6-2-2010

Legal and Ethical Implications of Corporate Social Networks

Gundars Kaupins
Boise State University

Susan Park
Boise State University

 doi: 10.1007/s10672-010-9149-8

Legal and Ethical Implications of Corporate Social Networks

Gundars Kaupins and Susan Park
Boise State University

Abstract

Corporate social networking sites provide employees and employers with considerable opportunity to share information and become friends. Unfortunately, American laws do not directly address social networking site usage. The National Labor Relations Act, civil rights laws, and various common law doctrines such as employment at-will and defamation provide the pattern for future social networking laws. Ethical considerations such as productivity, security, goodwill, privacy, accuracy, and discipline fairness also affect future laws. Corporate policies on corporate social networking should balance the employer's and employee's interests. Existing laws and ethical issues associated with social networking should impact social networking policies related to configuration, communication, discipline, and evaluation of policies. Corporate social networking policies should be business-related, ensure user notification of monitoring, maintain adequate records, and provide for reliable, consistent, and impersonal evaluation of monitoring effectiveness.

Keywords: corporate social networking, laws, ethics, organizational policy

Social networking sites such as MySpace, Facebook, and LinkedIn are making it possible for an organization to share information among employees, advertise its products and services, and relate to the customer in a new way on the Web. In April 2009, Facebook had 200 million active users (McCarthy, 2009). Facebook reaches 29.9% of global Internet users versus 22.4% for MySpace. MySpace continues to be the most profitable social network, having about $1 billion in revenue versus $300 million for Facebook in 2008. Facebook is the top social network in all countries except Germany, Brazil, and Japan (Ostrow, 2009). Facebook has grown 228 percent since February 2008. Twitter, a site that allows users to post 140 character blogs, saw a 1374 percent increase in unique visitors over one year and grew to 7 million users in February 2009 (Sutter, 2009).

Corporate social networking sites are becoming more popular because of internal brand building, finding, unlocking and engaging hidden employee intellectual capital, enhancing employees' motivation and satisfaction, and developing products and offerings faster regardless of the organizational design (Communitelligence.com, 2009). The software helps businesses find people and information, understand relationships, create a common culture, enhance friendships among customers, improve knowledge management, facilitate recruiting and retention of younger workers who live on social nets, and keep former employees in the loop (CIO Insight, 2009).

Purpose

The unique contribution of this paper is that it combines the legal and ethical implications of social networking sites in order to provide management policy recommendations for corporate involvement with such sites. Given the fluid nature of social networking laws and ethics, we also provide recommendations for future research on social networking.

Legal Issues

In general, the use of online social networking (OSN) sites, such as FaceBook, MySpace, and LinkedIn, by either employees or employers has been subject to traditional employment law. While several commentators have suggested that Internet use, including the use of OSNs and blogs, should be subject to new rules, this method of communication is such a recent phenomenon that few, if any, new laws have yet to emerge (Byrnside, 2008). Thus, while Congress and state legislatures grapple with this and other new forms of communication technology, courts continue to apply traditional common law and existing federal and statute statutes to employment issues relating to OSN sites.

Numerous legal issues might arise in the context of an employer-maintained OSN page. Although most employees in the U.S. are employed at-will, an employee's interaction with the employer's OSN page might involve legally protected activity, such as whistle-blowing or labor organizing or other concerted activity, or it might reveal information about the employee's membership in a legally protected class. Moreover, an employee who engages in online sexual harassment or posts defamatory or other private information on the employer's OSN page may subject the employer to vicarious liability. An employee also may disclose information to the public that the law requires the employer to keep confidential, such as certain personnel data, trade secrets, or material information regarding an upcoming securities sale. An employee may even post content of a criminal nature which could subject the employer to potential criminal liability. To protect against such liability, employers should update their current policies regarding Internet use to include clear and comprehensive directives to employees regarding their interaction with the employer's OSN site.

The Employment At-Will Doctrine and Exceptions

Employment issues are usually governed by the employment-at-will doctrine, which means generally that employees can be terminated or quit for any reason or no reason at all (Grubman, 2008). Thus, in general, an employee who inappropriately interacts with the employer's OSN site, either at work or during off-hours, may legally be terminated. However, various common law and statutory exceptions to employment at-will may be applicable to legal issues that arise regarding an employer-maintained OSN site, although the likelihood that such an action will justify an actionable claim against the employer is far from clear.

The Implied Covenant of Good Faith and Fair Dealing. In those relatively few states that recognize this exception to employment at-will, employers may be liable to an employee for acting in "bad faith" regarding the terms and conditions of employment (Lichtenstein and Darrow, 2006; Sprague, 2007). Generally, an employer acts in "bad faith" and breaches the implied covenant of good faith and fair dealing when it promises an employee a particular benefit, such as sick leave or retirement benefits, and then terminates or demotes the employee for taking advantage of that promised benefit (Grubman, 2008; Gutman, 2003). This means that an employer who implements a company policy regarding OSN may incur liability if the policy is not applied consistently to all employees, for instance, or if the employer indicates that an employee's social networking activity was acceptable but later disciplines the employee for such activity or uses it as a pretext for trying to avoid paying the employee promised benefits (Grubman, 2008; Sprague, 2007).

Implied or Express Contract. Numerous courts have held that if the employer creates either an express or implied contract with the employee, the employment relationship is not at-will (Gely and Bierman, 2006). Thus, an employer who has contractually agreed to terminate an employee only for just cause may be liable if the employee is fired for posting an item on the employer's OSN site that is not sufficiently inappropriate to the employer's interests and/or is unrelated to the employee's work.

Public Policy Exception / Whistle-Blowing. The public policy exception to employment at-will is broad enough to cover many different scenarios. Generally, it means that an employee is wrongfully discharged if terminated in a way that would violate the state's official public policy (Grubman, 2008; see also Gutman, 2003). For example, an employee who is fired for reporting to jury duty may have been wrongfully discharged because the state's public policy requires all citizens to perform this statutory duty. The public policy exception is also generally applicable when an employee exercises a constitutional right or refuses to break the law for the employer (Grubman, 2008; Lichtenstein and Darrow, 2006). Employers who encourage employees to participate on the employer's OSN page may also be inviting employees to discuss their work activities and relationship with the employer. This exception could protect an employee who posts comments or other information regarding legally protected activity on the employer's OSN page.

The public policy exception encompasses state and federal statutes which provide protection from employer retaliation against an employee who "blows the whistle" on the employer's illegal behavior. For instance, Section 704 of Title VII of the 1964 Civil Rights Act (1964) specifically prohibits retaliation against an employee who "has opposed any practice made an unlawful employment practice" by the Act. The Sarbanes-Oxley Act (2002), Family and Medical Leave Act (1993), Occupational Safety and Health Act (1970), and Fair Labor Standards Act (1949), as well as many state statutes, contain similar provisions (Kirkland, 2006; see also Clineburg and Hall, 2005). However, most state whistle-blowing statutes provide protection to employees only if the employee has properly reported the alleged violations to an

appropriate governmental agency (Kirkland, 2006). Thus, in general, an employee's comments on an OSN site, absent any other action taken, may not protect the employee from the employer's subsequent retaliation.

Labor Relations

Section 7 of the National Labor Relations Act (NLRA) (1947) gives to all covered employees, in part, the right to engage in "concerted activities for the purpose of collective bargaining or other mutual aid or protection." Employees might engage in such concerted activity in a variety of ways, including via the Internet.

In Konop v. Hawaiian Airlines (2001), the 9th Circuit Court of Appeals held that an online bulletin board maintained by a company pilot to discuss and criticize the employer's negotiation with the union was protected concerted activity under the Railway Labor Act (RLA). The Konop Court relied upon NLRA precedent to reach its decision, as is typical for courts in RLA cases, which indicates that the Konop holding would likely extend to employees covered generally by the NLRA (Grubman, 2008; Strege-Flora, 2005). The Konop holding suggests that an employer policy which prohibits employees from accessing the employer's OSN page to discuss work-related policies may violate Section 7 if it is overly-broad regarding confidentiality, wage-secrecy, solicitation, or is found to be discriminatory (*i.e.* the policy prohibits union activity on the employer's Facebook page but allows for other, non-business related activity) (King, 2003, Strege-Flora 2005). The NLRA also protects employees who engage in non-union related concerted activity, but it does not extend to an employee's individual action taken on his or her own behalf, nor does it allow an employee to disparage the employer, engage in insubordination, or post confidential information on the employer's site (King, 2003; Sprague, 2007).

Discrimination Statutes and Employer Liability for Sexual Harassment

Federal or state statutory law may be applicable in instances in which an employer is alleged to have discriminated against an employee for revealing some type of protected status via the Internet. For instance, suppose a corporate employer allows employees to use the company Facebook page to post announcements of a personal nature, so a supervisor extends an invitation to other employees to attend services at his church. If other employees complain, would the employer be obligated to remove the post? On the other hand, would the employer be obligated to allow the post to remain to fulfill its responsibility to reasonably accommodate an employee's religious beliefs or practices? Title VII of the 1964 Civil Rights Act may provide protection to employees who post comments, photos, etc. on an employer's OSN that reveal information about the employees' protected characteristics – race, color, religion, gender, and national origin. (Grubman, 2008). Several other federal statutes, such as the Americans with Disabilities Act (1990) and the Age Discrimination in Employment Act (1967), as well as many state statutes, also protect employee's from discrimination in the terms and conditions of employment because of a protected trait, belief, or activity.

Online harassment is a related concern. Online social networks may also be used as a vehicle for sexual or other harassment, potentially subjecting an employer to liability under Title VII or other anti-discrimination statutes. In Blakey v. Continental Airlines (2000), the New Jersey Supreme Court considered whether comments made by employees on an employer-maintained online bulletin board could result in the employer's liability for workplace sexual harassment. Applying Title VII, the court held that a work-related Website "could undoubtedly be so closely related to employment as to become an extension of the workplace." In fact, the court held this to be true even if others outside of the workplace had access to and the ability to post comments on the site. Finding that Continental was aware of the harassment occurring on its bulletin board but did nothing to remove the comments or reprimand the pilots who posted them, the court awarded the plaintiff $1.7 million in damages.

Although limited to only Continental Airlines crew, the online bulletin board in Blakey is quite similar to an employer-maintained OSN. Both are accessible outside of the workplace and allow users to post comments. Both create, as the Blakey court described, a "virtual community" through which employees communicate and "build relationships." Accordingly, it is quite possible that an employer may incur liability for sexually harassing posts and comments made on the employer's official OSN page if the employer is aware of the posts and fails to remove them promptly (Higgins, 2002; Lichtenstein and Darrow, 2006).

Vicarious Liability Issues

In general, under the theory of *respondeat superior*, employers will be vicariously liable for torts employees commit while acting within the course and scope of employment (Greenbaum and Zoller, 2006). An employer that maintains an official company OSN site could assume such liability for posts made on its site in several ways. Posts made on the site might be defamatory, invade an employee's or other person's privacy, or, if outrageous enough, inflict emotional distress. They could even suggest criminal behavior, for which the employer might be liable in certain circumstances.

Defamation. Employers should take precautions to avoid incurring liability for defamatory posts employees or others might make on the employer's official OSN site. Certainly an employer who posts defamatory material on its own site would likely be liable for the consequences (Lex, 2007). However, does that liability extend to comments employees or "friends" post on the employer's OSN site? For instance, assume an employee posts the following false statement on the employer's site: "Jane didn't show up for work today because she had too many margaritas last night with her crew." If this statement meets the general criteria for defamation (an untrue, damaging statement made to at least one other party), might the employer be vicariously liable to Jane, given that the employer "maintains" the site and has control over who has access to it?

In the context of defamatory statements employees make on an employer's blog, many authorities assume an employer's general liability under the theory of *respondeat superior* if the employee makes the statements while acting within the course and scope of employment (See Grubman, 2008; Gutman, 2003). This raises an interesting question about whether an employee posting comments on an employer's OSN page is indeed acting within the course and scope of employment. Employer-maintained OSN pages are similar to workplace blogs. In both instances, the employer has control over who has access to the site and the ability to post comments or other information. Most OSN sites also provide users with the ability to remove comments others post on their pages. As Gutman points out, "[t]ort liability could extend to the employer who does not exercise proper control or whose neglect made the activity possible."

On the other hand, Lex (2007) has suggested that many posts made on a company OSN page may *not* be defamatory because of the casual atmosphere of OSN. According to Lex, "[c]onsidering that MySpace is primarily a site for socializing and not the place to go for hard-hitting news or research, many potentially defamatory statements may escape liability simply because MySpace viewers will not necessarily take what they read as fact." However, Lex also suggests that "[o]n the other hand, the same casual atmosphere may lead users to believe that they can say anything they want without facing legal consequences. Despite the informal context of MySpace, any communication that meets the elements of defamation potentially faces legal liability. Given that there are over one hundred million users, even a few cases could represent a significant problem looming over the legal landscape." Particularly in instances in which an OSN page is officially maintained by the employer, it may be reasonable for a reader to conclude that any content found on the page is at least acceptable to the employer.

A related issue concerns the liability of those who "republish" defamatory statements. Generally, a new party who repeats a defamatory statement is also liable for defamation, as if he or she were the original publisher of the false statement (Lex, 2007). However, this law may not apply to an employer's liability for defamatory posts an employee or "friend" makes on the employer's OSN site. In 2000, Congress amended the Communications Decency Act of 1996 by adding the "Good Samaritan" provision to provide immunity for providers and users of an "interactive computer service" from liability for the posting of certain information, including potentially defamatory content (Benedict, 2009; Lex, 2007). Specifically, this provision provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." While it appears that Congress may not have intended the Good Samaritan provision to apply to individual OSN users, Lex suggests that both the language of the Act itself and subsequent court interpretations could lead to such immunity. Congress enacted this provision well before the advent of newer forms of technology such as online social networking, so the application of this immunity clause to individual OSN "users" is problematic. Whether a company is liable for an employer or friend's defamatory post on the company's OSN page will likely depend upon how actively involved the company is in the republication of the material. According to Lex:

> [T]the greater role that a [OSN] user plays in publishing the information, the more likely it is that courts will view the user as an original publisher. … The most obvious scenario in which the [OSN] user could enjoy immunity would be if a third party posted defamatory statements in the user's "Comments" section. In this case, the user would have republished the statements in a completely passive manner, much like the AOL and CompuServe 'republish' statements made on their forums.

Thus, while employers might be immune from liability for defamatory statements made on an official OSN page, the best approach for an employer is to approve of "friends" with care and carefully monitor all comments and other activity on the OSN.

Privacy. Workplace privacy violation claims may generally take one of three forms: intrusion upon solitude or seclusion, public disclosure of private facts, or publicly placing an individual in a false light (Gabel and Mansfield, 2003). Of the three, public disclosure of private facts is the likeliest cause of action that may arise when a post on the employer's OSN divulges private information. The essence of such a claim of invasion of privacy is whether the employee has a reasonable expectation of privacy regarding the information (Brandenburg, 2008). With regard to other forms of online communication, such as computer Internet access and work email systems, courts have almost uniformly held that employees do not have a reasonable expectation of privacy in these areas (Milligan, 2009). However, those cases generally concern employees who act affirmatively to transmit their own private information. Could such holdings extend to posts others make on a corporately maintained OSN site? Certainly an employer who knowingly posts private information about an employee on its public FaceBook or MySpace page could subject itself to direct liability for invading the employee's privacy. What about situations in which a friend or employee posts the offending information on the employer's site? Could that also subject the employer to vicarious liability? In light of the rational of Blakey, this is indeed possible. It seems reasonable to assume that if the employer's OSN is sufficiently work-related, and the employer knows of the offending post and fails to remove it within a reasonable amount of time, the employer may be vicariously liable for any resulting damage.

Intentional Infliction of Emotional Distress. Causes of action based upon intentional infliction of emotional distress require proof of intentional, outrageous behavior (Gabel and Mansfield, 2003; Sprague, 2007). In this situation, such a claim would require the employee claimant to show that the employer's conduct in either posting a comment directly or allowing another user's post to remain public on the employer's OSN was outrageous and that it caused the employee severe emotional distress.

Criminal Liability. Consider the following scenarios. An employee posts a link to pornographic material on the employer's OSN site. A recently-fired, disgruntled employee posts a death threat against his supervisor on the employer's OSN site. Might the employer be liable for this type of potential criminal activity? Perhaps. Generally, an employer may be liable even for the criminal acts of its employees if the criminal act in question originates "in activities so closely associated with the employment relationship as to fall within its scope" (AmJur 2d, 2009). Moreover, if the employer's property or resources are used in the commission of the crime, the employer could be subject to criminal action (Gutman, 2003).

Disclosure of Confidential Information / Misappropriation of Trade Secrets / Securities Fraud

Employees who post confidential information, such as personnel data pertaining to other employees, on an employer's OSN page (and perhaps the employee's personal page as well) may subject the employer to liability if the employee was acting within the course of employment at the time (Grubman, 2008; see also Gutman, 2003). The disclosure of an employer's trade secrets in a public forum could damage the employer (and also subject the employee to liability under state or federal trade secret laws) (Clineberg and Hall, 2005; Grubman, 2008). Moreover, Section 10b-5 of the 1934 Securities and Exchange Act prohibits the disclosure of material, nonpublic information under certain circumstances. An employee could potentially subject his employer to a 10b-5 violation by posting such information on the employer's networking site, especially when the price of the company's stock is fluctuating (Clineberg and Hall, 2005; Grubman, 2008).

Ethical Issues

Legal principles and ethical principles are often closely aligned, but they are not the same and they have different objectives. Laws involve a system of rules that stabilize social institutions. They have a function of deciding when to bring social sanction on individual citizens and their specific acts. Ethics involve why and how one ought to act. They are more concerned than laws in promoting social ideals. Ethical principles also may be viewed as the standard of conduct that individuals have constructed for themselves (Candilis, 2002).

Many professional codes of ethics prescribe principles that are perfectly legal to ignore. It is, for example, not a criminal offence for a professional engineer to be undignified. Relying on the law to resolve an ethical dilemma will fail to take into account many of the obligations and duties that our society expects of its members (Sims, 2003).

Ethical concerns provide another way to analyze appropriate use of social networking sites. Social networking concerns may overlap with similar concerns associated with the Internet, e-mail, and regular work behavior.
Though many social networking issues such as security, privacy, and accuracy are directly linked with the fair collection of information, we go beyond fair collection of information issues by also focusing on discipline and dignity issues. These are separate from fair collection of information issues because productivity focuses more on good business practices, discipline focuses on procedural fairness, and dignity focuses on the state of being honored and esteemed.

Ethical Concerns

Inappropriate Networking. What happens if your boss types personal and private notes on the corporate social networking site? This overlap between personal life and professional life could create potential sexual harassment problems and provide too much information to the boss (Greenbaum, 2008, Schultz, 2008).

Social networking among employees within corporate social networking sites can lead to considerable waste of time when employees are chatting with their friends or fellow employees on noncorporate-related topics. Kirkpatrick (2008) cited a study that found that corporate social networks are a waste of money and time. About thirty five percent of corporate social network activity has less than 100 members. Less than 25 percent have more than 1000 members, though over half of those companies have spent over a million dollars on the sites. The biggest problem with corporate networking sites has been overpriced, fancy features, inexperienced social network management, and poor information about the quality of information coming from social network sites.

To control inappropriate networking, monitoring content on a corporate social network site might take considerable time and resources (CIO Insight, 2009). A monitor might not be able to distinguish between what is personal and work-related. A monitor may disseminate information about an employee who has done something inappropriate that is personal. Even if it is work-related, a monitor could inappropriately accuse an employee of wrongdoing without doing a proper investigation. A monitor might investigate a non-random sample of employees to specifically try to hurt one individual or a group. A monitor also might investigate a sample right before Christmas when the temptation is highest to type personal information. Other times could be ignored.

Security. A security concern is that employees might share secret aspects of their company on a corporate network page such as passwords, new products, and new services. Social networkers may intentionally or unintentionally reveal organization secrets such as corporate finances, marketing intentions, business strategies, or new products and services. Warnock (2007) cited a study of 300 IT decision makers that indicated 10 percent of organizations investigated the unauthorized disclosure of financial information through blogs or message boards. Confidentiality violations can reveal organizational secrets to the whole world. Company secrets can lead the company open to hacking (Kaupins and Minch, 2006).

Privacy. The privacy of each employee may be breached many ways. Inappropriate pictures of binge drinking or doing illegal drugs can be posted. Nasty comments about ex boy or girlfriends can lead to jealousy and insults. Constant posting of comments on people's walls can irritate them and block other people's comments. Insensitive topics can be discussed including religion, politics, and racism/sexism (Urban Dictionary, 2008).

Employers can easily find details about employees not only through the Google and other search engines, but also through specialized spywebs. For example, Spokeo, like its competitors Piple and CVGadget, can import entire e-mail address books of individuals. They monitor contacts and know if anybody has done anything new on the Web (Raphael, 2009).

Further privacy is reduced when the terms of the social network can be changed at any time. Phrases such as "We reserve the right, at our sole discretion, to change, modify, add, or delete portions of the Terms of Use at any time without further notice" can drastically affect privacy policies.

When companies recruit potential employees, the employees' Facebook, Twitter, and MySpace pages can include information on race, health, politics, and religion that employers should not be investigating because such information is inappropriate and in violation of various Civil Rights laws. The employer should not request access to private social networking pages (Greenbaum, 2008).

Accuracy. A manager may not know if information on a corporate social networking site is accurate. An employee can post false financial information on a social networking site for a few minutes and then erase it after damage has been done. Determining whether that employee posted such damaging information can be difficult to prove if the information has been erased. People who put false information on such sites might intentionally insert false information as a prank (Ethics Scoreboard, 2009). Factual information can be taken out of context because only short snippets are seen on the screen at once. Other communications can be hidden by the "click here for more posts" button (Schultz, 2008).

Rejection. "Staff members that decline friend invitations from volunteers or even other staff members via corporate OSN platforms may end up hurting the feelings of those they work with. Encourage staff and volunteers to respect that some people may want to keep their OSN activities separate from their work or volunteering relationships" (Coyote Communications, 2008).

Dignity. Dignity is the quality or state of being worthy, honored, or esteemed. If an employer discovers or publicizes unsavory untrue personal details about an employee, mutual respect might be reduced (Kaupins and Minch, 2006).

Exclusion. "Many OSN platforms are blocked from being used by employees at various businesses and government organizations. Many of these platforms are also not accessible for people using assistive technologies, for people with certain disabilities, or for those using older software and hardware. This means an organization should not switch any of its outreach activities, such as blogging, instant messaging or photo sharing, entirely over to OSN platforms, as many people are prevented from accessing such. In other words, your OSN outreach activities should not replace your other online outreach activities, as they will exclude many people." (Coyote Communications, 2008; Bonfield, 2008).

Policy Recommendations for Organizations

Existing laws and ethical issues can have major implications on corporate social networking policies for organizations. The employer's business interests must be balanced with an employee's privacy interests. Legal monitoring policies tend to be associated with several dimensions— how monitoring is configured, how monitoring is communicated, how discipline is applied, and how the impact of monitoring is evaluated. Each dimension can range from no activity to significant action. These four dimensions are modeled off the location monitoring work of Kaupins and Minch (2006).

"Configuration" is the operational shell around OSNs. It refers to who shall be monitored, by what means are people monitored, and when and where monitoring take will place. It is the operational shell around OSNs.

"Communication" refers to communication of the OSN policies with employees. Employees should be informed of the timing, means, location, and security associated with policy communication.

"Discipline" focuses on major facets of discipline such as progressive discipline, corrective discipline, and the hot stove rule. Progressive discipline deals with providing employees increased discipline for greater infractions. Companies may start with an oral warning, then proceed with a written warning if the inappropriate behavior continues. Further discipline could be a suspension and discharge. Corrective discipline involves providing the employee with appropriate counseling to help correct inappropriate behavior on a social networking site. The counseling could be followed with appropriate monitoring of future networking behavior. The hot stove rule states that all discipline should be with a warning, impersonal, consistent, and immediate. Of course, all discipline should be appropriate for the business and the specific incident(s) involved.

Concerning "evaluation", all monitoring policies should be evaluated for their reliability, validity, and adverse impact on employees. Data about social networking activities should be produced. All monitoring policies should periodically be reviewed and revised.

Table 1 provides a summary of policy recommendations based on the four dimensions just discussed. Each dimension contains a list of major policy questions. Solutions are based on recommendations from employee handbook experts, ethics code developers, legal researchers, international organizations, and government directives and laws. In cases such as "who will do the monitoring", several choices are provided to organizations.

INSERT TABLE 1 HERE

Sample Employee Handbook Statements

To apply these policy recommendations, companies should establish clear corporate social networking policies that can be published in their corporate employee handbooks, disseminated on the Intranet and Internet, or distributed via letter or e-mail to employees. Employees should acknowledge that they have read the social network monitoring policy by signing an acknowledgment form. Unfortunately, employees tend not to read employee handbooks and letters even though they sign acknowledgment forms. Management may have to remind employees with additional e-mails of the policies and be familiar with the policies themselves in case of policy disputes (Dessler, 2009; Baskin, 1998). Many of these policies can be extensions of existing e-mail and blogging policies (Warnock, 2007).

Customers might need to be aware that employees' social networks are monitored to protect their privacy. They might not want to be discovered being with an employee who is a competitor, illicit lover, or any other person that can cause embarrassment.

Sample Policies

Figure 1 shows sample employee handbook policy based on research summarized in Table 1. It incorporates configuration, communication, and discipline dimensions. The statement allows management flexibility in implementation. Three policies are included: social network monitoring, corporate social networking, and evaluation of social networking policies.

INSERT FIGURE 1 HERE

Suggestions for Future Research

Corporate social networking research is still very young due to the young industry. Several future research avenues can be created.

More detailed case analyses can be made concerning any new developments in the use of social network monitoring by companies and the use of corporate social networks. The impact of any new laws on social networking policies needs to be made.

Empirical and survey research is needed to help analyze management and employee attitudes toward the need for limits on social network monitoring and corporate social networking. Legal liability might be a primary motivation to monitor employee social networking. Survey research also can help analyze what type of organizations will be most likely to use social networking and what social networking policies will tend to be the most important and most commonly used in practice. Data should be collected concerning corporate age group usage, purposes of social network sites within companies, and discipline for inappropriate behavior.

Conclusion

Existing laws and ethical considerations affect social networking policy recommendations related to configuration, communication, discipline, and evaluation issues. Business-related monitoring should be clearly defined and disseminated to all employees through a wide variety of communication methods. Employees should receive warnings for inappropriate social networking activities. Consistent evaluations of monitoring effectiveness should occur. Future research should analyze what type of social networking monitoring and corporate social networks are involved in organizations.

References

Age Discrimination in Employment Act, 29 U.S.C. §§ 621 *et seq* (1967).

American Civil Liberties Union (2008, February 8). Online Privacy Statement. Accessed August 7, 2009 at *http://www.aclu.org/infor/18864res20050401.html*.

Americans with Disabilities Act, 42 U.S.C. §§ 12101 *et seq* (1990).

AmJur 2d (2009). Employment Relationship, 27, § 381.

Attaway, M. C. (2001). Privacy in the workplace on the web. *Internal Auditor, 58,* 30-35.

Baskin, M. (Winter, 1998). Is it time to revise your employee handbook? *Legal Report*, Alexandria Virginia: Society for Human Resource Management.

Benedict, J. (2008-2009). Deafening Silence: The Quest for a Remedy in Internet Defamation. *Cumberland Law Review, 39,* 475.

Bersin, J. (2007, November 16). Social networking: meet corporate America. Accessed February 9, 2009 from *http://joshbersin.com/2007/11/16/social-networking-meets-corporate-america/.*

Blakely v. Continental Airlines, Inc., 751 A.2d 538 (N.J. 2000).

Boehle, S. (August, 2000). They're watching you: workplace privacy is going, going…. *Training, 37,* 50-60.

Bonfield, B. (2008, January 8). Should your organization use social networking sites? Accessed February 9, 2009 from *http://www.techsoup.org/learningcenter/internet/pages7035.cfm*.

Brandenburg, C. (2008, June). The Newest Way to Screen Job Applicants: A Social Networker's Nightmare. *Federal Communications Law Journal, 60,* 597.

Bureau of National Affairs (2009). *BNA Employment Guide*. Washington, D. C.: Bureau of National Affairs.

Byrnside, I. (2008, Winter). Six Clicks of Separation: The Legal Ramifications of Employers' Using Social Networking Sites to Research Applicants. *Vanderbilt Journal of Entertainment and Technology Law, 10,* 445.

Camardella, M. (2003). Electronic monitoring in the workplace. *Employee Relations Today, 30,* 91-100.

Candilis, P. J. (2002). Distinguishing law and ethics: a challenge for the modern practitioner. *Psychiatric Times, 19* (12). Accessed September 8, 2005 at *http://www.psychiatrictimes.com/ethics.html*.

CIO Insight (2009). Five reasons to deploy a corporate social network. Accessed February 9, 2009 at *http://www.cioinsight.com/c/a/past-news/5-Reasons-to-Deploy-a-Corporate-Social-Network/.*

Clineburg, Jr., W.A. and Hall, P.N. (2005). Addressing Blogging by Employees. *The National Law Journal.*

Communications Decency Act, 47 U.S.C. §§ 652 *et seq* (2000).

Communitelligence.com (2009). Building Employee Branding and Engagement with Internal Social Networks. Accessed March 3, 2009 from *http://wwwl.communitelligence.com/content/ahpg.cfm?spgid=361&full=1*.

Coyote Comunications (2008, November 27). Nonprofit Organizations and Online Social Networking: Advice and Commentary. Accessed August 7, 2009 from *http://www.coyotecommunications.com/outreach/osn.html*.

Deschenaux, J. (2009, March 12). Dealing With Employees' Offensive Blogs and Facebook Postings. Accessed March 16, 2009 from *http://www.shrm.org/legalissues/stateandlocalresources/pages/offensiveblogsfacebook.htm*.

Dessler, G. (2009). Fundamentals of Human Resource Management. Upper Saddle River, N. J.: Pearson.

Ethics Scoreboard (2009, March 4). Untitled. Accessed March 20, 2009 from *http://www.ethicsscoreboard.com/list/facebook.html*.

Fair Labor Standards Act, 29 U.S.C. §§ 215 *et seq* (1949).

Family and Medical Leave Act, 29 U.S.C. § 2601 *et seq* (1993).

Gabel, J.T.A. and Mansfield, N.R. (2003). The Information Revolution and Its Impact on the Employment Relationship: An Analysis of the Cyberspace Workplace. *American Business Law Journal, 40,* 301.

Gely, R., Bierman, L. (2006, Summer). Workplace Blogs and Workers' Privacy. *Louisiana Law Review, 66,* 1079.

Glazowski, P. (2008, August 30). Biz networking on Facebook could soon supersede LinkedIn. Accessed February 9, 2009 from *http://mashable.com/2008/08/30/b2b-ad-networking/.*

Goodwin, B. (2003, June 17). Tell staff about e-mail snooping or face court, new code warns. *Computer Weekly, 38,* p. 5.

Graham, J. (2009, March 31). Marketers Find Twitter a Tweet Recipe for Success. Accessed April 1, 2009 from *http://www.usatoday.com/tech/news/2009-03-31-facebook-twitter-status-marketing_N.htm.*

Greenbaum, K. (2008, October 6). Ethics of Facebook Friendship: Can It Really Be a Conflict? Accessed March 20, 2009 from *http://www.igreenbaum.com/20089/10/ethics-of-facebook-friendship-can-it-really-be-a-conflict/.*

Greenbaum, W., Zoller, B. (2006, July/August). Court Decisions Impact Workplace Internet and E-Mail Policies. *HR Advisor*.

Grubman, S. R. (2008, Winter). Think Twice Before You Type: Blogging Your Way to Unemployment. *Georgia Law Review, 42,* 615.

Gutman, P.S. (2003, Fall). Say What?: Blogging and Employment Law in Conflict. *Columbia Journal of Law and the Arts, 27,* 145.

Hawk, S. R. (1994). The effects of computerized performance monitoring: an ethical perspective. *Journal of Business Ethics, 13,* 949-958.

Higgins, M.A. (2002, Spring). Blakey v. Continental Airlines, Inc.: Sexual Harassment in the New Millennium. *Women's Rights Law Reporter, 23,* 155.

Hong, John S. (2007, Winter). Can Blogging and Employment Co-Exist? *University of San Francisco Law Review, 41,* 445.

James, G. (2004, March). Can't hide your prying eyes. *Computerworld, 38,* 35-36.

Kaupins, G. E. (2004), Ethical perceptions of corporate policies associated with employee computer humor. *Ethics and Critical Thinking Quarterly Review, 2004(1),* 16-35.

Kaupins, G. E. & Minch, R. (2006, July-September). Legal and ethical implications of employee location monitoring. *International Journal of Technology and Human Interaction*, (with Robert Minch), 2, 16-35.

King, N. J. (2003, Summer). Labor Law for Managers of Non-Union Employees in Traditional and Cyber Workplaces. *American Business Law Journal, 40,* 827.

Kirkland, A. (2006, Winter). "You Got Fired? On Your Day Off?!": Challenging Termination of Employees for Personal Blogging Practices. *University of Missouri-Kansas City Law Review, 75,* 545.

Kirkpatrick, D. L. & Kirkpatrick J. D. (2006). *Evaluating Training Programs: The Four Levels* (3rd ed.), San Francisco: Berrett-Koehler.

Kirkpatrick, M. (2008, July 17). Corporate Social Networks are a Waste of Money, Study. Assessed February 9, 2009 from *http://www.readwriteweb.com/archives/corporate_social_networks_are.php.*

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2001).

LegalAndrew.com (2007). *Facebook Isn't Private, and 7 Other Things You Should Know.* Accessed July 24, 2009 from *http://www.legalandrew.com/2007/07/21/facebook-and-the-law-8-things-to-know/.*

Lex, R., (2007-2008). Can MySpace Turn Into My Lawsuit?: The Application of Defamation Law to Online Social Networks. *Loyola of Los Angeles Entertainment Law Review, 28,* 47.

Lichtenstein, S.D., & Darrow, J.J. (2006, Fall). Employment Termination for Employee Blogging: Number One Tech Trend for 2005 and Beyond, or a Recipe for Getting Dooced? *UCLA Journal of Law & Technology, 2006,* 4.

McCain, R. S. (2009). Facebook Ethics. The Other McCain. Accessed March 20, 2009 from *http://rsmccain.blogspot.com/2008/03/facebook-ethics.html.*

McCarthy, C. (2009, April 8). Facebook Hits 200M Users, Looks to Charity. Accessed April 9, 2009 from *http://www.cbsnews.com/stories/2009/04/08/tech/cnettechnews/main4930230.shtml*.

Milligan, Tanya E. (2009, February). Virtual Performance: Employment Issues in the Electronic Age. *Colorado Lawyer*, *38,* 29.

National Labor Relations Act, 29 U.S.C. §§ 151-169 (1947).

National Workrights Institute (2004). Electronic Monitoring in the Workplace: Common Law and Federal Statutory Protection. Accessed October 12, 2004 at: *http://www.workrights.org/issue_electronic/em_common_law.html*.

Nolan, D. R. (2004). Privacy and profitability in the technological workplace. *Journal of Labor Research, 24,* 207-232.

Occupational Safety and Health Act, 29 U.S.C. §§ 651 *et seq* (1970).

Organization for Economic Cooperation and Development, (2000). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: OECD Publication Service, Accessed October 12, 2004 at: http://www1.oecd.org/publications/e-book/9302011E.pdf.

Ostrow, A. (2009, March 9). Social networking more popular than email. Accessed April 10, 2009 from http://mashable.com/2009/03/09/social-networking-more-popular-than-email/.

Owyang, J. (2009). What Facebook Connect means for corporate websites. Accessed February 9, 2009 from *http://www.web-strategist.com/blog/2008/07/23/what-facebook-connect-means-for-corporate-websites/.*

People Management (2007, November 15). Facebook-style site attracts staff on rebound. *People Management, 13,* 12.

Porter, W. G. and Griffaton, M. C. (2003). Between the devil and the deep blue sea: monitoring the electronic workplace. *Defense Counsel Journal,* 65-77.

Raphael, J. R. (2009). People Search Engines: They Know Your Dark Secrets…and Tell Anyone. Accessed March 30, 2009 from *http://tech.msn.com/products/articlepcw.aspx?cp-documentid=18632762&GT1=40000*.

Sarbanes-Oxley Act, 18 U.S.C. §§ 2510-2522; 2701-2711 (2002).

Schultz, J. (2008, November 25). Facebook Creeping! The Ethics Involved with Employers Usage of Facebook. Accessed August 7, 2009 at *http://www.jaytaylorschultz.com/PDFs/Research-Facebook-Creeping.pdf.*

Securities and Exchange Act, 15 U.S.C. §§ 78 *et seq* (1934).

Sims, R. R. (2003). *Ethics and Corporate Social Responsibility: Why Giants Fall*, Praeger, Westport, Conn.

Sprague, R. (2008, Fall). Orwell Was an Optimist: The Evolution of Privacy in the United States and its De-Evolution for American Employees. *John Marshall Law Review, 42,* 83.

Sprague, R. (2007, Winter). Fired for Blogging: Are There Legal Protections for Employees Who Blog? *University of Pennsylvania Journal of Labor and Employment Law, 9,* 355.

Strege-Flora, C. (2005, Autumn). Wait! Don't Fire That Blogger! What Limits Does Labor Law Impose on Employer Regulation of Employee Blogs? *Shidler Journal of Law, Commerce & Technology, 2,* 11.

Sutter, J. D. (2009). Is Twitter's Breakneck Growth Causing a Backlash? Accessed March 31, 2009 from *http://www.cnn.com/2009/TECH/03/31/twitter.fail.whale/index.html?iref=t2test_techtues.htm*

Title VII of the 1964 Civil Rights Act, 42 U.S.C. §§ 2000d *et seq* (1964).

Urban Dictionary (2008, September 18). Facebook Ethics. Accessed August 7, 2009, at *http://www.urbandictionary.com/define.php?term-facebook%20Ethics.*

Warnock, O. (2007, September 26). Networking or not working? *Contract Journal, 440,* 31-32.

Table 1
Suggestions for Social Network Monitoring Policies

Dimension	Issues	Sample Solutions
Configuration	Authentication systems	Through user authentication systems involving passwords or devices (Owyang, 2009)
Configuration	Monitoring individuals	Supervisors, top management, IT director (Bureau of National Affairs, 2009)
Configuration	Equipment used	Network of corporate computers (Bersin, 2007)
Configuration	Individuals monitored	Information is collected on an equal basis across all individuals for business purposes only (American Civil Liberties Union, 2008; Nolan, 2004)
Configuration	Time of monitoring	On company time (AllBusiness, 2001)
Configuration	Location of monitoring	Monitoring should be limited to the workplace (Hartman, 1998; National Workrights Institute, 2004) Monitor what is relevant (James, 2004).
Configuration	Behavior allowed	Be clear about the purposes of the social networking communication such as recording useful contacts (Warnock, 2007)
Configuration	Behavior not allowed	Avoid discussing confidential corporate matters. Do not represent yourself as a consumer if you are not one. Provide business-related communication and avoid personal chats. Avoid defamatory statements. (Warnock, 2007, Urban Dictionary, 2008)
Configuration	Policies coordinated	Integrate all electronic communications into one policy (Warnock, 2007)
Communication	Individuals warned	Use covert monitoring only when there is evidence that a crime has been committed (Goodwin, 2003)

		Avoid any covert monitoring (Kaupins, 2004; National Workrights Institute, 2004) Employers should not request access to private social networking pages (Greenbaum, 2008)
Communication	Means by which warnings are announced	Employee handbooks, letters of understanding, e-mails (Boehl, 2000)
Communication	Timing of warnings	A reasonable time before monitoring begins (Organization for Economic Cooperation and Development, 2000)
Communication	Reasons given for warnings	Major reasons may include productivity and security (James, 2003) Sexual harassment (Camardella, 2003)
Discipline	Individuals administering discipline	Supervisor (Bureau of National Affairs, 2009; Attaway, 2001; Hawk, 1994)
Discipline	Types of discipline	Apply progressive discipline and corrective discipline (Bureau of National Affairs, 2009)
Discipline	Appeals	Give employees the right to dispute electronic monitoring data (American Civil Liberties Union, 2008)
Discipline	Retaliation	Provide a non-retaliation policy (Coyote Communications, 2008)
Evaluation	Individuals monitoring monitors monitors	Top management or data collection experts (Organization for Economic Cooperation and Development, 2000)
Evaluation	Methods of monitoring monitors	Analyze the impact of monitoring (Goodwin, 2003) Develop a comprehensive records retention policy (Nolan, 2004)
Evaluation	Frequency of monitor monitoring	Periodical but negotiated evaluation of policies in general are recommended (Dessler, 2009)

Evaluation	Isolation	Check if any group or groups are isolated from the rest of the organization due to lack of access to the social network (Coyote Communications, 2008)
Evaluation	Monitoring success measurement	Monitor reaction of employees and managers to the policy, what management has learned about employee behavior, how employee and management behavior has changed, how policies affect the bottom line and other organizational measures (Kirkpatrick and Kirkpatrick, 2006).

Figure 1

Sample Corporate Social Network Policy

Employees shall use the corporate social network for business purposes only. Business purposes may include productivity, safety, and security issues related to the mission and objectives of the company. Sample productivity issues include generation of new ideas and getting opinions of products and services. Sample safety and security issues include generation of ideas of how to enhance safety and security and monitor possible breaches.

Employees shall not use personal social networking sites on company time. They shall not create personal blogs, disclose confidential information, include defamatory or racially and sexually offensive materials, disparage the company or its competitors, or use the company logo.

Any violation of the policy could lead to discipline following the company's discipline policy.

Sample Social Network Monitoring Policies[1]

Sample Policy

The company reserves the right to monitor the social networking activities of employees for business purposes only. Business purposes may include productivity, safety, and security issues related to the mission and objectives of the company.

Employees will be notified by their supervisor (or human resources, top management) that their social networking activities will be monitored.

Supervisors (or human resources, top management) are responsible for the storage and dissemination of social networking data. Employees have a right to dispute social networking data and discipline related to that data by contacting their supervisor (or human resources, top management) and following the standard discipline appeal procedures of the company.

Sample Monitoring Evaluation Policy

Top management will periodically review its social networking policies and procedures as needed to respond to internal company strengths and weaknesses and external threats and opportunities. The review process includes monitoring the reaction of employees and managers to the policy, what management has learned about employee's behavior, how employee and management behaviors have changed, and how policies affect the bottom line and other organizational measures.

---

[1]As an alternative to the policies shown, social network monitoring may be subject to negotiation between employees and employers. All social network monitoring could be banned unless managers and employees mutually agree to specific monitoring. Top management and employee representatives could periodically review its social networking policies and procedures as needed.