ISSUE

Selected, Edited, and with Issue Framing Materials by:
Gina Vega, *Organizational Ergonomics*

Is Employer Monitoring of Employee Social Media Justified?

YES: **Brian Elzweig and Donna K. Peeples**, from "Using Social Networking Web Sites in Hiring and Retention Decisions," *SAM Advanced Management Journal* (2009)

NO: **Steven Greenhouse**, from "Even if It Enrages Your Boss, Social Net Speech Is Protected," *The New York Times* (2013)

Learning Outcomes

After reading this issue, you will be able to:

- Explain why discussing the workplace using personal social media can cause problems resulting in harm to others.
- Explain what ethical values are needed when making choices to post photos or blogs that place the workplace in a bad light.
- Understand the differences between Elzweg and Peeples's and Greenhouse's positions on the rights involved in social media, as well as the prudence involved in social media.
- Distinguish between colorful social media posts and harmful social media produced by individuals in the workplace.
- Discuss how the individual and the corporation can be helped by ethics rather than law on this issue.

ISSUE SUMMARY

YES: Brian Elzweig and Donna K. Peeples write that although employers do need to be respectful of their employees' privacy, they also have the responsibility to avoid negligent hiring and negligent retention. They find that the monitoring an employee's, or a potential employee's, social media is a viable way to avoid these potentially serious problems. This is not to say that an employer's monitoring of social media should be without limits. Special care should be taken in respect to state privacy laws regarding the protection of employees outside of company time.

NO: Steven Greenhouse explains that new findings from the National Labor Relations Board state it is illegal for employers to fire employees based on social media posts. Often when an employee begins a job, part of the policy discussion revolves around social media use. In the majority of cases, the employee is told not to post materials that make the firm, the employer, and other employees appear in a bad light. It appears that many firms should begin rewriting their policy manuals based on the findings from the National Labor Relations Board as well as state law.

The social networking website Facebook has recently faced ups and downs. Facebook's creator, Mark Zuckerberg, and the site's tumultuous beginnings were the subject of an award-winning movie, *The Social Network*, and the site globally reached the 500-million-user milestone and shows no signs of slowing its growth. The only slow growth is fiscal, after a disastrous public offering in 2012. However,

sites like Facebook, such as Twitter, MySpace, and personal blogs, allow their users to stay in touch with friends and family as well as make new connections by posting photos, messages of varying length, and comments to other users' sites. As these forms of social media grow in size and number, so do the questions of their appropriate use by the creators and receivers of the information. Although the previous generation's employee privacy ethics focused on issues such as e-mail privacy, the advent and growth of this new use of the Internet has made employer monitoring of employees' social networking the twenty-first century's central employee privacy issue.

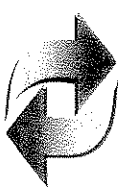
Although social networking has proven to be a useful tool for many companies, creating another inexpensive way to advertise products and events is not without drawbacks. Time wasted by employees updating their personal sites on company time has led many businesses to block access to such sites on work premises to maintain a productive environment. Although this step seems reasonable to most, it is not the only way a company's interests can be affected by an employee's decisions regarding social media. Disgruntled and careless employees have been known to take to their personal sites to air their grievances and share possibly damaging company or client information. This leads many to ask, should an employee's use of social media outside of the office affect his or her job?

With a plethora of personal information not normally found on a résumé or application now readily available with the click of a mouse, more and more employers are using social media in hiring and employee-retention decisions. As a result, as social media use increases, so has the number of people fired or passed over for jobs because of information found on their personal sites not directly related to their job. Items such as questionable photos and personal, defamatory remarks about their bosses and co-workers have been causes of dismissal.

Although social media has been used to help businesses identify which employees could prove to be a liability to the company, employer perusal of these sites can itself prove to be a liability. As mentioned previously, these sites often contain information not asked for on job applications, often times for legal reasons. A person's social profile, whether blatantly or by association with certain groups, can often contain information about one's religion, sexuality, gender, disabilities, or other indicators of minority status.

These sites have a myriad of ways to personalize security and block unauthorized persons from viewing profiles, or even just pieces of information. In their privacy policy, Facebook reminds us that one should "Always consider your privacy settings before sharing information on Facebook." With these layers of protection, can privacy be expected on the Internet, or considering the wise words of Benjamin Franklin, can three people keep a secret only if two of them are dead? Is the use of these settings a legitimate claim to privacy, or simply a false comfort?

While reading the YES and NO selections, consider whether information on the Internet can truly be considered as private. Does an employer have a right to access employee information on social media sites if precautions have not been taken to otherwise prevent their access? And should employers disclose their intention to use information found on social media sites?



YES

Brian Elzweig and
Donna K. Peeples

Using Social Networking Web Sites in Hiring and Retention Decisions

Social networking Web sites are a relatively new format that allows people to post personal information to be viewed by "private" friends and the public as well. Managers may wish to access these sites, with or without permission, and use that information in hiring and retention decisions. Managers may, in fact, be required to monitor employees' social networking sites to defend against the possibility of negligent hiring and retention lawsuits being filed against their companies. However, use of this information must be weighed against the expectation of privacy by the person posting the information. A better understanding of the law can provide guidelines of when and how managers may access this information, thus avoiding liability for invading the privacy of current or potential employees.

An Interesting Example of What Not To Do

Many people have heard stories about how some employees have lost their jobs because of what they posted on a social networking Web site. For example, Stacy Snyder (*Snyder v. Millersville University*, 2008), student at Millersville University, was dismissed from her job as a student teacher at a high school and denied her teaching credential when officials from the university were made aware of a photograph and a post on her MySpace.com (hereinafter MySpace) site.

The post also included what the *New York Times* described as a "surprisingly innocuous" picture containing a head shot of Ms. Snyder wearing a pirate hat while drinking from a plastic cup. In a self-titled caption she called the photograph "drunken pirate" (Stross, 2007). Nicole Reinking, who was Snyder's coordinating teacher at Conestoga Valley High School (CV), had been critical of Snyder's classroom performance and professionalism (*Snyder v. Millersville University*, 2008).

Millersville University claimed that Ms. Snyder's dismissal was due to her competency as a teacher; however, the court held that her dismissal was based at least in part on the MySpace posting. Millersville University stated that the photograph was "unprofessional" and may "promote underage drinking." The college also claimed that Ms. Snyder was in violation of a section of the teacher's handbook requiring teachers to be "well groomed and appropriately dressed" (Stross, 2007). Snyder sued Millersville University alleging that her "First Amendment right to free expression protected the text and photograph in her . . . MySpace posting" (*Snyder v. Millersville University*, 2008). The United States District Court for the Eastern District of Pennsylvania ruled that Snyder was acting as an employee of CV, not as a student at Millersville University, when she was a student teacher. In doing so, the court denied her First Amendment claim stating that Snyder "was a public employee . . . when she created her MySpace posting, [therefore] she would be obligated to show that the posting related to matters of public concern to receive First Amendment protection" (*Snyder v. Millersville University*, 2008).

Snyder's case illustrates a dilemma facing many managers today and gives rise to important questions. First, may information available on a personal Web site be legally used in decisions relating to hiring or other employee decisions such as retention? Second, if such information may be used legally, should a manager seek this information and act on it? These fairly new questions are exacerbated by the prevalence of social networking sites and the potential wealth of information contained on them. Some interesting findings are:

- According to Ipsos Insight's (2007) latest "Face of the Web" study, social networking is becoming the dominant online behavior. The study found that 24% of American adults have visited a social networking Web site, with two thirds visiting within the 30 days previous to the polling. This usage is even higher in other countries such as South Korea, where 49% of adults had visited a social networking site at least once (Ipsos Insight, 2007).

Elzweig, Brian; Peeples, Donna K. From *SAM Advanced Management Journal*, Autumn 2009, pp. 27–35.

- The two most popular social networking sites are MySpace and Facebook.com (Facebook) (Hitwise, 2008).
- In May of 2008, Facebook had 123.9 million unique visitors and MySpace had 114.6 million (McCarthy, 2008).
- The fastest growing demographic on Facebook is those who are 25 years old and older (ComScore, 2007).
- More than half of its users are over age 35 (Comscore, 2006).

With this many users, most of whom have their own Web page, it would seem that for a manager who is trying to hire the best employees, these sites (along with hundreds of smaller ones) are a veritable treasure trove of information (Boyd and Ellison, 2007). Ostensibly, information that is not available on a résumé may be available on a job candidate's Web site. The problem for managers, however, is that while they may want to mine the sites for information about a candidate, the site's creator may have a legal right to privacy, and there may also be problems with accuracy of data obtained.

Can Managers Use Social Networking Web Sites in Hiring Decisions?

According to a recent survey by Careerbuilders.com,

- 22% of hiring managers used social networking Web sites to screen job candidates, double the amount from two years ago.
- Of those using the sites for screening, 34% reported that the information obtained caused them not to hire a particular candidate.
- 24% found content favorable to the candidate in their hiring decision.
- The number of hiring managers using social networking Web sites is likely to increase in the future as 9% who reported not using them planned to do so in the future (Grasz, 2008).

Since this has become a source of information, would a manager be remiss in *not* using these sites? Before deciding, managers should address some liability issues that generally revolve around the expectation of privacy.

Right to Privacy—Or Not?

In this age of information, especially information posted on the Internet by private individuals, should there be an expectation of privacy? Does utilizing the Web sites' privacy settings create an expectation of privacy? These are not simple questions with answers fully tested in the courts.

Whether or not there is an expectation of privacy may depend on how the user's account is set up and the information provided by the site regarding the conditions of privacy. Both Facebook and MySpace allow a user to set up a private site so that only those given permission by the user should be allowed access. It has been suggested that Snyder's biggest mistake was "not knowing or choosing to turn on any sort of privacy controls on her social network profile page . . . which would have prevented anyone except those who were accepted as Snyder's friends, [anyone who had been granted access, and those exempted by the terms of service/use], to have access to the items she posted. Facebook also offers extensive privacy controls that should be configured" (Perez, 2008).

This answer appears overly simplistic. While there is probably no expectation of privacy for a user who does not use privacy settings, a general expectation cannot be relied upon just by using the privacy settings.

Terms of Service—The Great Unread Section

When joining either MySpace or Facebook, the user must agree to the terms of service and to the Web sites, privacy policies. These policies weaken a user's argument that just setting the site's privacy control functions guarantees privacy. The Facebook Principles notes that: "Facebook helps you share information with your friends and people around you . . . And you control the users with whom you share that information through the privacy settings on the Privacy page" (Facebook Principles). This is contrasted later in the policy:

> You post User Content . . . on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other Users with whom you may choose to share your pages and information. Therefore, we cannot and do not guarantee that User content you post on the Site will not be viewed by unauthorized persons. We are not responsible for circumvention of any privacy settings or security measures contained on the Site. You understand and acknowledge that, even after removal, copies of User Content may remain viewable in cached and archived pages or if other Users have copied or stored your User Content. (Facebook Principles).

MySpace goes further in its safety settings noting that: "Every profile has the option of being 'private.' This means that only you and those you have added and

approved as friends can see the details of your profile, including your blog, photos, interests, etc." (MySpace safety tips and settings: Safety settings).

That is contrasted with specific warnings in another part of the same document:

> *Don't forget that your profile and MySpace forums are public spaces. . . . Don't post anything that would embarrass you later.* It's easy to think that only our friends are looking at our MySpace page, but the truth is that everyone can see it. Think twice before posting a photo or information you wouldn't want your parents, potential employers, colleges or boss to see!" (MySpace safety tips and settings: General tips). [Emphasis added].

Is "Privacy" a Misnomer on Social Networking Sites?

Web sites themselves recognize that setting privacy options to limit access to a social networking site does not prevent all unwanted users from seeing the site's content. It has been suggested that hiring companies can access applicants' sites in a variety of ways. Facebook allows college students to give blanket access to anyone in their college. Recent graduates who remain active in their college's social network may become useful to their new employer because of their access to the Web sites of students still attending the school from which they graduated. Some companies may also hire current students who can access their peers' social networking profiles (Brandenburg, 2008). While searching for a specific person on both Facebook and MySpace, even before becoming a "friend" and being able to access a person's private site; certain information is still shared with the default settings. A user's "profile picture" (the picture that identifies their page) is available, as well as place of residence. MySpace also identifies the person's age, and Facebook shows other networks they are affiliated with (which can relate to work, hobbies, interests, politics, and a myriad of other things). In addition, Facebook allows someone doing a search to access the "target's" list of friends. Thus, a hiring company could ask a third party to access a potential hire's Web site for them.

Is There Tort Liability for Invasion of Privacy?

No case law directly addresses the point of whether there is an expectation of privacy on a social network Web site. Analogies must be made from case law as to expectations of privacy in other areas. The right to bring a private action for invasion of privacy was first discussed in legal literature in an 1890 *Harvard Law Review* article by Samuel Warren and Louis Brandeis. This article led to courts creating tort claims for invasion of privacy (Warren and Brandeis, 1890). The seminal case in this area is *Katz v. United States*, in which the Supreme Court first recognized that "the Fourth Amendment protects people, not places." The issue in the Katz case was whether a wiretap of a telephone booth could be used as evidence against [Katz] the defendant, who was on trial for illegally transmitting bets or wagers by wire. The defendant argued that he had an expectation of privacy in the telephone booth; therefore, a warrant would be needed. In a concurring opinion that found for the defendant, Justice Harlan laid out the test for when a search and seizure requires a warrant: "There is a twofold requirement, first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable" (*Katz v. United States*, 1967).

The basic principle in Katz has been tested in the context of cyberspace, but not specifically in the context of social networking Web sites. In *United States v. Maxwell*, the Court of Appeals for the Armed Forces examined the expectation of privacy as it pertained to e-mail communications. The court contrasted e-mail, if considered to be the equivalent of first-class mail and telephone conversations—both with high expectations of privacy—with e-mail if considered to be "postcards," which have lower expectations of privacy. In addition, the court also noted that if the e-mail communication was sent to a chat room then the public at large would have access—much like placing a letter on a public bulletin board. Once the communication is given public access, then the expectation of privacy would be eliminated (*U.S. v. Maxwell* as discussed by Hodge, 2006). However, other courts have not found a blanket expectation of privacy in e-mails after they are sent, noting that the recipient should be figured into whether there is still an expectation of privacy (*U.S. v. Charbonneau* as discussed by Hodge, 2006).

Cases such as these would surely be used by a court determining if there is a reasonable expectation of privacy for a person's social networking site. The court should take into account that with a social network site, the user permits many people to have access. If access is allowed to some people, it is hard to know how a court would rule on a claim of privacy if the people who were allowed access gave other people access. However, it should also be noted that a person who took steps to ensure privacy, such as enacting privacy settings within their Web site, would

have a higher expectation of privacy than those who did not (Brandenburg, 2008).

It has been suggested by Brandenburg (2008) that the following elements would be relevant in deciding whether or not a person using a social networking site would have a reasonable expectation of privacy:

1. Whether privacy settings are available;
2. Whether the social networker attempted to or did enable the privacy settings;
3. The level of privacy the networker attempted to or was able to set with an eye to the spectrum of privacy settings and measures available to the social networker;
4. The kinds of people and groups to whom that networker chose to disclose the information he or she later claims to be sensitive and private; and
5. Whether the unwanted or unauthorized person who accessed the networker's information was able to happen upon the information or had to hack through security measures to find the information (Brandenburg, 2008).

The question that has not been answered yet by the courts is how these factors would withstand scrutiny under the Katz test. Katz requires that the person claiming privacy must have a subjective expectation of privacy. It is hard to tell where the courts would draw the line to say that expectation was met. The more effort a user of a social networking site expends in attempting to maintain privacy the more likely the court will find that the first part of the Katz test was met. However, a court would most likely consider these elements in light of the user agreement and would have to decide if any privacy claims would be waived by that agreement. In addition, these elements do not address the second part of the Katz test. A court may see the pervasiveness of social networking Web sites as society accepting their use. Some courts may see this as society accepting the use of these sites to disseminate private information, and so the expectation of privacy would be reasonable. However, other courts may see examples like Snyder's as a warning. The more public stories there are about people having adverse employment decisions, the more likely it is that a court would rule that expecting privacy is not reasonable.

Stored Communications Act

In addition to the potential tort liability for invasion of privacy, another area of concern for managers is the Stored Communications Act (SCA) (18 U.S.C. §§ 2701–2711 (2000). The SCA makes it illegal to "intentionally access without authorization a facility through which an electronic communication service is provided" (18 U.S.C. §§ 2701(a)(1)). However, the SCA has a specific exception for "conduct authorized . . . by a user of that service with respect to a communication of or intended for that user . . ." 18 U.S.C. §§ 2701(c)(2). Questions arise as to what would qualify as conduct "authorized by a user" under the SCA. Certainly a user of a social networking Web site who allows access by designating others as "friends" would be authorizing their use. However, more questionable would be whether someone who was not granted access, such as an employer, was given information that was accessed by a "friend." Since the original person was authorized, the exception would probably apply. However, if an employer were to hack into a site without permission of the networker, then that employer would probably have liability under the SCA (Brandenburg, 2008).

Does the Right to Privacy Extend to Off-duty Current Employees

Davis (2007) has suggested that there should be an expectation of privacy for off-duty conduct of current employees, and that this expectation of privacy should extend to employees' social networking habits. The analysis is based on the issuance of lifestyle protection laws and some specific federal laws suggesting that once a person leaves work, they "expect to be let alone" (Davis, 2007). These laws soften the traditional employment-at-will doctrine available in most states. Two states, Colorado and North Dakota, have enacted broad protection for current employees. Colorado code states that it is a

> discriminatory or unfair employment practice for an employer to terminate the employment of any employee due to that employee's engaging in any lawful activity off the premises of the employer during nonworking hours unless such a restriction . . . [r]elates to a bona fide occupational requirement or is reasonably and rationally refted to the employment activities and responsibilities of a particular employee or a particular group of employees, rather than to all employees of the employer (Colo. Rev. Stat. Ann. § 24-34-402.5 (2008)).

Similarly, in North Dakota,

> [i]t is a discriminatory practice for an employer to fail or refuse to hire a person; to discharge an employee; or to accord adverse or unequal

> treatment to a person or employee with respect to application, hiring, training, apprenticeship, tenure, promotion, upgrading, compensation, layoff, or a term, privilege, or condition of employment, because of race, color, religion, sex, national origin, age, physical or mental disability, status with respect to marriage or public assistance, **or** *participation in lawful activity off the employer's premises during nonworking hours which is not in direct conflict with the essential business-related interests of the employer . . .*" (N.D. Cent. Code § 14-02.4-03 (2008). [Emphasis added].

Davis (2007) notes that other states have also enacted less broad protections for off-duty conduct, such as New York, which protects off-duty conduct including legal recreational activities, consumption of legal products, political activity, and union membership. In addition "[o]ther states have enacted much more limited statutes protecting specific categories of lawful off-duty conduct and lifestyle, including consumption of tobacco products, sexual orientation, and marital status" (Davis, 2007).

Using these examples and the rationale that people have an expectation of privacy outside of the workplace, Davis concludes that "[i]n a world where people simply have begun to conduct much of their social lives over the Internet, the same expectations apply: an employer should not be snooping into an employee's personal life when it has nothing to do with business" (Davis, 2007). This may be correct, but courts have interpreted what is considered to be "related to," "in direct conflict with the essential business-related interests of the employer," or other similar language. In *Marsh v. Delta Airlines,* Marsh, a Delta Air Lines baggage handler wrote a letter to the editor [of] the *Denver Post* that criticized Delta. He was subsequently fired due to the publication of the letter (Marsh, 2007). Marsh then sued, claiming he was wrongfully terminated under the Colorado lifestyle statute. The court held in favor of Delta stating that there "is an implied duty of loyalty, with regard to public communications, that employees owe to their employers" (Marsh, 1997). In finding that Marsh violated the implied duty of loyalty, his firing was justified as this duty was a *bona fide* occupational requirement as contemplated in the exception to the broad-reaching Colorado statute. The court interpreted the statute to protect off-duty privacy as a shield for employees who are engaged in activities that are legal but are distasteful to their employers, such as homosexuality or political affiliation.

In the only case interpreting the North Dakota statute, a chaplain was fired from his job after it was revealed that he was caught masturbating in an enclosed public restroom of a department store. The chaplain claimed that he had broken no law since the enclosure prohibited him from being found guilty. The court held that it is a factual dispute whether this behavior was unlawful. If it is not, the court implied that the statute may protect him since it "may fit the protected status of lawful activity off the employer's premises" (Hougham, 1998).

The off-duty lifestyle statutes seem to protect activities that are completely divorced from the employer in that to protect an employee they must take place off-site, during nonworking hours, and have no relationship to the employer's interests (Sprague, 2007). Even if there is an expectation of privacy, the legitimate needs of the employer may override. The cases in which employers have been found to invade privacy are ones in which the "employer has pried into the employee's life far beyond a legitimate business need" (Sprague, 2007).

While there is a suggestion that there should be an expectation of privacy for off-duty social networking, outside of the exceptions noted, no laws make it illegal to search an employee's *publicly available social networking Web site.* Still, since the argument relating to the public or nonpublic nature of information on a social networking site is not clearly settled, employers using such information may be doing so at their own peril. On the other hand, an employer *not using* such information may create liability by the "negligent hiring" or "negligent retention of an individual." A negligent hiring claim suggests that at the time an employee was hired, it was negligent for an employer to engage the employee's services based on what the employer knew or should have known about the employee (*McGuire v. Dean J. Curry,* 2009). Negligent retention liability is typically predicated on an "employer . . . placing a person with known propensities, or propensities which should have been discovered by reasonable investigation, in an employment position in which, because of the circumstances of the employment, it should have been foreseeable that the hired individual posed a threat of injury to others" (*Mandy v. 3M,* 1996). The negligent retention occurs "when, during the course of employment, the employer becomes aware or should have become aware of problems with an employee that indicated his unfitness, and the employer fails to take further action such as investigating, discharge, or reassignment" (*Mandy v. 3M,* 1996).

> It is important to note that the tort[s] of negligent hiring and retention [are] based on the principle that a person conducting an activity through employees is subject to liability for

> harm resulting from negligent conduct "in the employment of improper persons or instrumentalities in work involving risk of harm to others." (quoting [in part] Restatement (Second) of Agency [s]ection 213(b) (1958)). . . . The duty to hire employees who are competent and not dangerous is, by its very nature, a duty of a master or employer, and this duty is nondelegable. . . . Thus, the liability of an employer for the negligent supervision or hiring of an unfit employee is an entirely separate and distinct basis from the liability of an employer under the doctrine of *respondeat superior*. (*Magnum Foods, Inc. v. Continental Cas. Co.*, 1994 (*original citations deleted*).

Negligent hiring and negligent retention only require constructive notice of the employee's propensity to cause injury and can be imputed to an employer who fails to take reasonable care in determining an employee's fitness for a position. The more contact an employee has with the public, the higher this duty to investigate becomes (*McGuire v. Dean J. Curry*, 2009). This would make it dangerous for an employer *not* to check any information to which the organization could have access. The evidence for negligent hiring and negligent retention claims can come outside of the theory *respondeat superior*. Therefore, the evidence that may be used to show that someone was negligently hired or retained may come from actions that happened outside of the scope of employment. As such, they are attractive to plaintiff's lawyers, and the number of these claims has increased in recent years (Richmon, 2001).

While there is little case law on social networking Web sites themselves, courts are increasingly looking for evidence that may be obtained from the Internet. Courts are recognizing "Googling" and "Internet searches" on parties as part of a due diligence search for missing defendants and have overturned cases when this was not done. Practitioners have warned that to find potentially relevant evidence lawyers need to look past traditional avenues and should include social networking Web sites in their search for evidence (Levitt and Rosch, 2007). Language on the sites tends to be frank and graphic and often includes pictures that show very well to juries. To effectively represent a party, an attorney needs to know what has been posted on the Internet and should assume that if it were posted publicly, the other party already has it. Once something has been posted on the Internet, it is difficult to remove all traces of it (Menzies, 2008). However, since the Katz analysis allows for a subjective expectation of privacy as one part of the test, a user believing that the information was erased may persuade a court that the privacy expectation exists.

It appears that courts, when determining whether an employer had constructive notice of information that could lead to a negligent hiring or negligent retention claim, need to examine the ease of availability of the information. Similarly, a job applicant's expectation of privacy would probably depend on similar factors that were discussed previously. Managers, it would seem, may have an affirmative duty to at least check for information available to the general public on social networking Web sites, but the practice may be considered an invasion of privacy if they were to hack into a private site without permission. However, managers should be cautioned to check their state's privacy and lifestyle laws before making any decisions that affect employment, since violation of these may create liability for the employer. Even if the employer is in a state with broad privacy and lifestyle rights (Colorado and North Dakota), managers should search for public information on their employees. Those states, as well as states with limited protections, allow exceptions to the lifestyle provisions for *bona fide* conflicts with the employer's business. It would seem that if Snyder had been in one of those states, as a teacher, her actions may still have been directly contrary to the employer's business. For example, if she were to have hurt a student while intoxicated, her MySpace posting would have been strong evidence against the school board in a negligent retention lawsuit.

Penalties for Invasion of Privacy

If a court were to hold that the social networker had an expectation of privacy for his or her Web site, and an employer used this in making a negative employment decision, the potential employer could be liable for the invasion of privacy. The employer may also subject itself to an action for wrongful termination of a current employee. Kirkland suggests this would be a proper remedy for employees who are fired for blogging (a similar activity using a social networking Web site) on their own time (Kirkland, 2006). In addition, it should be noted that the two states that have blanket privacy and lifestyle rights both enacted them as part of the state's anti-discrimination statutes. Courts looking for guidance may use this persuasive authority to help determine a penalty. As such, the penalty for invading the privacy of an employee, and using the information gained to make a negative hiring decision, could subject the employer to penalties similar to those found in discrimination cases, which are indeed substantial.

Other Potential Problems

The Potential for Liability for Discrimination

As discussed, information may be made available about a specific job candidate by searching their MySpace and Facebook accounts. On many social networking sites, information available without being a "friend" include a user's profile picture (usually the user's picture), age, networks in which they are members (which could include religious, political, sexual orientation, and other interests of the user), as well as other information. This information would not appear on a traditional job résumé and could lead to discriminatory acts. Many questions that are not typically asked in interviews, since they may lead to discriminatory hiring practices, may be answered by the job candidate's social networking site. The profile picture may tell the employer the candidate's sex or race, and other information may give clues about the candidate's religion or national origin. Using information gained from the social networking Web site in hiring decisions could run afoul of Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act, the Americans with Disabilities Act, or state discrimination laws. The social networking Web site may reveal information that would show a candidate to be in a protected class or category. Since this information is now provided prior to seeing a candidate face to face, the candidate could be passed up for an interview based on one of those factors. Human resource managers must have procedures in place to ensure that this does not occur (Davis, 2007). Evidence of an employer routinely checking potential job candidates' social networking profiles could easily be used to make a case for discrimination if they do not have enough workers who are members of protected classes.

The Possibility for Inaccurate Information in an Employment Decision

Another problem for potential employers is that the information contained in a social networking site may be false or inaccurate. One commentator imagines a scenario where a candidate is competing for a highly coveted job, knowing that the employer may do an online search of the candidates. The candidate then makes a Web site containing false or misleading information about one of the competitors for the job. The competitor may be eliminated from consideration without knowing why and may never know of the false information (Davis, 2007). Even without malicious intent, a manager's biases may come into play. If there is a picture of a job candidate drinking, will the manager think that person is an alcoholic? If a person is pictured holding a hunting rifle, is that person homicidal or a member of a militia? The manager's biases, triggered by one picture or bit of information, could wrongly frame his or her entire view of the candidate (Davis, 2007). Even the 24% of employers (Grasz, 2008) who made positive employment decisions based on a social networking Web site could be doing this on misinformation. A site that shows great communication skills or looks very professional may not have been designed by the person who owns it. Many people hire others to make their Web sites.

Additionally, information may be posted about a candidate by someone else, and the candidate themselves may not know about it. Both MySpace and Facebook allow "friends" to post things on other "friends" sites. The owner of the site can remove the posts, but the manager may see it before the candidate does. Any of the above scenarios, and many others, could allow a hiring manger to make adverse employment decisions using inaccurate information.

What Now?

Reviewing the current information on social networking sites and applying it to good business practices, it would appear that an employer would be remiss if the Internet was *not* routinely searched for information regarding *potential* employees. Searching for information on *current* employees may be constrained by the time and effort required. Certainly if there is a reason to update information, such as a transfer, promotion or a behavior issue, a search would be to protect the organization. The following are suggestions for employers before accessing and using information obtained from the Internet.

- Check social networking sites before making employment decisions in order to gain important information—good or bad.
- Verify accuracy of the information gathered.
- Recognize the purpose of the sites. Do not have unrealistic expectations of propriety.
- Consider the age of the employee or potential employee.
- Develop clear policies and procedures regarding use of social networking sites. Clearly disseminate this information to employees.
- Post information regarding your potential use of social networking sites on your job postings and application forms.
- Have employees and persons seeking employment sign consent forms prior to accessing information.

- Check state statute for privacy and lifestyle laws. Many states have some protections even if there is not a blanket protection for off-duty conduct.
- Train all employees on the important issues discussed in this paper.

Conclusion

With social networking Web sites becoming more prevalent, especially among individuals in the workforce, use of them is becoming more common in employment hiring and retention decisions. Since social networking sites are relatively new to users as well as employers, there are many issues to consider before using them for employment decisions. Employers should take steps to avoid invading privacy or committing discriminatory acts in using the sites, but should not fear using them if they have a legitimate interest at stake. These Web sites contain a treasure trove of publicly available information. Employers may be at risk if they *do not*, in fact, check for publicly available information on their current and potential employees. Employers should also take steps to ensure the accuracy of the information gathered. In addition, employees and job seekers should be put on notice that employers are using these sites to gather information and should assume that nothing posted on them is actually kept private.

References

Boyd, D. M., and Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), article 11.

Brandenburg, C. (2008). The newest way to screen job applicants: A social networker's nightmare. *Federal Communications Law Journal, 60*(3), 597.

Colo. Rev. Stat. Ann. B 24-34-402.5 (2008).

ComScore press release: Facebook sees flood of new traffic from teenagers and adults (2007, July 5). Retrieved December 19, 2008 from http://www.comscore.com/press/release.asp?press=1519

ComScore press release: More than half of MySpace visitors are now age 35 or older, as the site's demographic composition continues to shift. (2006, October 5). Retrieved February 4, 2009 from http://www.comscore.com/press/release.asp?press=1019

Davis, D. (2007). My Space isn't your space: Expanding the fair credit reporting act to ensure accountability and fairness in employer searches of online social networking services. *Kansas Journal of Law and Public Policy, 16,* 237.

Facebook Principles (n.d.). Retrieved on January 21, 2009 from http://www.facebook.com/policy.php

Grasz, J. (2008, September 10). One-in-five employers use social networking sites to research job candidates, CareerBuilder.com survey finds. Retrieved December 18, 2008 from http://careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr459&sd=9%2f10%2f2008&ed=12%2f31%2f2008&siteid=cbpr&sc_cmp1=cb_pr459_

Hitwise US-Top 20 websites-October, 2008. Retrieved December 18, 2008 from http://www.hitwise.com/datacenter/rankings.php

Hodge, M. (2006). The fourth amendment and privacy issues on the "new" internet: Facebook.com and MySpace.com. *Southern Illinois University Law Journal, 31,* 95.

Hougam v. Valley Memorial Homes, 1998 ND 24 (Supreme Court of North Dakota 1998).

Ipsos Insight Marketing Research Consultancy: Online video and social networking websites set to drive the evolution of tomorrow's digital lifestyle (2007, July 5). Retrieved December 18, 2008 from http://www.ipsosinsight.com/ pressrelease.aspx?id=3556

Katz v. United States, 389 U.S. 347 (1967).

Kirkland, A. (2007). You got fired? On your day off?! Challenging termination of employees for personal blogging practices. *University of Missouri Kansas City Law Review, 75,* 545.

Levitt, C., and Rosch, M. (2007, February). Making internet searches part of due diligence. *Los Angeles Lawyer, 29,* 46.

Magnum Foods, Inc. v. Continental Cas. Co., 36 F.3d 1491 (United States Court of Appeals for the Tenth Circuit 1994).

Mandy v. 3M, 940 F. Supp 1463 (United States District Court for the District of Minnesota 1996).

Marsh v. Delta Air Lines, 952 F. Supp. 1458 (United States District Court for the District of Colorado 1997).

McCarthy, C. (2008, June 20). ComScore: Facebook is beating MySpace worldwide.

CNet News. Retrieved from http://news.cnet.com/830113577_3-9973826-36.html

McGuire v. Dean J. Curry, 766 N.W.2d 501 (Supreme Court of South Dakota 2009).

Menzies, K.B. (2008, July). Perils and possibilities of online social networks. *Trial, 44,* 58.

MySpace safety tips and settings: General tips. (n.d.). Retrieved on January 21, 2009 from http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safety_pagetips

MySpace safety tips and settings: Safety settings. (n.d.). Retrieved on January 21, 2009 from http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safety_pagetips & sspage=4

N.D. Cent. Code B14-02.4-03 (2008).

Perez, S. (2008, December 5). Social network profile costs woman college degree. *Read Write Web*. Retrieved from http://www.readwriteweb.com/archives/social_network_profile_costs_woman_college_degree.php

Richmon, A. (2001). Note: restoring the balance: Employer liability and employer privacy. *Iowa Law Review, 86*(4), 1337.

Snyder v. Millersville University, Civil Action No. 07-1660, 2008 WL 5093140 (E.D. Pa December 3, 2008).

Sprague, R. (2007). From Taylorism to the Omnipticon: Expanding employee surveillance beyond the workplace. *John Marshall Journal of Computer & Information Law, 25*(1), 1.

Stored Communications Act, 18 U.S.C. BB 2701–2711 (2000).

Stross, R. (2007, December 30). How to lose your job on your own time. *The New York Times*. Retrieved from http://www.nytimes.com/2007/12/30/business/30digi.html

United States v. Charbonneau, 979 F. Supp. 1177 (United States District Court for the Southern District of Ohio 1997).

United States v. Maxwell, 45 M.J. 406 (United States Court of Appeals for the Armed Forces 1996).

Warren, S.V. and Brandeis L.D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193.

Brian Elzweig is an assistant professor of business law at Texas A&M—Corpus Christy. Elzweig holds a JD from California Western School of Law and an LLM from the Georgetown University Law Center.

Donna K. Peeples is an associate professor of management at Texas A&M—Corpus Christie. Peeples holds an MBA from Texas A&M and a PhD from Texas A&M—Corpus Christie.