Advances in Business Research
2010, Vol. 1, No. 1, 82-93

Legal and Ethical Issues Associated with Employee Use of Social Networks

Gundars Kaupins, Boise State University
Susan Park, Boise State University

Social networking sites such as Facebook and Twitter can help employees enhance a company's marketing, recruiting, security, and safety. However, employees' use of social networking sites and employers' access of those sites can result in illegal and unethical behavior, such as discrimination and privacy invasions. Companies must gauge whether and how to rely upon employees' use of personal social networking sites and how much freedom employees should have in using networks inside and outside of the companies. This research summarizes the latest legal and ethical issues regarding employee use of social networks and provides recommended corporate policies.

Online social networks (OSNs) provide employees and job applicants with a powerful vehicle to communicate personal and company information. These Web-based services, which include Facebook, MySpace, Twitter, LinkedIn, Wikipedia, YouTube, Yelp, and Flickr, and others, "allow individuals to (1) construct a public profile..., (2) articulate a list of other users…, and (3) view and traverse their list of connections" (Boyd and Ellison, 2007: 1). A broader definition of OSNs also could include Internet forums, blogs, online profiles, podcasts, e-mail, instant messaging, music-sharing, and voice over IP (Churches, Crockett, and Jukes, 2010).

OSN use has seen significant growth in recent years. Facebook especially has grown so much it is number one among OSNs (Churches et al, 2010). As the number of Facebook and other OSN users continues to rise, so too will the amount of personal information employees and job applicants post. A quick Google search of "Facebook" and "employment" results in numerous examples of job applicants or current employees, particularly young ones, who have been denied or lost a job because of personal information posted on an OSN site such as Facebook or MySpace. Moreover, the number of employers who research applicants and employees on the Internet is also on the rise. A recent survey indicates that 75% of U.S. recruiters and human resource professionals research job applicants on the Internet, including social networking sites. A large majority of those surveyed have rejected applicants because of information they have discovered online (Rosen, 2010).

Employers may encourage employees' engagement with personal OSN sites to enhance marketing and recruit new employees. Job applicants may use OSNs to their advantage when seeking employment by posting only information which shows them in a positive light. However, the possible consequences of posting personal information on an OSN, or elsewhere on the Internet, may outweigh the benefits, especially for young college graduates who are more likely to participate in online social networking than older employees. Moreover, posting personal information also can lead to ethical lapses such as privacy violations, inaccuracies, subjectivity, and sharing inappropriate information. Using the Internet to search job applicants and current employees raises legal and ethical questions that both employers and employees should consider, such as privacy, discrimination, fairness, and authenticity.

Legal Issues

The Internet offers employers with an easy, inexpensive way of exercising their duty to learn as much job-related information about applicants and employees as possible. Employers generally have an affirmative obligation to act reasonably with regard to hiring and supervising employees. Regarding hiring, employers have a duty to exercise reasonable care when researching particular applicants. This means that employers typically have an obligation to do a reasonable investigation of the employee, including job qualifications, work history, and personal character. The employer has a similar obligation with regard to supervising and retaining current employees (AmJur2d Employment, 2009). These obligations may compel employers to "Google" employees (i.e. search the Internet) for information about job applicants and even current employees to avoid subsequent liability should they discover material which indicates that the applicant or employee is unfit for the job. "Googling job applicants offers a compelling substitute for a reference, as a search is more likely to reveal (snippets of) the character of the applicant" (Sprague, 2008: 399).

On the other hand, some practitioners advise against searching the Internet for information about applicants and employees. One employment attorney stated that "it's unlikely employers are going to learn a good deal of job-related information from a Facebook page they won't learn in the context of a well-run interview, so the potential benefit of doing this sort of search is outweighed by the potential risk" (LegalBlogWatch, 2009: 1). This may be especially true when considering that employers continue to have traditional avenues through which to investigate applicants. If

employers do search applicants' OSN sites, they should document a legitimate business reason for rejecting applicants who have been researched on the Internet, and perhaps even disclose the practice to job applicants and employees before doing the search (LegalBlogWatch).

At-will Employment

An analysis of employment law and employee rights typically begins with the doctrine of employment-at-will. In general, employees in the United States are employed at will, which generally means they may be fired for any reason or no reason at all (Gutman, 2003; Sprague, 2008). This means that an employer may generally have the right to refuse to hire a job applicant or to terminate an existing employee based upon information publicly posted by or about the applicant or employee on Facebook or another OSN site.

However, most states recognize two or three common law exceptions to employment-at-will. For instance, a majority of states recognize a public policy exception which generally means that an employer may not take any adverse action against a job applicant or employee for reasons that violate official public policy. A second exception prohibits employers from terminating an employee in violation of an express or implied contract of employment (Gutman, 2003). Finally, in a small handful of states, employers are prohibited from taking action against an employee that violates an implied covenant of good faith and fair dealing. Generally, courts have applied the implied covenant of good faith and fair dealing to situations in which the employer gave the employee a benefit, such as sick or personal leave, and then treated the employee unfairly for taking advantage of the benefit the employer provided (Lee, Thue, et al., 2009).

Of these three common law exceptions, violation of public policy is the most likely to apply to a situation in which the employer relies upon information posted by or about the applicant or employee on the Internet (Gutman, 2003; Lichtenstein and Darrow, 2006; Patel 2007). The public policy exception encompasses several different scenarios: whistle-blowing, exercise of a statutory right, performance of a statutory duty, or a refusal to break the law (Zehrt, 2010). This means, for instance, that an employee who posts public information about the employers' illegal activity on the employee's personal OSN site, or who mentions being called to jury duty (a typical statutory duty) may be protected from retaliation for such posts (Gutman).

With regard to whistle-blowing in particular, many federal statutes specifically provide protection for employees against retaliation for reporting the employer's illegal behavior. Zehrt reports that "[a]lmost all of the federal civil rights statutes enacted in the twentieth century contain specific provisions protecting employees from retaliation" (Zehrt, 2010; 152). For instance, the Occupational Safety and Health Act (OSHA) (2006), National Labor Relations Act (NLRA) (2006), Employee Retirement Income Security Act (ERISA) (1974), Family and Medical Leave Act (FMLA) (1993), and Sarbanes-Oxley Act (2002) all contain provisions that protect employees from retaliation for simply opposing an unlawful practice and for participating in an investigation, hearing, or proceeding regarding the unlawful act.

A small handful of states have limited the application of the at-will employment doctrine by providing specific protection to employees for private legal behavior. For instance, North Dakota and Colorado have enacted statutes which protect employees from adverse employment action for any off-work activities which are otherwise legal and which do not have a negative impact on the employer's business. However, these statutes typically contain a business-related exception which can be far-reaching. As Sprague points out, "[i]mportantly, all of these statutes also condition the conduct of not having any connection with the employer's business concerns. An employer could argue that information derived about a candidate, from the Internet, had a direct correlation to the employer's business since it was used in the hiring decision. …Today's employer may argue it has a legitimate business interest in whether its employees are publishing pictures on the Internet of themselves drinking excessively" (Sprague, 2008; 415). Marsh v. Delta Airlines (1997) provides an example of this. In Marsh, the Colorado Supreme Court held that an employee who was terminated after openly criticizing the employer in a letter to the editor of a local paper was not wrongfully discharged because the letter was a breach of the employee's duty of loyalty to the employer and was thus work-related.

An employee's duty of loyalty extends beyond a mere duty to refrain from publicly embarrassing the employer. Lee, Thue, et al, point out that: According to the Restatement (Third) of Agency, the duty of loyalty is broad and includes both the duty of obedience and confidentiality. Modern law also interprets the duty of loyalty to include an obligation to refrain from acting in a manner that would adversely impact an employer's interests. …an employee may also be in breach of the duty of loyalty where he has engaged in '[h]armful speech, insubordination, neglect, disparagement, or disruption of employer-employee relations…,' or where he brings 'dishonor to the business name, product, reputation or operation.' In fact, the prevailing rule directs that an employee breaches the duty of loyalty by merely criticizing the employer's products or services. …In sum, in most cases, an employer is

justified in terminating the employee for publishing negative or confidential employer information on the Internet (Lee, Thuet al, 2009: 411-12).

Discrimination

Many federal discrimination statutes, such as Title VII of the 1964 Civil Rights Act (1964), the Americans with Disabilities Act (ADA) (1990), and the Age Discrimination in Employment Act (ADEA) (1967), protect employees and job applicants from discrimination on the basis of personal characteristics, status, and religious beliefs. Various state statutes also protect employees from discrimination on the basis of a wide variety of personal characteristics such as marital status, political affiliation, sexual orientation, and veterans' status (DeCenzo and Robbins, 2010). Employers who access an applicant's Facebook or other OSN page may in, many circumstances, discover information that human resource experts routinely advise employers not to ask about in an interview. Personal OSN pages, such as those on Facebook or MySpace, typically reveal all sorts of information about the user's characteristics, some of which may be protected.

For instance, the applicant may reveal information about her marital status, political affiliation, and religious beliefs. Photos may show the applicant's race, age or gender. Evidence of a possible disability may be available. An employer who has access to such information may find it difficult to avoid relying on it when making employment decisions. As Byrnside states, "employers that make hiring decisions based on applicants' social networking profiles may find it difficult to defend against a claim that this information was used as the basis for their hiring decisions. This would be particularly true if it was found that applicants with a certain characteristic of a protected class - race, sex, age, or disability - were being systematically refused by employers who viewed applicants' social networking profiles at the earlier stages of the application process" (Byrnside, 2008: 463).

Privacy

Privacy is perhaps the most common legal and ethical issue raised in discussions of employers who search the Internet for information on employees and applicants. Invasion of privacy suits generally involve a claim that the defendant intruded into an area in which the plaintiff had a reasonable expectation of privacy (Brandenburg, 2008; Byrnside, 2008), and may take one or more of three possible forms: intrusion upon solitude or seclusion, public disclosure of private facts, or publicly placing an individual in a false light (Gabel and Mansfield, 2003). Recent literature suggests that intrusion upon seclusion is likely the most appropriate tort applicable to situations in which employees have been terminated because of personal social networking (Lichtenstein and Darrow, 2006).

In related cases regarding online communication such as computer Internet access and work e-mail systems, most courts have held that employees do not enjoy a reasonable expectation of privacy in these areas because the employer has legitimate interests for monitoring this type of workplace activity, such as protection of property rights, managing employee performance, and protecting employees from workplace harassment (Sprague, 2007). This attitude is likely to apply to social networking as well. The following statement by Sprague (2008) is indicative of the prevailing opinion. "Current privacy law suggests that a job applicant who posts embarrassing or personal information on a blog or within a social networking site which can be accessed by anyone with an Internet connection should have no expectation of privacy, and therefore, no recourse, when that publicly-available information is viewed, and potentially used, in an employment decision" (Sprague, 2008: 407).

The limited available case law indicates fairly clearly that employees who willingly post personal information on the internet, even on a personal OSN page which allows access to only friends or others in the user's contact list, do not have a reasonable expectation of privacy in that material. For instance, in U.S. v. Gines-Perez (2002), the U.S. District Court in Puerto Rico considered whether a criminal defendant whose image was posted on his employer's public website had a reasonable expectation of privacy in that image. The Court held that "[a] reasonable person cannot place 'private' information - such as a 'private' photograph - on the Internet, if he or she desires to keep such information in actual 'privacy.' A reasonable person does not protect his private pictures by placing them on an Internet site" (Gines-Perez, 2002: 225).

More recently, in Moreno v. Hanford Sentinel, Inc., (2009), the California Court of Appeals wrestled with the question of whether publishing information on a social networking site could be considered private if the intent was to reach only a limited audience. In Moreno, the plaintiff posted content about her hometown on her personal MySpace page, which was available only to those she granted access. When the principal of her former high school submitted her post to the local newspaper as a letter to the editor, attributed to the plaintiff, the community responded with violence and death threats against the plaintiff and her family, who subsequently closed the family business and then sued the defendant and school district for invasion of privacy and infliction of emotional distress. In language

similar to the court's in Gines-Perez, the Moreno court ruled against the plaintiff's privacy claim, noting that an individual who published information on the Internet could not have a reasonable expectation that it would remain private, despite the fact that she anticipated only a limited audience (see also Dexter v. Dexter, 2007).

Thus, while many applicants and employees who participate on an OSN site may believe they have created a reasonable expectation of privacy by relying upon the privacy settings the site provides them, the law does not appear to support such a claim, absent some additional facts suggesting employer wrongdoing. As discussed below, an invasion of privacy claim may succeed if the employer goes beyond a general Internet search for public information and gains access to the employee's OSN page through illegal means.

Unauthorized Access - Stored Communications Act

The Stored Communications Act (SCA) (2000) prohibits any person from intentionally accessing a "facility through which an electronic communication service is provided" without authorization. Two federal courts have considered the definition of "authorized user" in cases in which an employer gained access to an applicant's or employee's personal OSN account through questionable means.

In Konop v. Hawaiian Airlines (2001), a Hawaiian Airlines pilot (Konop) created a Website through which he and other employees criticized Hawaiian Airlines' handling of its negotiations with the pilots' union. Only those Konop approved and provided with a password could access and make comments on the site. The site's terms and conditions specifically prohibited any Hawaiian Airlines management from accessing it, and also prohibited approved users from sharing information found on the site with outsiders. When two Hawaiian Airlines pilots gave their username and password to the President of the company, who then accessed the site several times without Konop's permission, Konop sued Hawaiian Airlines claiming, among other things, violation of the SCA. Noting that the SCA provides protection only to authorized users of an internet service, the court held that the Vice President was not such an authorized user and, as such, violated the SCA when accessing Konop's site through the other pilots' user information.

More recently, in Pietrylo v. Hillstone Restaurant Group (2009), the U.S. District Court of New Jersey considered an issue similar to that in Konop. In Pietrylo, a group of employees created a MySpace page for the purpose of criticizing the employer. The defendant employer was not an authorized friend of the site and so requested, and received, the login information from another employee, who testified at trial that she felt as though she was required to provide that information as part of her job. The court upheld the jury's decision that the defendant's access of the site was not authorized because the employee was "coerced" into provide the information, and thus the employer violated the SCA.

It is important to make clear that Konop and Pietrylo apply only to situations in which the information was not available to the employer by other means. If the information is publicly available, even though the employer gained unauthorized access, the employee's claim might fail because the employee was still in control of the information and chose to post it on a quasi-public forum (Byrnside, 2008). Also, the SCA is unlikely to apply to situations in which an employer actually hires students or other young people demographically similar to job applicants for purposes of "friending" the applicants to gain access to their sites. This type of sleuthing, while possibly unethical (see below), is not likely to violate the SCA because the applicant willingly allowed access to the "spy" (Brandenburg, 2008).

Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) (1970) may provide an applicant a cause of action in a limited number of circumstances in which the employer hires a third party to conduct a background search of the applicant. The FCRA provides that job applicants must be notified when employers hire a third-party company to conduct a background check of the applicant. The FCRA is not likely to apply in those cases in which the employer does the Internet searching itself. "However, if an employer hires a third party to search applicants' profiles, the employer would be bound by the provisions of the FCRA. While the FCRA would not prohibit employers from using the information found in applicant profiles, it would at least require the employer to inform applicants that such an investigation would occur and that information from the investigation resulted in the adverse employment decision" (Byrnside, 2008: 465-66). The FCRA may also be applicable in those situations previously mentioned in which the employer hires outside "sleuths" to connect with job applicants by becoming "friends" of the applicant.

Labor Law

In Konop (2000), discussed above, the 9th Circuit Court of Appeals also considered whether the employee's use of an e-bulletin board to criticize the employer Hawaiian Airlines' negotiations with the pilot's union violated the

Railway Labor Act (RLA). Because Konop provided access to the site to other Hawaiian Airlines employees who also used the site to comment on the negotiations, the court held that the site was a form of concerted activity protected by the RLA. The Konop holding could easily be applicable to an OSN or other Internet sites as well, provided that more than one employee has access to the site and is contributing comments (Strege-Flora, 2005).

Employer Vicarious Liability

Employers would also be wise to consider their potential vicarious liability for posts an employee makes on a personal networking site. Employees who post defamatory or confidential information about others might subject the employer to liability if a court finds that the employee was acting within the course and scope of employment at the time. Even posts made on an employee's personal social networking page might create employer liability if the employee posted the comments during the time and place of work or by using employer resources, or if the employer's neglect of the employee's work performance "made the activity possible" (Gutman, 2003: 151). Employee posts could also give rise to a cause of action against the employer for intentional infliction of emotional distress (Gable and Mansfield, 2003) or criminal liability (Gutman).

Defamation

Although unlikely, employers should consider the possibility that an applicant denied a job based upon information the employer discovers about the applicant on the Internet could sue the employer for defamation. For instance, if a company relies upon inaccurate information to make an employment decision and shares that information with others, the denied applicant could have a valid defamation claim (Byrnside, 2008).

Legal Summary

In summary, the legal issues employers may face as a result of employees' Internet and social networking use are myriad and complex. It remains unclear how traditional law will apply to this relatively new source of information for employers. To avoid legal liability, employers may wish to implement a social media policy, such as the sample found in Figure 1. This may be especially important in light of the various ethical issues employee social networking may raise, as the next section discusses.

Ethical Issues

Laws and ethics are often closely linked but they involve different goals. Laws provide stability to social institutions. Individuals are penalized for specific acts that do not conform to the published rules. In contrast, ethics involve questions regarding why and how people should behave. They promote social ideas more than laws do (Candilis, 2002). Ethical issues go beyond legal concerns by focusing on the duties society expects of its members (Sims, 2003). Ethical questions frequently arise when existing law is inadequate to address new circumstances, such as the issues related to OSNs. Both legal and ethical considerations are needed to draft adequate employee handbook policies regarding OSNs.

The purpose of this part of the paper is to raise and discuss the ethical issues surrounding employees' and job applicants' use of OSNs. This portion of the paper is divided into two sections: those ethical issues which point in favor of employers' research of employees' private social network sites and those issues which point against such use. A sample employee handbook statement associated with OSN use also is provided.

Ethical Benefits

Source of Recruits

According to Rosen (2010), about 75% of companies research the Internet and social networking sites for recruiting and selection purposes. According to Olson (2007), job candidates may use social networking sites as resume banks for searching for education, experience, and other skills.

Source of Information

Employers can use OSN sites for selection to see what online behaviors current and potential employees exhibit.

A relevant part of the interview process is to look at applicants in nonformal situations. With such a large investment in employees, the nonformal lifestyle might be a make or break issue to increase the chance of having the employees conform to the culture of the company and to reduce the chance of negligent hiring (Brandenburg, 2008).

Accuracy

Another argument for relying upon an employee's or applicant's social networking is to consider cross-reference accuracy. Beyond the resume and application form, employers need many ways to check applicants such as employment history, credit reports, and criminal activity (Kaupins and Park, 2010).

Spotting Inappropriate Behavior

Employers also have a simple legitimate interest in employees' personal online behavior while at work. Numerous examples show up on the Web. Copyright violations, pornographic, obscene, or sexually explicit material, inflammatory language, cyberbullying, and language or images that advocate violence or discrimination toward other people are among the few examples of inappropriate behavior. Employers need to monitor such behavior and provide appropriate discipline (Bissonette, 2009; Kist, 2010; Nitzschke, 2006). Use of social networking sites might reduce the chance of negligent hiring if employers find potential illegal, unethical, unsafe, or dangerous behaviors in a social network that is backed up by hard outside evidence (Kaupins and Park, 2010). Employees might provide confidential information about their organization such as passwords, financial secrets, inventions, marketing programs, and business strategies. Warnock (2007) revealed that about 10% of organizations studied the unauthorized disclosure of financial information via message boards and blogs. Password revelations can lead to considerable hacking of corporate internal operations and Websites (Kaupins and Minch, 2006).

Marketing

Companies have been known to use social networking sites to market their products and services. They can create company communities on Facebook, post locally relevant updates and photos, read what company fans say about themselves to get clues about their needs, and provide incentives not only to visit the page but to buy the company's products or services (Quigley, Summerfield, and Tarbox, 2010).

Politics

Facebook has been instrumental in helping Harvard students share political opinions since 2004. It also helped Columbians lead a campaign against guerillas known as the Revolutionary Armed Forces of Columbia (known by its Spanish initials - FARC). OSNs can potentially allow employees to air negative actions by management. According to Zuckerberg, founder of Facebook, a more transparent world might be governed better (Kirkpatrick, 2010).

Ethical Problems

Questionable Accuracy

Social networking sites do not offer any guarantee that information posted on them is accurate, which can lead to legal and ethical hiring issues. Many sites do not have a verification process, and nearly all allow users to create profiles in another person's name. Even factual information on a social networking site can be taken out of context (Kaupins and Park, 2010).

Subjectivity

Screening employees based upon information found on social networking sites may not be objective. Not all job applicants engage in social networking, and those who do often use different sites, each of which has different features and purposes. Thus, fair and equal treatment of job candidates may be difficult (Kaufman, 2008).

Irrelevant Information

According to Kaupins and Park (2010), employers can easily discover job applicants' identity in terms of age, citizenship, disability, gender, genetic information, marital status, national origin, pregnancy, race, color, religion, sexual orientation, and veteran's status though social networks. In addition to legal issues that may arise, as discussed previously, this may also pose ethical concerns for the employer.

Loss of Company Secrets

Current employees may post company secrets such as passwords, new products, or prototypes on their personal network sites. They may also defame competitors, clients, employees, suppliers, customers, or franchisers, or misuse proprietary information of clients (Bauer, 2010). Other inappropriate posts may include employee secrets such as passwords or other personal information, personal customer or stockholder information, such as Social Security numbers, and possibly inside information regarding ongoing labor negotiations. Employers who conduct regular Internet research of employees may discover and demand immediate removal of this type of information, thus limiting the potential damage.

Privacy

Many social networks are intended for personal use, especially popular sites such as Facebook and MySpace. The personal and professional lives of job candidates might be considerably different. Employers can find out about an employee's interests, friends, and a host of other personal information that would not be related to the workplace (Whittier, 2006). Moreover, employees and applicants may purposely refuse to friend bosses to protect their privacy. Some companies have engaged in the practice of hiring young people, often college students, to "friend" applicants on behalf of the employer, who then has potentially unethical access to the applicant's personal OSN page (Brandenburg, 2008).

Reduced Productivity

Employers may certainly have a legitimate business reason to search when employees are engaging in personal social networking. According to Woolnough (2008), the time employees waste on social networking sites is a main concern of 69% of employers. In addition to the simple personal activities employees engage in on social networking sites at work, they could also social networking at work to find other jobs. According to Gaudin, the use of Facebook in businesses cuts "an average of 1.5% in total employee productivity, according to a new report from Nucleus Research, an IT research company. The survey of 237 employees also showed that 77% of workers who have a Facebook account use it during work hours" (Gaudin, 2009: 1). Moreover, about 87% of those employees claim to have no legitimate business use of the site while on working hours.

Ethics Summary

In spite of social networking's association with recruiting, marketing, and monitoring company information and employees, employers should be concerned about questionable accuracy, loss of company secrets, privacy violations, and decreased employee productivity. The foregoing discussion of the ethical considerations raised by employee social networking makes clear that appropriate employee monitoring and discipline are important. Employers would be wise to develop and enforce clear social media acceptable use policies, as discussed in the next section.

Social Media Acceptable Use Policies

A Peacock (2008) study found that 69% of companies seek more control over employees' use of the Internet. Of those, approximately 50% have considered limiting Internet use to lunch times, and 33% have considered completely banning the personal use of the Internet at work. Seventy percent reports that they would consider discipline if they saw inappropriate photos on social networking sites that somehow reveal the employer.

Deciding on whether to limit social networking inside the business is a function of the strategy of the business, potential positive opportunities, potential negative threats, and managerial ethical preferences. Management leadership styles may range from having complete control over employees by banning social networking to giving

employees free range by offering few restrictions. The strategy of the business might allow considerable social networking inside and outside of the business not only because of the positive ethical considerations, as discussed above, but also because of the enormous amount of outside contacts and input it can create. Marketing opportunities are also significant. Potential negative aspects include legal problems with trade and discrimination laws and ethical problems with inaccuracy, subjectivity, false information, and lack of privacy.

Whatever the case, given the increasing prevalence of social networking use, and the potential benefits employers may enjoy, companies should take strategic advantage of such use and create policies to keep up with social networking software challenges. According to Arnold (2009), when drafting such policies, employers should consider the restrictions on employees (the specific behavior both condoned and prohibited), employer monitoring, reporting violations, discipline, and acknowledgements. Below are some examples of major policy provisions developed by Winter Wyman Companies described in Arnold (2009).

General Provisions

Employees should be restricted in their company-related personal use of social media applications, which are numerous. Such applications include Facebook, MySpace, Twitter, LinkedIn, Wikipedia, YouTube, Yelp, Flickr, Second Life, Yahoo groups, Wordpress, ZoomInfo, Internet forums, blogs, online profiles, podcasts, e-mail, instant messaging, music-sharing, and voice over IP.

Training

All employees should be informed of organizational policies and be trained on the proper use of social networks. The training could also involve employee monitoring, reporting violations,

Employee Monitoring

Employees should have no expectation of privacy associated with the use of any social media applications. The company has a right to monitor anything on the Web.

Reporting Violations

Employees should report any violations of company social networking policy to their supervisors, managers, or HR department.

Discipline for Violations

The company should reserve the right to discipline employees concerning their behavior on social networks. Discipline may include oral warnings, written warnings, suspension, or discharge. The company should also reserve the right to take legal action for inappropriate Internet behavior by employees.

Acknowledgement

Employees should sign an agreement acknowledging they have read and understood the employer's social networking policy (Winter, Wyman Companies 2009).

Given the major issues shown above, Figure 1 reveals sample social networking policy statements. To avoid legal and ethical problems, corporations should consider implementing this or a similar statement.

Figure 1: Sample Social Networking Policy Statements

1. If you have a personal social network and discuss job related materials about the company, identify yourself as a company employee and inform readers that your views do not necessarily match the views of the company.
2. All posts must be truthful.
3. If there are any testimonials concerning endorsing products or services, endorsers must disclose information showing the endorsement relationship (receiving the product for free or being paid to endorse).
4. Make sure that the message about the company is consistent with other messages related to the company.

5. Ensure that all parties associated with social media within the organization are trained to appropriately use the media.
6. You might have to make a disclaimer that your views do not necessarily represent the company's views. The views expressed on this website are mine and may not reflect the views of my employer.
7. Employees who have personal social media pages should ensure that such activity does not interfere with work. Employees may express their views as long as they don not conflict with company policies.
8. Employees may engage in social media activity during work if it is directly related to their work, approved by their manager, and does not reveal company clients, customers, or vendors without express permission.
9. Show respect for vendors, customers, managers and employees.
10. Employees may write about their jobs in general but should avoid disclosing confidential information
11. Do not post any financial, confidential, sensitive, or proprietary information about the company.
12. Employees should comply with all laws regarding their behavior, not just with social-media use.
13. Provide respect for current, former, and potential customers, employees, and competitors.
14. Social networks should not be a place to share personal complaints.
15. Forward unfavorable opinions or statements post about yourself or the organization to the human resources department.
16. Do not post obscenities.
17. If you have an in-house policy prohibiting anything other than neutral recommendations, posting online recommendations should be prohibited.
18. Do not post socially unacceptable or criminal behavior such as sharing information about sex or criminal accomplishments such as stealing from the company (Arnold, 2009; Bauer, 2010; Bissonette, 2009; Churches et al, 2010; Manafy, 2010).

Future Research

This study discussed many of the legal and ethical issues associated with social networking. Much of the focus of this research has been on major federal laws and court cases. Future research should update current federal law and also focus on state, municipal, and international law. The ethics research included some anecdotal and empirical studies. There will be many more studies analyzing organizational attitudes and behaviors. For example, a researcher could gather data on cases in which employees were terminated based on social network use to analyze increasing trends over time. Employers could be surveyed regarding their reactions to various types of information found about an employee such as race, religion, political affiliation, binge drinking, and other characteristics. Their reactions could affect hiring, compensation, training, and other human resource dimensions of an organization.

Summary

Social networking will be a major challenge for employers. Not only does it provide vital ethical benefits such as improving recruiting, enhancing safety and security, improving accuracy of information, enhancing discipline, and providing inexpensive yet useful marketing, but also it can create significant legal and ethical challenges such as invasion of privacy, discrimination, inaccuracy, and subjectivity. Companies must ascertain how they respond to employee social networking use by examining their corporate strategy, balancing the opportunities and threats of social networks, and by considering their ethical values. A policy might provide employee restrictions, employer monitoring, reporting violations, discipline, specific behavior condoned and forbidden, and acknowledgements.

References

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

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

AmJur 2d. (2009). Employment relationship, 27, §§ 392-97.

Arnold, J. 2009. Twittering and facebooking while they work: Set clear guidelines about the use of social media in the workplace. **HR Magazine**, 54: 53-55.

Bauer, M. 2010. I know I need a social media policy: Now what should it say? **Franchising World**, 42: 1.

Bissonette, A. 2009. **Cyber law: Maximizing safety and minimizing risk in classrooms**. Thousand Oaks, CA: Corwin.

Boyd, D., & Ellison, N. 2007. Social network sites: Definition, history, and scholarship. **Journal of Computer-Mediated Communication**, 13: 210-230.

Brandenburg, C. 2008. The newest way to screen job applicants: A social networker's nightmare. **Federal Communications Law Journal**, 60: 597-626.

Byrnside, I. 2008. Six clicks of separation: The legal ramifications of employers' using social networking sites to research applicants. **Vanderbilt Journal of Entertainment and Technology Law**, 10: 445-477.

Candilis, P. 2002. Distinguishing law and ethics: A challenge for the modern practitioner. **Psychiatric Times**, 19. Retrieved September 8, 2005 from http://www.psychiatrictimes.com/display/article/10168/48616?pageNumber=1.

Churches, A., Crockett, L., & Jukes, I. 2010. **The digital diet: Today's digital tools in small bytes**. Thousand Oaks, CA: Corwin.

DeCenzo, D., & Robbins, S. 2010. **Fundamentals of human resource management**. Hoboken, N. J.: Wiley.

Dexter v. Dexter. 2007 WL 1532084 (Ohio App. 11 Dist.).

Employee Retirement Income Security Act. 18 U.S.C. § 1001 et seq (1974).

Fair Credit Reporting Act. 15 U.S.C. §§ 1581 et seq (1970).

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).

Fletcher, D. 2010. Friends without borders. **Time Magazine**, May 31: 33.

Gabel, J., & Mansfield, N. 2003. The information revolution and its impact on the employment relationship: An analysis of the cyberspace workplace. **American Business Law Journal**, 40: 301-351.

Gaudin, S. 2009. Facebook cuts workplace productivity - survey. **Computerworld**, 25: 17.

Gely, R., & Bierman, L. 2006. Workplace blogs and workers' privacy. **Louisiana Law Review**, 66: 1079- 1110.

Greenbaum, W., & Zoller, B. 2006, July/August. Court decisions impact workplace internet and e-mail. **HR Advisor**.

Gutman, P. 2003. Say what?: Blogging and employment law in conflict. **Columbia Journal of Law and the Arts**, 27: 145-185.

Kaupins, G., & Minch, R. 2006. Legal and ethical implications of employee location monitoring. **International Journal of Technology and Human Interaction**, 2: 16-35.

Kaupins, G., & Park, S. 2010. Legal and ethical implications of corporate social networks. **Employee Responsibilities and Rights Journal**, Forthcoming.

Kirkpatrick, D. 2010. **The Facebook effect: The inside story of the company that is connecting the world**. New York: Simon & Schuster.

Kist, W. 2010. **The socially networked classroom: Teaching in the new media age**. Thousand Oaks, CA: Corwin.

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

Lee, K., Thue, M., Oldham, J., & Stephenson, T. 2009. An exercise for teaching the employment law implications of employee blogging. **Journal of Legal Studies Education**, 26: 399-431.

LegalBlogWatch. 2009). **Do employers using Facebook for background checks face legal risks**? Retrieved August 3, 2010 from http://www.legalblogwatch.typepad.com/legal_blog_watch/2008/03/do-employers-us.html.

Lex, R. 2007. Can MySpace turn into my lawsuit?: The application of defamation law to online social networks. **Loyola of Los Angeles Entertainment Law Review**, 28: 47-70.

Lichtenstein, S., & Darrow, J. 2006. Employment termination for employee blogging: Number one tech trend for 2005 and beyond, or a recipe for getting Dooced? **UCLA Journal of Law and Technology**, 10: 4.

Manafy, M. 2010. Social web etiquette. **EContent**, 33: 1.

Marsh v. Delta Airlines. 952 F. Supp. 1458 (D. Colo, 1997).

Millier, S. 2009. The Facebook frontier: Responding to the changing face of privacy on the internet. **Kentucky Law Journal**, 97: 541, 544.

Milligan, T. 2009. Virtual performance: Employment issues in the electronic age. **Colorado Lawyer**, 38: 29.

Moreno v. Hanford Sentinel. 172 Cal.App. 4th 1125, 91 Cal.Rptr. 3d 858 (2009).

National Labor Relations Act. 29 U.S.C. §§ 151 et seq (1947).

Nitschke, B. 2006, June. Investigating staff misuse of district technology. **School Administrator**, 63: 8.

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

Patel, B. 2007. Myspace or yours: The abridgement of the blogosphere at the hands of at-will employment. **Houston Law Review**, 44: 777.

Peacock, L. 2008. Employers watch Facebook usage. **Employers Law**, 4.

Pietrylo v. Hillstone Restaurant Group. 2008 WL 6085437 (D.N.J.).

Quigley, K., Summerfield, B., & Tarbox, K. 2010. Tech it up a notch, 9 strategies for doing more with the technology and web sites you already use. **Realtor Magazine**, September 10: 20-24.

Rosen, J. (2010, July 25). The end of forgetting. **The New York Times Magazine**.

Sanders v. American Broadcasting Companies. Inc., 978 P.2d 67 (1999).

Sarbanes-Oxley Act. 18 U.S.C. §§ 2510 et seq (2002).

Sims, R. 2003. **Ethics and corporate social responsibility: Why giants fall**. Westport, CT: Praeger.

Sprague, R. 2008. Rethinking information privacy in an age of online transparency. **Hofstra Labor & Employment Law Journal**, 25: 395.

Sprague, R. 2007. Fired for blogging: Are there legal protections for employees who blog? **University of Pennsylvania Journal of Labor and Employment Law**, 9: 355.

Stored Communications Act. 18 U.S.C. §§ 2701 et seq (2000).

Strege-Flora, C. 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.

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

U.S. v. Gines-Perez. 214 F.Supp.2d 205 (2002).

Warnock, O. 2007. Networking or not working? **Contract Journal**, 440: 31-32.

Whittier, D. 2006. Cyberethics in the Googling age. **Journal of Education**, 187: 1-86.

Woolnough, R. 2008. Get out of my Facebook. **Employer's Law**, May: 14-15.

Zehrt, L. 2010. Retaliation's changing landscape. **George Mason University Civil Rights Law Journal**, 20: 143.

Gundars Kaupins is department chair and professor of management at Boise State University. He received his Ph.D. in human resource management from the University of Iowa and is a certified senior professional in human resources. He teaches human resource management, labor relations, and compensation. His publications include over 300 articles in job evaluation, training and development, Baltic studies, and human resource ethics in journals such as the Academy of Management Perspectives and International Journal of Technology and Human Interaction.

Susan Park is a legal studies lecturer at Boise State University. She received her J.D. (summa cum laude) from the University of Idaho College of Law. She has taught legal environment of business, commercial law, and human resource law. Her current research interests include the use of social media in the workplace, employee privacy, and discrimination. Before teaching at Boise State, Professor Park was a law clerk at the Idaho Supreme Court and an attorney in private practice in Boise, Idaho.