Social Networking Web Sites: The Legal and Ethical Aspects of Pre-Employment Screening and Employee Surveillance

Renee L. Waring and F. Robert Buchanan
University of Central Oklahoma

ABSTRACT

The education of human resource practitioners requires cutting edge knowledge that may be in advance of developments in the law. Such is the example of usage of Online Social Networks (OSNs) in screening job applicants and current employees. Many organizations inquire into the off-duty behavior of workers in this fashion and are not in violation of existing laws. There are, however, potential legal challenges on the horizon based on workers' reasonable expectations of privacy, pointing toward the need of a legitimate business rationale for rejecting applicants based on information that was not visible from the application and interview process. Implications and recommendations for practitioners are offered.

INTRODUCTION

Cyberspace has provided an enormous opportunity for people to meet each other and to share personal details. Private information that workers make public through such services as Facebook, MySpace, and numerous weblog providers is being utilized by a growing number of recruiters, potential employers and current employers who seek additional information regarding after-work behavior of employees (Roberts & Roach, 2009). In teaching HR at the university level, it has been observed that realism is essential to being prepared to be a competent practitioner (DeGroot, Stambaugh, & Owen, 2009; Rudin, Byrd, & Fleming, 2009). Additionally, some of the issues being faced are ahead of legal developments and may be ethically challenging.

Online Social Networking Web Sites (OSNs) are growing at a staggering rate. Facebook added 50 million users in a 100 day period in 2009 (Smith, 2009). Facebook's registered users now number over 350 million, making it the leading online social networking site (Facebook Statistics, 2009). Their monthly viewers of 97 million have surpassed 2008's leader MySpace by more than 30 million viewers (eMarketer, 2009). Hi5 has 50 million monthly visitors. Internationally, Mixi in Tokyo has 19 million members and Maktoob, an Arabic OSN has 13 million users (Schonfeld, 2009). With such large numbers, it is clear that online social networking sites play prominent roles in people's everyday lives. The use of these sites extends beyond simply "befriending" people to extensive personal networks that seek information about employers, employees and job opportunities (Kiviat, 2009; Limbach, 2008).

When individuals choose to use social networking sites for both personal and professional purposes, issues arise regarding the nature and amount of information shared. While some social networkers tightly control information about themselves, others provide full access to anyone on the internet. MySpace pages are open to the public with correspondence, photos, demographics profiles, sexual orientation, and smoking/drinking habits. A study of 200 Facebook profiles found that 53 percent included photos involving alcohol use and 50 percent posted revealing information. Easy access to "friends" groups is likely to allow profiles to be accessed by casual acquaintances, families and even prospective employers (Peluchette & Karl, 2010).

Human resource management practices and policies have not kept pace with the rapid use and abuse of social networking websites used for job searches, background checks and employee surveillance. With unemployment rates in the United States hitting a 16-year high, employers are faced with a swell of job applicants and larger pool of qualified candidates vying for open positions (Scherzer, 2009). While employers may enjoy having access to a greater number of resumes, now more than ever they have stakeholder obligations to ensure that they are hiring the most qualified personnel and that they know exactly who they are hiring. Human resource professionals and business owners are turning to internet searches to find out more about potential employees – and finding more personal information than they should legally be knowledgeable of just by Googling their names. According to a 2007 survey, 44 percent of employers used social networking sites such as Facebook to screen job candidates (Recruiting inside, 2009). A 2009 survey by CareerBuilder.com (2010) also found that more than half of those managers chose not to hire an applicant after viewing their online profiles.

Selection of the right employee is critical for several reasons. Those with the right attributes contribute the most to productivity. The cost of hiring the wrong employees and having to retrain and rehire continues to rise exponentially as well as costs of loss related to employee theft, vandalism, absenteeism and hostile work environments. Careful selection is also important because of the legal implications of incompetent selection. Courts will find employers liable when employees with criminal records or other problems exploit positions of employment to access clients' homes or to find other opportunities to commit crimes within the employer's organization against other employees. Hiring workers with documented or observed aggressive backgrounds that place others in danger is considered to be "negligent hiring." Avoiding negligent hiring claims requires taking "reasonable" action to investigate the candidate's background. Employers must make a systematic effort to gain relevant information about the applicant, verify documentation, follow-up on missing records or gaps in employment, and keep a detailed log of all attempts to obtain information (Dessler, 2009).

The purpose of this paper is to define the phrase "taking reasonable action" in light of the information availability on social networking web sites. The two major categories of concern reside in both the legal and ethical aspects of personnel screening practices and policies. In looking up information on the internet, employers need to be aware of potential claims against them such as federal discrimination and invasion of privacy.

TAKING REASONABLE ACTION

Discrimination

Unless employers have clear anti-discrimination policies, they are vulnerable to charges that they are using information viewed on OSNs to cull minorities, homosexuals and other applicants who are members of a protected class. According to Matthew Effland (2010), there has been no decision so far that says using information available on web sites is a violation of employee rights because the internet is considered public domain, but warns that law will soon catch up to technology.

It is presently not illegal to know about a job candidate's marital status or religion or race, color, age or national origin or even an applicant's political activities so long as employers can prove that this knowledge was not used to discriminate. Any rejection based upon this knowledge must be defended as bona fide occupational requirements. Employers should have a policy in place that details what the purpose of the internet search is and that specifically spells out that the firm does not base its decision on demographic data that would not appear on a resume or application form. Proof of legitimate rationale for rejecting applicants should be documented.

Unfair Inferences

Hiring decisions based on information that is not part of the application or interview presents a possible charge of unfair inference. Principles of unfair inference prohibit information from witnesses as being considered factual unless it can be shown that the information is relevant and accurate (A party's failure, 2004). Whether from traditional hearsay or in the use of OSNs, not all information can be considered truthful or accurately depictive. Sites such as YouTube and MySpace have few content requirements, and nearly all sites allow users to make up a profile for other individuals. When evidence appears before a jury, it is essential to instruct them to consider all relevant information from a witness and the circumstances, particularly if the witness is not present (*Crosby v. Beaird*, 1983). As unfair inference arises from concepts of missing witnesses (Ross, 2002), it is unlikely that OSNs will be successfully implicated in hiring decisions involving information posted about individuals. In invoking this charge, the OSN would have to possess additional information relevant to the case (*Zeeck v. Melina Taxi Co*., 1991; *Chandler v. Flynn*, 1985), and OSNs do not compile additional information about users.

Use of Information

Risk factors to employers in using information from OSNs include noncompliance with Fair Credit Reporting Act (FCRA) regulations and Equal Employment Opportunity Act (EEOC) guidelines. The Society of Human Resource Management (SHRM) maintains that once the candidate has been met, employers are obligated to consider the "whole of an applicant." This would include using all viable resources in getting some sense about an applicant's character and the soundness of their decision making (Fishman, 2009). However, SHRM cautions that most OSN sites have no verification process and some can be edited or receive contributions from anyone with access to the internet. A recent example of this would be pictures appearing on a

website showing Olympic Gold Medalist Michael Phelps smoking marijuana. This was a youthful indiscretion made permanent in cyberspace for all to see. The question is how long should an applicant be penalized for lack of judgment? The Phelps photos appeared just to commemorate a "party" but were eventually utilized to result in a negative image of one of the most successful athletes in US Olympic history.

Legally, privacy in the U.S. is covered under the Fourth Amendment. Individuals are protected from illegal search and seizure and guaranteed due process unless information is found in plain view. Information obtained from OSNs is not considered an illegal search of a person's private information because it is found in plain view in a public forum (Lane 2006). Eugene Spafford (2010), information specialist at Purdue suggested that students not commit anything to cyberspace that they would not commit to print in a hometown newspaper. Spafford projected that the problem will only compound in the future as the capacity for information storage and retrieval expands.

Privacy, Social Networking and Employee Surveillance

Little empirical research has been related to technology and privacy issues, especially as it applies to employee spying. However, numerous anecdotal and opinion articles explain the negative aspects of increasing worker scrutinization by human resource management professionals. When contemplating issues of privacy, there are two important considerations: the intent of the information shared and the expectation that it will remain private (Hodge, 2006). This differs from e-mail, where the sender intends the information to be sent to a specific individual, although this information too can be accessed by others. Therefore, much of what is posted on an OSN is public and cannot be assumed private even though intended for specific readership.

Individuals think that the First Amendment protects their rights to post information on a social networking site. The first Amendment does protect individual rights to speak, write and gather freely so far as it does not cause harm or incite violence (Verga, 2007). A fundamental misunderstanding exists when applicants believe what they have posted on an OSN is private and protected when it is neither. An example would be an employee who posts negative comments about a boss including threats of a violent nature, on a web site that is accessible to other members of the business. The employee does have the right to post this information under the First Amendment; however, if the employer is threatened, the speech is not protected. In this situation, privacy rights are not violated because the employee chose to share the information in the open forum (Timm & Duven, 2008).

Both Facebook and Myspace provide a clear privacy statement to inform users about the limits of protection that the site maintains for the information shared, as well as how the site will use the personal information provided. These privacy policies do not delineate who can access the information provided, but do outline the actions that are taken by the site's administrators. The focus of these privacy statements is about what information will be shared with a third party but does not speak to others that may access the information posted. Little is known about whether individual users read and are aware of the privacy policies. Facebook states that it will do everything possible to protect the information posted on its sites but "cannot and will not

guarantee that user content will not be viewed by unauthorized persons" (Facebook, 2008). Facebook goes on to state "you may not want everyone in the world to have the information you share on Facebook; this is why we give you control of your information."

Ethics

Organizations have ethical obligations to their employees and business partners, customers and society, as well as to themselves. What is ethical and what is unethical? Answers are not straightforward. The increasing number of computer users, applications and systems interconnections blurs the line between authorized and unauthorized usage.

Social contract theory posits that consumers assume an implied social contract when exchanging information in a transaction (Pan & Zinchan, 2006). The theory involves three aspects of 1) individual consent, 2) agreement among the moral agents, and 3) an approach for which the agreement is made (whether actual or hypothetical agreement). Social contract theory has been applied to many situations related to business ethics. It has been used to understand situations related to risk taking, privacy and trust as well as gender issues. Some persons are comfortable with higher risk-taking, based on their assumptions toward the social contract. Acquisti and Gross (2006) found that more than 75 percent of graduating students had created a social networking profile and were posting information about themselves. This study found that web site users were more comfortable with the possible risks of their disclosures being seen by others. In addition, this study found that males were higher in risk taking behavior than females. This is consistent with the literature on risk taking behavior where adolescents or young adult men have greater risk taking behavior than women (Huang, Gupta, Derevsky, & Paskus, 2007). These demographics should be taken into consideration for purposes of using OSNs to screen workers.

The numerous ways that social web site users share ideas, pictures, and just connect with one another has become more and more pervasive. Professionals that have a thorough understanding of the "reasonable use" of the information contained on these sites are better equipped to face the ethical issues present, and identify strategies for appropriate use. The challenge for HR professionals is how to engage in either monitoring employee behavior or evaluating applicants' information in a legal, ethical and reasonable manner. Mitrano (2006) recommends that employers learn all they can about social networking sites before setting polices, educating employee, or determining expectations for background searches.

Employees should be informed that content posted on social networking sites can reflect positively or negatively on themselves or the organization. Activities they take part in through OSNs may seem innocuous, such as using LinkedIn to network professionally. However, for example, a current employer who sees a worker's profile posted might interpret it as active job-hunting.

Professionals using the network for background searches must understand that they are acting in the role of an agent of their organization. There are four factors to consider related to the identification of this role (Berg, Berquam, & Christoph, 2007).

- What an agent of the organization can examine.
- When an agent of the institution can formally report information discovered on a web site.
- The type of information that needs to be formally reported.
- What liability an agent of the organization assumes in knowing information discovered online.

It becomes critical for managers to set clear parameters for the justifications on using OSNs as investigative tools, specifying when and how the websites are to be accessed. By establishing these policies professionals may be better equipped to demonstrate compliance with EEOC and Privacy law. Additionally, they become aware of the moral aspects of evaluating workers based on the information retrieved from OSNs.

IMPLICATIONS FOR HUMAN RESOURCE POLICIES AND PRACTICES

As the economy emerges from the recession employers will begin hiring again. Every organization is unique in their hiring needs and practices. Every individual that will be considered for employment should be evaluated on their own merit, strength and weaknesses, by someone in the hiring organization that will consider the complete individual. Employers must consider that social networks such as Twitter and Facebook have no verification process and may be accessed and edited by anyone with internet access. Disturbingly, anyone can make up a profile in another's name.

Employers should remain vigilant in conducting background checks. They can continue to expect to see increases in false information from job applicants. Resume falsifications and diploma mills flourish when job seekers grow desperate to regain employment. Verification studies reveal that approximately 50 percent of resumes received have some kind of inconsistency and 17 percent of background studies conducted identified criminal activity (Fishman, 2009).

Background Screening Trends

Employers should be able to demonstrate that their knowledge of protected class demographic information regarding potential applicants is not used as a basis for hiring decisions. The EEOC frequently investigates claims of perceived discrimination in screening and hiring decisions. Employers need to ask if there is a nexus between the hiring standard and the job the individual is being hired to do. Lawyers warn of increasing numbers of "failure to hire" lawsuits if it can be proved that employers are using these sites as a tool for seeking demographic information as a basis for applicant hiring decisions. The push toward the emergence of legal parameters to control the privacy aspects of the rapid proliferation of information exchange on ONS is an observed legal trend (Effland, 2010).

The New York Times (Helft, 2010) reported on a broad coalition of advocacy groups across the political spectrum including AT&T, Google, and Microsoft named The Digital Due Process Coalition. Their intent is to push Congress to strengthen online privacy laws to protect digital information. Under a proposed set of principles, agencies would have to obtain a search warrant based on a showing of probable cause before they could obtain an individual's online

documents. In a move toward holding OSNS more accountable, a California lawsuit filed against Facebook in August, 2009 claims that Facebook violated California privacy and online privacy laws by disseminating users' posted personal information posted to third parties. The plaintiffs seek damages and attorney fees. (Facebook will fight, 2009).

Clearly, it will become increasingly more imperative that employers promulgate policies that require the agent to state the purpose of the background check before engaging in a search. Policies should mandate that there be a legitimate business rationale for the search and that hiring rejections should not result solely from information found on web sites. Employers should specify the documentation methods that will accompany retrieved information from OSNs in order to be prepared to justify hiring and/or termination decisions. The safest practice is to meet the potential candidate in person and then get a written consent that a background check will include an online search.

CONCLUSIONS

Employers should offer transparency both to potential applicants and to current employees about their screening processes and practices pertaining to their use of OSNs. MySpace and Facebook both have terms of use that talk about their noncommercial usage. Some attorneys, particularly in litigious states like California, advise complete avoidance of OSN screening during the hiring process (Genova, 2009). The fear is that unfair inference could be claimed when adverse personal information from outside sources has been utilized in evaluations. If OSN screening is to be used, it should be a recommendation for practice that background investigations do not delve so deep as to break firewalls and search the private components of OSNs.

Further research and conversation are needed on the topic of privacy, legality and ethics related to social networking web sites as guides to practice. As more legal issues come to the fore, it will be critical for professionals to stay abreast of precedents set. Most importantly, human resource professionals need to understand users' perceptions of privacy as it relates to their online activity. Likewise, workers need to be educated to apply great caution to the images and content that they allow to go out over the internet. The frightening reality is that the moment personal information goes out on the Web, it may be permanently available for anyone, anywhere to examine in whatever context the viewer desires.

Social networking online is a way technology enables users stay in touch with one another, where just a decade ago it was very different, more on a person to person basis. It is the professional's responsibility to understand the uses of this technology and the issues surrounding it. This can be accomplished by learning about the rights and responsibilities of involvement on OSNs and setting behavior standards for employees. Until the law catches up, policymakers are obligated to draw on a mature and reasoned sense of fairness and honesty. Online social networking is not just a fad and is unlikely to disappear. Issues related to user privacy and vulnerability are growing concerns that need to be addressed.

Renee L. Warning is an associate professor of management at the University of Central Oklahoma. She earned her Ed.D. in Human Resource Development from Oklahoma State University (1992) after serving as a HR professional for more than 20 years. She has been active for many years in SHRM both as a practicing professional and a student advisor. Contact: rwarning@uco.edu.

F. Robert Buchanan is an assistant professor of management at the University of Central Oklahoma. He earned his Ph.D. from the University of Texas at Arlington (2006) in HR/OB and international management. His research interests are in diversity, training & development, and globalization. Contact: fbuchanan@uco.edu.

REFERENCES

A party's failure to call a witness. 2004. *Criminal jury instructions*, New York State Unified Court system. Retrieved April 17, 2010 from www.nycourts.gov/cji/1-General/CJI2d.Missing_witness.pdf

Acquisti, A., & Gross R. 2006. *Imagined communities: Awareness information sharing and privacy on the Facebook.* Presentation at the 2006 privacy enhancing technologies workshop, June 28. Cambridge, UK: Robinson College. Retrieved April 2, 2010 from http://petworkshop.org/2006/preproc/preproc_03.pdf

Berg, J., Berquam, L., & Christoph, K. 2007. Social Networking Technologies: A Poke for Campus Services." *EDUCAUSE Review*, March–April, 32–44.

Careerbuilder.com. 2010. *Pre-Employment screening background check blog for employers, human resources and security by ESR: Statistics and employment screening background checks*, January 12. Retrieved January 23, 2010 from http://www.esrcheck.com/wordpress.

DeGroot, T., Stambaugh, J., & Owen, J. 2009. An empirical examination of the use of a simulation in teaching human resource management. *Journal of Human Resources Management, 3*(3), 1-12.

Dessler, G. 2009. *A framework for human resource management* (5th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Effland, M. S. 2010. Lawyer warns Facebook a risky tool for background checks. *Workforce Management*. Retreived April 10, 2010 from http://www.workforce.com/section/06/feature/25/45/83/254585.html.

eMarketer. 2009. *Social networking worldwide: Ad spending and usage*. Retrieved February 15, 2010 from http://www.emarketer.com/Reports/All/Emarketer_2000567.aspx.

Facebook. 2008. *About Facebook.* Retrieved January 23, 2010 from http://lhup.facebook.com/about.php.

Facebook Statistics. 2009. Retrieved January 19, 2009 from http://www.facebook.com/press/info.php?statistics.

Facebook will fight privacy lawsuit. 2009. New Zealand Herald, August 18. Retrieved April 14, 2010 from: http://www.lexisnexis.com/vortex3uco.edu2050/us/inacademic/framedo?reloadentyirepage=true&rand=12712.

Fishman, N. 2009. *Background screening trends: Social networking among issues to spark hiring controversies.* Retrieved January 22, 2010 from http://www.shrm.org/hrdiscipline/staffing management/Articles/pages/baclgroundscreening/trends.aspx.

Genova, G. L. 2009. No place to play: Current employee privacy rights in social networking sites. *Business Communication Quarterly, 72*(97), 97-101.

Helft, M. 2010. A Wide Call to Improve Web Privacy. *New York Times*, March 31, Op, 1.

Hodge, M. J. 2006. Comment: The Fourth Amendment and privacy issues on the new internet: Facebook and MySpace. Com. *Southern Illinois University Law School Journal, 31*, 95-122.

Huang, D. F., Gupta, R., Derevsky, R., & Paskas, T. S. 2007. Gambling and health risk behaviors among US college student-athletes: Finds from a national study. *Journal of Adolescent Health, 40*(5), 390–397.

Kiviat, B. 2009. Using Twitter and Facebook to find a job. *Time Magazine*. Retrieved January 19, 2009 from http://www.time.com/time/busFness/article/0,8599,1903083,00.html.

Lane, J. E. 2006. Facebook Freedom; Student speech on the internet. *ACPA Development.* Winter. Retrieved September 10, 2007 from http://www.myacpa.org/pub/develop,ents/archives/2006/winter/article.php?.

Limbach, J. 2008. *Social networking explodes as job search tool*. Retrieved January 19, 2009 from http://www.ConsumerAffairs.com.

Mitrano, T. 2006. Thoughts on Facebook. *Cornell Information Technologies*, Retrieved March 2, 2010 from http:// www. Cit.cornell.edu/policies/socialnetworking/facebook.cfm.

Pan,Y., & Zinchan, G. M. 2006. Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing, 82*(4), 33–338.

Peluchette, J., & Karl, K. 2010. Examining students' intended image on Facebook: What were they thinking?" *Journal of Education for Business, 85*, 30-37.

Recruiting inside the loop. 2009. *Lawyers warn Facebook a risky tool for background checks*. Retrieved February 15, 2010 from http://www.workforce.com/section/06/feature/25/45/83/254585.html.

Roberts, S. J. & Roach, T. 2009. Social networking web sites and human resource personnel: Suggestions for job searches. *Business Communication Quarterly, 72*(1), 110–114.

Ross, S. L. 2002. Missing witness charge. *Richmond County Bar association Journal*, Spring, 14- 15, 29-31. Richmond County Bar Association: Staten Island, NY.

Rudin, J., Byrd, K., & Fleming, R. 2009. Assessing HRM-specific knowledge. *Journal of Human Resources Management, 3*(2), 1-10.

Scherzer, L. 2009. Facebook profiles can foil job searches. *Smart Money,* January 17.

Schonfeld, E. 2009. *TechCrunch: A map of social network dominance*. Retrieved February 15, 2010 from http://techcrunch.com/2009/06/07/a-map-of-social-network-dominance.

Smith, J. 2009. Facebook crosses 250 million user mark in six months. *Tracking Facebook and the Facebook platform for developers and marketers*. Retrieved January 19, 2009 from http://www.insidefacebook.com/2009/07/15.

Spafford, E. 2010. *Purdue University News Service*. Retrieved Jan 20, 2010 from http://news.uns.purdue.edu.

Timm, D. M., & Duven, C. J. 2008. Privacy and social networking sites. *New Directions for Student Services, 124*, 89-101.

Verga, J. 2007. Policing their space: The First Amendment parameters of school discipline of student cyberspace. *Santa Clara Computer and High Technology Law Journal, 23*, 727–748**.**

Court Cases

Chandler v. Flynn, NY 111 AD2d 300, 301 (1985)

Crosby v. Beaird, NY 93 AD2d 852 (1983)

Zeeck v. Melina Taxi Co., NY 177 AD2d 692 (1991)