or forums, to include, but not limited to: Facebook, Google, Yahoo, YouTube.com, MySpace, etc.." The job application also showed a space for passwords.[10] After the city was inundated with "worldwide" negative feedback about the policy, they withdrew it.[11]

All of these situations illustrate the need for employers to keep social networking policies within reasonable limits.

Dissemination of Defamatory Information

As the Eagles found out, there always is a risk that a disgruntled employee may defame an employer on his blog or Facebook page. While the employer may sue the employee for defamation, such a suit may be difficult to win (both in the courtroom and in the court of public opinion). Even if the employer succeeds in litigation, however, the damage done by the initial publication of the defamatory material cannot be undone.

Productivity Reduction

Concern over employees wasting time using social networking sites such as Facebook has resulted in many employers banning the use of the sites during work hours on work computers.[12] However, many companies felt the same concern when they first opened up access to the internet and e-mail. At its core, then, employee productivity and social media is more a people problem than a technology problem. Unproductive people will find ways to be unproductive without using the internet. Proper supervision and performance policies are the real solution to this concern.[13]

---

[9] Dawkins giving ex-Eagles worker tickets, ESPN.com news services, available at http://sports.espn. go.com/nfl/news/story?id= 4041720.

[10] Sharon Fisher, City of Bozeman Demands Passwords from Job Applicants, NewWest Bozemand, June 18, 2009, available at http://www.newwest.net/city/article/city_of_bozeman_demands_passwords_from _job_ applicants/C396/L396/.

[11] Courtney Lowery, City of Bozeman Abandons Hiring Policy on Social Media Passwords, NewWest Bozeman, June 22, 2009, available at http://www.newwest.net/city/article/city_of_bozeman_abandons _hiring_ policy_on_social_media_passwords/C396/L396/.

[12] Benzie, Robert,"Facebook banned for Ontario staffers," TheStar.com, May 3, 2007, Retrieved August 16, 2008.

[13] Doug Cornelius, *Online Social Networking: Is It a Productivity Bust or Boon for Law Firms?*, Law Practice Magazine, March 2009

Dissemination of Proprietary or Confidential Information

An employer's or employee's use of social networking sites creates a risk of disseminating proprietary or confidential information, such as customer information, internal policies and procedures, product information, financial records, and trade secrets. An employee's post about a successful day for the company, for example, could violate notice, disclosure or reporting requirements. Employees in the healthcare industry are especially susceptible to potential confidentiality breaches due to close contact with patients' private medical records and information. For example, in Yath v. Fairview Clinics, No. A08-1556, 2009 Minn. App. LEXIS 117 (Minn. Ct. App. 2009), discussed further below, a patient sued when a clinic employee posted information about the patient's sexually transmitted disease on a MySpace page.

IV. LEGAL RAMIFICATIONS FOR EMPLOYERS

The most pressing concern for employers with respect to their use of or employees' use of social networking sites is liability stemming from that use. Although it is a new and developing area of law, already a number of scenarios related to the use of social media have prompted plaintiffs to bring suits against employers. This section describes these scenarios in more detail.

A. Liability Based On An Employer's Use of Social Media

Recruiting and Screening through Social Media Networks: Potential Liability under Federal Anti-Discrimination Laws

Although social media allows employers to recruit and screen job applicants with reduced costs and increased efficiency, doing so may expose them to liability under federal anti-discrimination laws. If, for example, an employer screens a candidate by looking at the candidate's blog or Facebook page, the employer may view photos or posts revealing a person's race or religious affiliation. If the applicant is not hired, and claims that the employer's knowledge of their protected characteristic factored into the decision not to hire, the employer's use of social media to gather information will come under scrutiny. In order to avoid liability, employers will need to show that the information revealing the protected characteristic played no part in the decision and otherwise will need to reveal their hiring practices.

In the recruiting context, employers should be concerned about disparate impact claims asserted under Title VII because some statistics suggest that social networking sites may exclude certain populations. According to the latest data from Quantcast, only five percent of LinkedIn users are African-American, and only two percent are Hispanic. Users are generally white and age 20 to 40. To the extent that a hiring pool comprised of LinkedIn users can be viewed as one not open to the general population, the use of this social network as the sole means of recruiting may be open to challenge under a disparate impact theory. As long as social networks are used in connection with other methods, however, using them to recruit is valid.

Claims Based on Statements on Employers' Blogs or Networking Sites

If employers chose to use and maintain their own blogs or networking sites, they must strictly monitor the content that is placed on those sites to avoid liability. Google, for example, is being sued for defamation in India after a blogger posted allegedly false statements on the company's blog. There is a real risk that companies in America may be held liable for the statements posted on their websites or blogs.

Invasion of Privacy Claims Based on Employers' Access to Employees' "Private" Social Networking Pages

Some argue that social networking pages are "private areas," like an employee's home, where employers may not go without permission. However, establishing an invasion of privacy claim (or, as to public employers, a constitutional claim for unreasonable search and seizure) can be problematic because of the difficulty in proving that the employee had a "reasonable expectation" of privacy. Liability may arise, though, if (1) the employee reasonably believes that the website is private; (2) the site promotes itself as private; and (3) the employer used nefarious means to gain access to the site. In addition to perhaps creating invasion of privacy liability, an employer's untoward conduct also could subject it to liability under the "terms of use" conditions commonly established by social networking sites and under the Stored Communications Act.

The Stored Communications Act ("SCA") is one of two key provisions of the Electronic Communications Privacy Act.[14] The SCA makes it an offense to "intentionally access without authorization a facility through which an electronic communication service is provided" or to "intentionally exceed an authorization to access that facility" in order to gain access to wire or electronic communication "while it is in electronic storage." In short, the SCA makes it illegal to use illicit or coercive means to access employees' private social media accounts. In Pietrylo v. Hillstone Restaurant Group d/b/a Houston's, an employer was found to have violated the SCA when it fired two employees for complaining about management and posting sexual remarks about managers and customers on a password-protected MySpace account. The employer's managers pressured a third employee into providing her password, logged onto the third employee's account, and viewed conversations occurring among other employees in the chat room. Without the password to the chat room, the managers would have had no way to view the conversations among the other employees. The jury decided that the third employee was impermissibly pressured into revealing the password and that this element of coercion triggered liability under the SCA -- the coercion meant that the employer accessed the MySpace page "without authorization" under the SCA.

B. Liability Based On An Employee's Use Of Social Media

Adverse Actions Taken against an Employee after Learning of the Employee's Social Networking Activities

Employers also potentially expose themselves to liability when they take adverse employment actions against employees based on that employee's activities on a social networking site. In January

[14] The other key provision, the Wiretap Act, prohibits the "intentional interception, disclosure, or use of any wire, oral, or electronic communication."

2004, Ellen Simonetti, a flight attendant for Delta Airlines, initiated a blog titled "Diary of a Flight Attendant" at www.queenofsky.net. Ms. Simonetti posted on the web site photographs of herself posing suggestively on an airplane in her Delta Airlines uniform. When Delta learned of the web site, it discharged Ms. Simonetti for posting inappropriate photographs while wearing her Delta uniform. Ms. Simonetti sued for gender discrimination and retaliation, and for interference of her rights to organize and bargain collectively in violation of the Railway Labor Act. Ms. Simonetti specifically claimed that male employees who posted pictures of themselves on web sites while wearing Delta uniforms were not similarly discharged even though Delta was aware of these postings. She also contended that Delta terminated her because she had participated in labor-organizing campaigns.

Liability Based on an Employer's Knowledge of an Employee's Posts on a Racially Offensive Web Site

It also is possible for employers to expose themselves to liability when they have knowledge of an employee's posts on a racially offensive website. In July of 2009, an association of black police officers (the Guardian Civic League) sued the Philadelphia Police Department for allowing its officers to post "blatantly racist . . . and offensive" content on a popular web site called Domelights.com devoted to law enforcement topics. The website was a private site that was not operated or overseen by the Philadelphia Police Department. The complaint claims that, when white officers posted racist content to the forum site, the Police Department created a hostile work environment on the basis of race, discriminated, and conspired to interfere with the plaintiff officers' civil rights. The Guardian League seeks a ban on "the operation and use of Domelights.com by Philadelphia Police Officers" as well as compensatory and punitive damages. Before the court could rule on whether to shut the web site down, the web site operator voluntarily did so.[15] The case against the City is currently pending.

Tort Liability

It's possible that an employer may be liable when an employee publishes confidential information about a client or patient of the employer on a social networking site. In Yath v. Fairview Clinics, a clinic employee saw an acquaintance visit a doctor and decided to inquire into the acquaintance's medical records. The employee learned that the acquaintance had been diagnosed with a sexually transmitted disease, and a MySpace page disparaging the individual who had been diagnosed with the sexually transmitted disease was eventually created by either the clinic employee or someone who the clinic employee had told about the individual's disease. The MySpace page gained at least six "friends," meaning that at least six people had seen the disparaging page. The individual sued the clinic for invasion of her privacy and for negligent infliction of emotional distress.

The court likened the MySpace posting to the temporary posting of information in a shop window – the information was in view of any member of the public, in large or small numbers, who happened to be passing by. The court concluded that the publicity element of an invasion of privacy claim was satisfied when private information was posted on a publicly accessibly social networking site. The court nevertheless ruled in favor of the clinic-employer, however, because the plaintiff could not prove that the clinic employee had been involved in creating the MySpace page.

[15] http://www.citmedialaw.org/threats/guardian-civic-league-v-philadelphia-police-department#description.

Employers also may be found liable under a negligence theory when employees use their company-owned computers to commit torts. For example, if an employee uses a company computer to access a social networking site in order to defame or harass someone, an individual could assert a negligence claim against the employer. In Sigler v. Kobinsky, however, the Wisconsin Court of Appeals held that summary judgment was properly granted to the employer on the plaintiffs' negligent supervision claim based on giving computer access to an employee who used the computer to harass the plaintiffs. The court explained that there were no facts indicating that the employer should have foreseen that injury was probable from its failure to monitor its employees' use of computers. Accordingly, the court found that, when an employer does no more than provide an employee a computer with Internet access, it is not liable for whatever misuse he may make of the computer.

In Doe v. XYZ, Corp., on the other hand, the New Jersey Appellate Court found that an employer could be liable by not fully investigating an employee's prohibited activity on a company's computer. An accountant for a New Jersey employer (called XYZ Corp. in the lawsuit) was arrested on child pornography charges. A police investigation prior to the employee's arrest revealed that he had viewed child pornography blogs and websites on his work computer, and had also stored nude pictures of his step-daughter on the computer. The child's mother sued the company for negligence, claiming that it knew or should have known that the accountant was using company computer systems to view, download, and participate in child pornography. The Court found that, if the employer had properly investigated the employee's computer usage, it would have discovered the child pornography. The Court also found that, if the employer had discovered the illegal usage, it had an obligation to report the employee to law enforcement authorities. The court's ruling in Doe demonstrates that employers, at least in New Jersey, have a legal duty to both monitor computer use and take prompt and effective action when misuse is discovered.

C. Fair Credit Reporting Laws

The federal Fair Credit Reporting Act ("FCRA") requires an applicant's or an employee's consent before an employer may engage a "consumer reporting agency" to conduct a background check and produce a "consumer report" on that individual. The FCRA does not prohibit employers from receiving or using information it receives directly from a social media site, but if an employer used a third party to secure information derived from social networking sites or blogs, then the employer is required to first gain consent prior to the search and then disclose to the individual that such information was the basis for an adverse employment decision.

State fair credit reporting laws may provide even greater protections to employees than federal laws. For instance, Washington's Fair Credit Reporting Act restricts the scope of employers' background checks to information that is reasonably related to the applicant's or employee's job duties, and an employer may not rely on information in a consumer report that contains information from an applicant's Facebook site or blog unless the information is reasonably related to the work that the applicant or employee would be performing.

D. National Labor Relations Act

If an employer has an overly broad policy that constrains employees' use of social media, an employer may run the risk of violating Section 7 of the NLRA. Section 7 protects employees' right to

form, join, and assist labor organizations, engage in collective bargaining, and to engage in other concerted activities for mutual aid or protection. In this regard, on June 23, 2009, the Associated Press issued a policy which prohibits employees from posting on their personal web pages material about the AP's internal operations, and states that employees should remove third-party posts from their personal sites if they violate AP standards. The president of the News Media Guild Local 31222 has asked the AP to rescind the policy.

V. EMPLOYER POLICIES

Half of employers lack a policy to address employees' use of social networking sites outside of work, even though one-fourth of employers have disciplined an employee for improper activities on Facebook, Twitter, or similar sites, according to survey results released September 25, 2009 by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association. If an employer institutes a clearly defined policy regarding social media use, the risks and potential liability discussed above can be managed and minimized. Other benefits to implementing a social media policy include the following:

1. Employees will have a clear idea of your position when it comes to social media so they will be able to communicate that to the outside world.
2. Employees will feel empowered that they can leverage their social networks in support of their role, as well as for their professional careers.
3. Companies will appear more innovative, forward thinking and knowledgeable of how social media has integrated through employees lives and the rest of the world.
4. Employees will have a set of best practices and guidance while they venture into the social media world, so even the beginners have some reference guide to turn to.[16]

The following section describes in detail what such a policy should and should not contain.

A. Specific Policy Considerations And Suggestions

Considerations and Suggestions Regarding Employees' Use of Social Media

Employers should not ban employees' use of social media altogether. Employers cannot control their employees' online conduct away from the office, and, for the most part, they should not try.

Social-media activities should be subject to all existing company policies that govern the use of the company's communication and computer systems, as well as those that protect the confidentiality of company information, and those which prohibit unlawful discrimination or harassment. In fact, if employers add language about "social media" and "social networking sites" to their existing policies, there may be no need to develop entirely new policies.

Employers should require that employees make clear they are speaking for themselves when they blog or post on social networking sites, and there should be guidelines regarding what employees can and cannot blog about. Specifically, employers should ensure through policy guidelines that:

[16] Brian Solis, Implement Social Media Guidelines, Now, available at http://www.briansolis.com/ 2009/09/implement-social-media-guidelines-now/.

- employees do not use the name, trademarks, logos or copyright-protected material of the company or its clients;
- employees make it clear in any online activity that their views and opinions about work-related matters are their own, have not been reviewed by their employer, and do not necessarily represent the views and opinions of the employer;
- employees do not complain about the company on their blog or networking site before they bring those complaints to HR;
- employees do not list their company e-mail address unless the social networking site is used purely for Company business or professional purposes;
- employees do not disclose information regarding the company's clients, business partners, or the details of a particular engagement or project;
- employees remain respectful of the company's products or services and do not denigrate the quality of your service or products; and
- employees do not post anything obscene, vulgar, defamatory, threatening, discriminatory, harassing, abusive, hateful, or embarrassing to a fellow employee.

Employers should make it clear to employees that they should expect compliance monitoring, meaning that any information they create, transmit, download, exchange or discuss on any social media may be accessed by the company at any time without prior notice (although recall that companies should not use improper and illegal measures to access an employee's private social networking site).

An effective online publishing policy also should identify one person or several people within the company that employees can contact with any questions.

Unless an employee is asked by his supervisor to maintain a blog for the company, employers should insure that blogging is done on the employee's own time, with the employee's own resources and not on the company's time.

Most social networking sites require that users, when they sign up, agree to abide by a Terms of Service (ToS) document. Your policy should hold employees responsible for reading, knowing, and complying with the ToS of the sites they use. It should not contain rules that require employees to violate the common ToS stipulations. For example, most ToS agreements prohibit users from giving false names or other false information, so the company policy should not require users to use pseudonyms when signing up for social networking sites.

Finally, to have teeth, a policy must include disciplinary consequences for violations.

Policy Considerations and Suggestions Regarding an Employer's Use of Social Media

When employers use Facebook, MySpace, or Twitter to reach a younger, hipper audience and/or promote company business, they should do so cautiously. The following recommendations can help prevent information released on a blog or other social networking site from having a negative impact:

- Limit the number of employees that can post on or update the company's web site;
- Establish a strict policy as to what can be posted on the web site;
- Place a high-ranking employee in charge of supervising the web site and require that every site update or change be reviewed and approved by this individual;
- Prohibit the posting of negative comments about competitors;
- Prohibit posting information about the company's finances (or other private or confidential information) without checking with counsel;
- Avoid posting about controversial issues; and
- Be sure that the company's discipline policy addresses violations of its web posting policy.

SAMPLE SOCIAL MEDIA POLICY

In general, the Company views social networking websites (e.g., MySpace, Facebook, Twitter), personal websites, and blogs positively and respects the right of employees to use them as a medium of self-expression. However, the use of these types of websites can impact both the Company and employees alike. Therefore, the Company has created this policy to establish its expectations for employee use of these types of websites.

Applicability. This policy is meant to apply to social networking sites, personal websites, blogs, photo sharing sites, video sharing sites, podcasts, as well as bulletin boards and comments posted on other websites. For ease of reference, this policy refers to all of these types of websites generically as "social media websites". The absence of an explicit reference to a specific website is not meant to limit the application of this policy. Where no policy or guideline exists, employees should use their professional judgment and take the most prudent action possible. You should consult with your manager or supervisor if you are uncertain about any of your activities on a social media website.

No interference with job duties. The Company's Internet and computer resources are provided to employees to allow them to complete their job duties, and should be used for business purposes only. As such, the Company does not allow personal use of social media websites during work time.

Use outside of work. Employees may use social media websites during their personal time outside of work. Employees must be aware, however, that information they display on the Internet reflects not only on themselves, but could be associated with the Company as well. Therefore, employees are expected to follow these guidelines when using any social media website:

1. Employees may not in any way identify themselves as representatives of the Company or employees of the Company on any website unless otherwise permitted by federal law. This includes user profile fields that may ask employees to identify their place of employment, job title, work experience, etc. Employees should leave these fields blank and not display any identifying information about the Company.

2. The Company's relationships with its clients, customers, and partners are valuable assets. Even positive references can be noticed by a competitor and used to the Company's disadvantage. Therefore, employees may not reference or display any information about any of the Company's clients, customers, or partners without obtaining their express permission to do so.

3. Without permission from the Company, employees should not post or cause to be posted any information about the Company without express permission unless otherwise permitted by federal law. If given permission, employees are expected to be respectful of the Company and its employees, clients, customers, partners, and competitors. All information you display on the Internet should reflect this common respect owed to the Company.

5. Confidential and proprietary information of the Company is not to be discussed or referred to by employees on any social media website, even in private messages between site members who have authorized access to the information. This includes information such as

financial information about the Company, pricing, strategies, intellectual property, and customer information.

6. Employees are responsible for reading, knowing, and complying with the Terms of Service of the social media websites they use.

7. Employees are expected at all times to comply with the law in regard to copyright, trademark, and plagiarism. Posting of someone else's work without permission is not allowed. In addition, employees are expected to not make disparaging comments about other persons or entities on social medial websites.

Other Company policies. All other policies in this handbook apply with equal force to employee use of social media websites. In particular, employees are expected to follow the Company's EEO policy when participating in social medial websites. The Company considers behavior that is inappropriate in the workplace to be inappropriate on the Internet as well, meaning that the Company's EEO policy concerning discrimination, harassment, and retaliation applies equally to the treatment of employees in the workplace or on the Internet.

Disciplinary action. While the Company respects the right of employees to use social media websites, it has established this policy for the benefit and protection of the Company and its employees. Any employee witnessing or who believes a violation of this policy has occurred should utilize the complaint procedure set forth in the Company's EEO Policy. The Company takes the expectations explained above very seriously. As such, employees are advised that violating this policy may result in disciplinary action, up to and including termination.