

Employer's Use of Social Networking Sites: A Socially Irresponsible Practice

Leigh A. Clark
Sherry J. Roberts

ABSTRACT. The Internet has drastically changed how people interact, communicate, conduct business, seek jobs, find partners, and shop. Millions of people are using social networking sites to connect with others, and employers are using these sites as a source of background information on job applicants. Employers report making decisions not to hire people based on the information posted on social networking sites. Few employers have policies in place to govern when and how these online character checks should be used and how to ensure that the information viewed is accurate. In this article, we explore how these inexpensive, informal online character checks are harmful to society. Guidance is provided to employers on when and how to use these sites in a socially responsible manner.

KEY WORDS: background check, character check, social networking, social responsibility

Abbreviation: SNS: Social networking site

Introduction

Advances in technology have once again shifted how people communicate with each other. Not only has wireless communication made it possible for us to talk to one another when thousands of miles apart, but now we can instantly receive e-mails, send text messages, and “twitter.” Older generations recall how people mainly talked face to face, while members of the newest generation often prefer texting to talking face to face (Reid and Reid, 2004). New communication tools are available such as blogs, wikis, and chat rooms, as well as entire virtual communities such as Second Life. There are 1.6 billion Internet users worldwide (Internetworld-stats.com, 2009).

Many people use social networking sites (SNSs) to stay in touch with each other. SNSs such as Face-

book and MySpace initially began as forums for young people to connect and have evolved into a new type of community for social and commercial exchange. Through a variety of tools (e-mail, chat, blogging, instant messaging, photo sharing, news feeds), SNSs are used for job networking, targeted marketing, and entertainment. The impact of SNSs for communication is just now being understood. Following the 2009 elections in Iran, SNSs were credited with keeping communication open with people within and outside of Iran when traditional means of communication were limited by the Iranian government (Labott, 2009).

Many SNSs require the user to create a webpage that contains information about the user that he or she wants to share with others. Some members use these pages as billboards about themselves while others use them as personal diary pages. Most SNSs allow the user to limit access to posted online material to a designated group of people while sharing a public portion with all fellow users. However, users are learning that information posted on the SNS often becomes available to people beyond the intended audience. For example, Facebook allows its advertisers to use members' posted photos in their advertisements without requiring further consent or compensation to members. Few users are aware of this policy or the steps required to prevent their posted photos from being used in this manner (Harrington, 2009). Depending on how the SNS works and the privacy restrictions selected, friends of friends, including employers, may have access to their full profiles (Brandenburg, 2008; Facebook, 2008).

SNSs are also serving as an inexpensive and quick source of background information on job applicants and current employees for employers. We are at the crest of a major shift in practice by employers.

Employers have always been able to request background and reference information on job applicants but have been self-restrained in doing so because of the cost and legal requirements. Typically, background checks were reserved for serious candidates and for jobs which had a business necessity for the background information. This norm is now shifting, as employers are routinely conducting informal online background checks on people and without applicants' knowledge. Based on the information they find, employers are making decisions.

In a study of students and current human-resources professionals about their attitudes toward online background checks, we found that future employees expect employers to check online for information available about them. Many employers also believe that this is an acceptable practice.¹ Other studies support this conclusion that employers are carrying out these checks and that employees understand that they are doing so (Brandenburg, 2008; Zeidner, 2007).

In this article, we argue that, even though employers may have a legal right to use SNSs in this way and future employees expect them to do so, it is wrong for employers to do this unless the information obtained in this manner is essential to the job. To support our position, we explore how social responsibility theory directs employers to conduct online background checks only when there is a business necessity because of the negative impact such checks have on society. We conclude by providing guidance to employers on when and how to conduct online checks responsibly.

Technology and interaction

Advances in technology have greatly impacted on how people communicate. Prior to the existence of the postal service, people depended on messengers to deliver messages verbally. Then, people depended on word to come from others via handwritten letters (Bellis, 2009). The telegraph made communication possible over great distances and within a shorter time. The telephone greatly changed how people communicated, becoming a main mode of communication for more than 100 years (Bellis, 2009).

During the past 20 years, technology has evolved rapidly. The creation of the fax machine allowed

people to send documents instantly to people elsewhere, to be followed by the Internet and e-mail, which has provided a new way for people to communicate. Now, people use sophisticated cellular telephones to access the Internet, send instant messages, text, shop online, determine their location, and document their lives in small "tech bytes" by "twittering" or posting comments to their SNS's "walls" (New Media Consortium, 2007).

Clemmitt (2006) noted that advances in technology have an impact on how people interact socially. This is evident with the growth in the use of SNSs. Facebook, a popular SNS, began in 2004 as a way for college students to interact with each other (Brandenburg, 2008; Facebook, 2009a). In 2006, Facebook expanded membership to the corporate sector in the hope of retaining college alumni as members (Peluchette and Karl, 2008). In 2009, Facebook reported over 200 million users (2009b), Friendster had more than 100 million (Friendster, 2009), MySpace declined to 100 million users (Arrington, 2009), and hi5 had more than 80 million users (hi5, 2009). hi5 states that it is the most globally diverse SNS, with 80% of its users outside of the USA (hi5, 2009). When ranking sites based on the number of unique monthly visits, the top three in 2009 were Facebook, MySpace, and Twitter (Kazeniac, 2009). Wikipedia (2009) lists more than 100 SNSs.

Facebook describes its purpose as a "social utility that helps people communicate more efficiently with their friends, family and coworkers" (Facebook, 2009a) and explains that it digitally maps users' real-world social connections. A growing site, Bebo, purports to integrate all social networking and Internet sites so a person can go to one place "for Facebook, MySpace, YouTube, Delicious, Twitter, AIM, AOL Mail, Google Mail and Yahoo! Mail updates" (Bebo.com, 2009). Some sites are more targeted to interest areas or time periods. Reunion.com and Classmates.com help people reconnect with people from their past, while Eons.com is for Babyboomers, Café.com is for mothers, Epernicus targets research scientists, and Disaboom is an online community for people with disabilities (Wikipedia, 2009).

The online social community is continuing to evolve. Twitter is "a service for friends, family, and co-workers to communicate and stay connected

through the exchange of quick, frequent answers to one simple question: “What are you doing?” (Twitter, 2009). In 1 year, Twitter moved from the 22nd SNS based on monthly visits to 3rd place in 2009 (Kazeniak, 2009). SNSs are more than a fad. They are the next step in the evolution of interaction between people, in particular among younger generations. They are beginning to be used more and more by older consumers. Facebook noted significant growth in users with people over the age of 35 years in 2009 (Gaudin, 2009).

Growth in online checks

Despite the infancy of SNSs, surveys by various entities over the last few years have found a growing trend of employers conducting online checks using SNSs for information on job applicants. An employer can type an applicant’s name into a search engine such as Google to see what he or she finds. Some SNSs allow Internet search engines to search the names of its users and make public profiles available. Some employers have their own Facebook accounts and may be able to see more than the public profiles, depending on the friends-of-friends links and privacy settings. In this way, an employer can get a quick “character” picture of an applicant, depending on what is available online (Campbell, 2008) (Table 1).

Consequences of online checks

There are two main negative consequences that result when employers view information online that they deem unacceptable: employers do not hire the job applicant, and current employees are fired. We know that the former occurs because employers are telling us that they make decisions based on the information they find online (Careerbuilder.com, 2008; Peacock, 2009). However, most job applicants are not notified by the employer that an adverse decision was made for this reason. Rather, an applicant receives a standard “the position has been filled” letter or the person hears nothing more about the position. An applicant could also have an offer rescinded, as experienced by a law student in the

USA. The law firm found that the student was affiliated with a web site that contained negative statements about female law students, even though the law student had not posted any offensive remarks (Samborn, 2007).

Evidence that employees are being fired for online information is discussed in the media and in court documents. For example, a University of Loyola swim-team member was kicked off the swim team for posting disparaging remarks about her coaches on Facebook (Clemmitt, 2006). Joe Gordon is reported to be the first British blogger fired from his job for making rude comments about his boss on his blog (LaFerla, 2006). A US flight attendant lost her job for posting a picture of herself online in her uniform (LaFerla, 2006). A producer for one of CNN’s news shows was fired for blogging offwork, even though he did not identify himself as a CNN employee (Wolgemuth, 2008). Sprague (2007) contains additional examples of employees who were fired for information they posted online.

The discussion above demonstrates that, as the use of SNSs is exploding, employers’ use of online background checks is increasing rapidly as well. While the practice seems to be taken for granted as acceptable, particularly in the USA, few employers have explored whether the practice is ethical. The authors, in their survey of US human-resources personnel, found that 43% of respondents reported using SNSs to gain information about job applicants, but only 21% had received any training on doing so, and 5% of respondents surveyed had a policy in place governing the practice. In this article, we provide a framework for that discussion, first by examining whether privacy is a right, followed by an exploration of why it is a company’s social responsibility to refrain from using SNSs unless there is a strong, legitimate business reason to do so.

Privacy

There is no universal definition of what privacy is or what constitutes workplace privacy (Miller and Weckert, 2000; Rosenblum, 1991). The Merriam-Webster Online Dictionary defines privacy as “freedom from unauthorized intrusion” (2009). We will discuss privacy in terms of a natural or fundamental right to privacy and as a legal right.

TABLE I
Studies reporting employers searching SNSs for background information

Date of study	Study	Percentage of employers performing online checks	Use of information
2006	National Association of Colleges and Employers (Business & Legal Reports, Inc., 2006)	27% of employers report searching SNSs for information on employers	Not reported
2006	Careerbuilder.com (Brandenburg, 2008)	25% of hiring managers have conducted Internet searches (i.e., Google) 12% have looked at SNS profiles	63% (of the 12% who have looked at SNSs) said they did not hire because of information found
2007	Society of Human Resource Management Survey (Zeidner, 2007)	50% of human-resources professionals ran an Internet search (Google, Yahoo!) 15% reported checking SNS, and 40% of those who do not currently check said they were somewhat likely to likely to check within a year	20% of those who ran searches said they have disqualified a candidate based on what they found
2007	University of Dayton Survey (Read, 2007)	40% of employers would look at SNSs for information	Not reported
2008	Vault's Social Networking Web Site Survey (Vault.com, 2009)	44% of employers reported checking SNSs for information	82% reported that they would let something negative on the SNS impact their hiring decision
2008	Careerbuilder.com (2008)	21% of employers reported checking SNSs for information	34% (of the 21% who looked at SNSs) reported finding content which caused them to dismiss the person from consideration
2008	Jackson Lewis LLP Survey (Hrtools.com, 2008)	12% of New York employers had looked at online sites	Not reported
2008	Authors' Human-Resources (HR) Personnel Survey	43% of HR professionals reported they had looked at SNSs to gain additional information	Not reported
2009	Global Interviewing Practices and Perceptions Survey (Peacock, 2009)	25% of global employers 12% of UK employers reported they had looked at SNSs/online for information	52% (of the 25% of the global employers who looked) said the information impacted hiring decisions

Natural or fundamental right to privacy

Discussions of privacy are traced back to Aristotle as he delineated between governmental activity and a private sphere associated with a man's household (DeCew, 1997). In 1690, John Locke also emphasized two distinct domains between public and

private spheres in his writings (DeCew, 1997); he espoused that the earth and what was produced by nature belong to all in common, but that "each person possesses himself (or herself) absolutely and has property rights to that with which he mixes his labor" (p. 11). A person owns that which belongs to and is acquired by himself or herself. Alan Westin provides

support that privacy is a natural right, documenting that animals also share a need for individual or small-group seclusion (DeCew, 1997). Margaret Mead also observed that different cultures have a universal need to establish realms of privacy: “All societies have techniques for setting distances and avoiding contact with others in order to establish physical boundaries to maintain privacy” (ibid., p. 12).

Although there is a lack of consensus about how privacy should be defined, there is a general belief that there is a natural right to have some information about oneself kept from others. Warren and Brandeis (1890), in an influential paper, *The Right to Privacy*, argued that humans have a natural right to be left alone. They wrote this paper in response to the press taking photographs of people and publishing the pictures without a person’s consent. They built the privacy right on common law that “secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others” (Warren and Brandeis, 1890, p. 198).

Introna and Pouloudi (1999) presented some historical perspectives which describe privacy as a “freedom from the judgements of others” (Introna, 1997, p. 28), as having “control over knowledge about oneself” (Fried 1968 cited by Introna and Pouloudi, 1999, p. 29), or “the exclusive access of a person to a realm of his own” (Van Den Haag, 1971, p. 149).

Legal right to privacy

Several countries have created or clarified a right to privacy related to human dignity as a fundamental right in their constitutions or laws. For example, UK enacted the Human Rights Act of 1998 which provides a person with “the right to have one’s private life respected” (Jeffery, 2002b, p. 304). France refers to Article 8 of the European Convention on Human Rights for a right to personal privacy (Vigneau, 2002). Historically, courts in the USA have interpreted the existence of a right to privacy stemming from nature and guaranteed from several constitutional amendments (freedom of speech, freedom of religion, and freedom from unreasonable search and seizures) (DeCew, 1997).

Whether there is a legal right to privacy varies greatly depending on the jurisdiction. Each country

and smaller jurisdictions within each country have different rules as to what information is deemed private and out of the purview of the employer to consider. We will provide an overview of some of the major differences in these jurisdictions. Some legal systems, such as Spain’s, strongly protect a personal realm of privacy that seems to trump an employer’s interest in considering personal information when making employment decisions (Arranda, 2002). Other jurisdictions (i.e., Brazil and Italy) guarantee that a person has the right of self-determination, which includes prior notice and consent as to how his or her personal data will be processed by an employer (Faleri, 2002; Filho and Leonel de Rezende Alvim, 2002). Others interpret privacy in terms of a balance between protecting the employee’s information and the legitimate needs of an employer to consider the information (Jeffery, 2002a). Some jurisdictions, Germany and UK, hold that it is most important to protect the contractual agreement made between two private individuals (employer and employee), acknowledging that an employee can walk away from the employment relationship if he or she does not want to provide the information (Jeffery, 2002a, b; Reinhard, 2002). The US courts often take this position, citing the doctrine of employment at will (Finkin, 2002). Other jurisdictions take the position that employees should not lose basic rights of citizenship (rights to privacy) when they walk through an employer’s door (Jeffery, 2002a). This latter position is held by France and has been repeated in recent directives by the European Union (Jeffery, 2002a; Vigneau, 2002).

More than 15 years ago, the European Union issued Directive 95/46/EC which specifies minimum standards of data protection that must be granted by all member states and any other state where data may go (Jeffery, 2002a). The directive requires that personal data be processed fairly and lawfully, be obtained for a specific purpose, be accurate, and be stored securely (Jeffery, 2002a). Directive 95/46/EC has led to new legislation and court interpretations which strengthen workplace privacy in France, UK, Spain, Germany, and Italy. Other entities, including the Organization for Economic Cooperation and Development, the Council of Europe, the International Labour Office, and the United Nations, have also have passed directives

which protect an individual's right to privacy (Jeffery, 2002a). The USA has few legal limitations on the use of personal data by employers when making employment decisions (Finkin, 2002). See Appendix A for a summary of workplace privacy laws in selected countries.

It is unclear how privacy laws will be interpreted when it comes to information an individual posts on a SNS. Key legal questions are whether the individual consented to the information being made available to everyone, whether the information is relevant to the employment decision, and whether the information falls within a protected realm of personal privacy even if a person makes the information available to many people or does not use provided privacy settings.

Legally it is debated where the line is drawn between an employer's right to access information and an employee's right to keep certain information private. Advances in technology make it possible to store lots of information about people and to access that information quickly, cheaply, and without knowledge that such information has been accessed (Miller and Weckert, 2000). For these reasons, many urge that a right to privacy be clearly established (Stross, 2007).

Expectations of privacy

Even if the information that an individual places on SNSs is personal or protected information, many argue that a job applicant waives an expectation of privacy to that information when he or she places it on a SNS (Introna and Pouloudi, 1999). Warren and Brandeis (1890) were clear that a person's right to privacy ceases once the individual publishes the information or consents to its release. Legally, the critical issue is whether a person "publishes" information about himself or herself when he or she places it on a SNS.

A person's Facebook site often has recent photographs of the person with his or her family and friends, short blogs describing daily activities, and online dialogue by family and friends. For example, as a friend of John's site, one can view the dialogue posted by John and his "friends." When John updates his profile or posts a picture, all of John's friends are notified that an update has been made.

Facebook provides users with some options to limit who has access to their full profile. Even by selecting the most restrictive settings, the information displayed may not be hard to access (Brandenburg, 2008). A Facebook user has the ability to search and access profiles more thoroughly. To ensure complete privacy, some SNS users create a public page using their real name and a pseudo site for friends that contains the pictures and dialogue intended for them.

Simms (1994) suggests that there is a difference between self-presentation and self-disclosure. Self-presentation is the "communication of self-data an individual might reveal to most any other person" (p. 317). Self-disclosure is the "explicit communication of self-data another would not have access to" (p. 317). Self-disclosure strengthens a relational bond and includes sharing of emotional experiences (Simms, 1994). Given this difference, perhaps employers should have access only to self-presentation information and not to self-disclosure information. Young people may also see their profiles as self-presentation tools rather than self-identity tools (Livingstone, 2008). Employers may be basing decisions on information that shows poor judgment in what a young person decides to present to others but may not represent whether the individual is of good character or not.

Some argue that young people have a different expectation of privacy than older employees. Livingstone (2008) disagrees, noting his research that teenagers want control over who has access to the information they post online (see also Thibodeau, 2008). They want their friends to read their profiles but do not want their parents or employers snooping through their private space. Currently, social networking privacy settings are too limited to allow users to designate who is able to receive what type of information beyond allowing a "friend" into the site (Livingstone, 2008). Facebook is tweaking its privacy settings to allow users to control who can view each post (Noyes, 2009). Privacy advocates urge Facebook to default to the highest privacy settings rather than defaulting to the lowest as it currently does (Noyes, 2009).

There appears to be a disconnect between how members use their SNSs to communicate daily on a personal level with friends, and employers' practice to judge job applicants based on what is posted. The

online sites serve as a local gathering place where people run into each other, make plans, and share news. Unlike a traditional bricks-and-mortar gathering place, now conversations are immortalized, and it is very easy for others to be voyeurs and make judgments based on social interactions. The purpose and activity taking place in the gathering places are the same as those that would occur in a bricks-and-mortar gathering place. The difference is that the digital information becomes permanent and employers are being the voyeurs. Employers are taking in all kinds of personal information, and making decisions based upon that information, without job applicants being aware. Employers are doing so because it is easy and cheap to do so. We contend that an employer would not ask a human-resources staff member to follow a job candidate to a local restaurant or bar and sit in the booth beside him or her for the purpose of overhearing conversations and witnessing behavior for a character check. As long as the job candidate is in a public place, the employer could legally do so, but for most this action would seem extreme and inappropriate. Why do we not have a similar reaction when the same behavior occurs online?

Next, we discuss how this change in practice is damaging to society and why employers need to curb this practice.

Corporate social responsibility

The traditional view of a company is that the company has a responsibility to make as much profit as it can for its shareholders (Friedman, 1962; Grossman, 2005; Jensen and Wygant, 1990). An alternative view of the firm was suggested by Edward Freeman in 1984 and termed the stakeholder approach. The stakeholder approach directs organizations to manage the interests of and acknowledge a duty of care to a range of stakeholders (Jamali, 2008). A stakeholder is “any group or individual who can affect or is affected by the achievement of the firm’s objectives” (Freeman, 1984, p. 25). Stakeholders include the traditional ones – shareholders, customers, employees, and suppliers – but are expanded to include such groups as competitors, governmental entities, special interest groups, media, and local community organizations (Freeman, 1984).

A stakeholder perspective of social responsibility has been developed and is categorized as descriptive or normative. The descriptive stakeholder theory examines how well an organization attends to the needs and interests of various stakeholders. An organization is viewed as being socially responsible using this approach if it attends to the needs and interests of at least half of its stakeholders (Jamali, 2008). The normative stakeholder approach focuses “on the ethical requirements that cement the relationship between business and society” (Jamali, 2008, p. 219).

Using the traditional view of the firm or a limited stakeholder view of the firm, one can understand why an organization would conclude that online character checks are an acceptable business practice. From the employer’s position, there are many reasons why conducting an online background check is in the interest of its shareholders. It provides an easy way to gain a “character” assessment of candidates without much hassle and allows the employer to learn more about a candidate than is possible any other way. Employers argue that they have a right and need to protect themselves (i.e., shareholders) from negligent hiring (Blackwell, 2004). Negligent hiring may occur if a company “fails to uncover an applicant’s incompetence or unfitness by a diligent search of references, criminal background or even general background” (Edwards and Kleiner, 2002, p. 137). Employers also state that using SNSs gives them a sense of the type of decisions job applicants will make (Brandenburg, 2008).

In the USA, many job applicants, having been warned of the practice, believe it is acceptable for employers to check up on them by conducting Google searches or reviewing their SNS pages. In a University of Dayton study, 68% of students surveyed did not believe it was unethical for employers to look at their SNSs (Read, 2007) despite many students reporting that they believed there is a strong line between personal and work life (Read, 2007). In the authors’ study of students about their perceptions of an employer’s use of SNSs in the hiring process, only 33% of students thought that viewing SNSs was unethical. Thirty-six percent thought the practice was ethical, while 32% were undecided about the practice. In follow-up interviews, some students expressed a view that what is online is public. They argue that a job applicant should know by now not

to post anything that the applicant does not want a potential employer to see. Employers also share the view that job applicants need to clean up their sites and remove anything that could be viewed negatively, stating that nothing is safe online. Some employees are willing to give up some privacy to ensure that they are safe in the workplace, which they believe is more likely if employers conduct thorough background checks (Blackwell, 2004).

We believe that these views of the firm ignore the impact that online character background checks have on stakeholders not considered in this reasoning and on society at large. There are users of SNSs who are not yet of an age to apply for jobs. There are older stakeholders who have a different view of privacy and are not willing to concede that an employer can look. Also not considered are the stronger views of privacy held by global partners and employees. Some stakeholders are in a better position to articulate their interests (Introna and Pouloudi, 1999) and others are in a position of power imbalance and cannot honestly represent their concerns.

Blanket acceptance of this practice destroys the utility and positive impact of this new communication medium. The practice sends a message to SNSs users that you cannot communicate honestly online for fear that your views will be judged and prevent you from getting a job. Currently, people use SNSs as they would a telephone or restaurant table. If a realm of personal privacy is not provided to this type of communication, society will forever lose the benefits that online communication provides. For these reasons, a return to more conventional social responsibility focused on what is in the best interest of society is warranted.

A broader view of the purpose of a company gained momentum in the 1960s with the discussion of corporate social responsibility (Wines, 2008). Corporate social responsibility includes the claim that organizations should be not only concerned about making a profit but also engaged in “actions that appear to further some good, beyond the interests of the firm and that which is required by law” (McWilliams et al., 2006, p. 1).

Proponents of social responsibility justify this approach, explaining that businesses do not exist in isolation, they receive benefits from society to exist, and they have an obligation to give back to society. Some use a marketing approach to justify social

responsibility, arguing that it is sound business practice for a business to appear socially responsible (Shaw, 2009). Grossman (2005) explains that there is an interconnectedness between social and financial performance and true corporate social responsibility which is focused on the long term. Grossman (2005) defines true corporate social responsibility as “the implementation of sound management structures aimed at minimizing risk in areas such as governance, environmental impact, social impact and workplace practices” (p. 582). Stated simply, companies should “earn money in a moral and ethical way” (McCle-nahan, 2005, p. 64). For the purposes of this paper, corporate social responsibility is defined as “a business obligation to pursue policies, make decisions, and take actions that benefit society” (Williams, 2010, p. 71).

Currently, the virtual door is wide open and companies are racing through. With the click of the mouse, employers are conducting unfettered online character checks, creating a global norm that this intrusion into one’s personal realm is acceptable. There is no time to wait for laws to be passed to curb this practice. We believe that companies must act out of a higher responsibility to society, a global society, to preserve a natural right to personal privacy. Bloustein (cited by Manning, 1997) stated that invasions of privacy are wrong because “they are invasions of liberty as individuals to do as we will,” and “they undercut individuality and create a society of conventional, mediocre persons” (p. 818).

Online character checks harm society

In the following section, we explore in greater detail why conducting online character checks is damaging to society in the following ways:

- Online communities are a new way for people to interact, and this evolution of communication should be protected;
- Areas of privacy should be shielded from employer use;
- Online communication is permanent, and consideration of decisions years later may be harmful;
- It is good for society for there to remain boundaries between one’s work and personal life.

Online communities

Advances in technology have always changed how society communicates and interacts. With the creation of the Internet in the 1970s, “online socializing has helped people worldwide link to others with common interests for conversation and support” (Colin, 2006, p. 625). A generation ago, people were more likely to remain in the same place and develop long-term friendships based on face-to-face contact. Now, many of us live in a city different from where we grew up, and the number of traditional friendships is down (Clemmitt, 2006).

The use of the Internet is largely social (Clemmitt, 2006). A survey by the Pew Internet and American Life Project found that 34% of respondents said that the Internet played an important role in a major decision they had made, meaning they sought advice and support from other people online (Clemmitt, 2006). In the same survey, 84% of Internet users reported joining a group or organization with an online presence. “Members of online groups also say the Internet brings them into more contact with people outside their social class or their racial or age group” (Clemmitt, 2006, p. 627). The Internet allows people to stay in touch with old friends and make new ones (Clemmitt, 2006).

Others argue that web-based socializing strengthens online and offline relationships because it is facilitating a shift to new communication modes rather than causing a decrease in communication altogether (Clemmitt, 2006). A report by the Pew Internet and American Life Project and the University of Toronto discusses “a shift from neighborhood and village-based groups to communities oriented around geographically dispersed social networks” (Clemmitt, 2006, p. 634). The Pew Internet study found that people were in more contact with members of their communities and social networks than before, and those who e-mailed closest friends/family often were more likely to speak to them on the phone as well. A University of Toronto study found that people who had high-speed Internet access knew more names of neighbors than those who were not wired (Clemmitt, 2006).

Online socializing is very important for teenagers because they need to have their own space, and social networking provides them with their own

space online (Clemmitt, 2006). Online communities also provide previous outcasts with a way to connect with friends who have similar interests from around the world (Clemmitt, 2006). Socializing online may occur without initial judgments based on physical appearance, disabilities or other stereotypes (Clemmitt, 2006).

Despite these benefits, critics of online socializing argue that online communication cannot “support human bonding the way real-world communities do” (Clemmitt, 2006, quoting Clifford Stoll, p. 633). Stanford University’s Institute for the Quantitative Study of Society found that Internet use was directly related to social isolation (Clemmitt, 2006). This study found that, for every hour spent online, a person spends 23.5 min less face to face with family and friends (Clemmitt, 2006). Online socializing does not allow physical contact.

In contrast, some argue that online communication makes people more connected. “Tele-cocooning” is described as “carrying your friends around with you, using technology to be literally in contact with them all the time” (Clemmitt, 2006, p. 634, quoting Mimi Ito). For example, Sam posts comments throughout the day on his Facebook wall such as: “Leaving for kids’ soccer games. Dawson made a goal. Mom’s surgery went well.” An e-mail alert is sent to each of Sam’s Facebook friends letting them know that Sam has updated his wall. Friends can immediately read and post a return comment on Sam’s wall.

The invention of the telephone changed the interaction between people drastically from face-to-face meetings and letter-writing to verbal communication. Likewise, the Internet and wireless communication is quickly modifying how humans interact. There is no stopping this process, and there is a global interest in protecting some realm of privacy within this communication medium. If employers continue to conduct online character checks, we believe there will be a chilling effect on this type of communication. People will modify what they post and write to conform to the expectations of employers, resulting in what Bloustein predicted: Invasions of privacy will lead to a society of “conventional, mediocre persons” (cited by Manning, 1997, p. 818). The chilling effect will render this form of communication inferior, as people will be less honest and self-censor interactions.

Privacy

As a Facebook user, a person is able to search the profiles and invite acquaintances to become friends. Facebook will search for potential friends based on people a new user has e-mailed in the past. When a new user reviews a suggested person to invite as a friend, he or she can review the list of that person's friends. When reviewing a friend of a friend's list of friends, a user is able to access portions of the friend of a friend's profile and the online communications that are posted on that person's wall. A person is a voyeur to various conversations to which he or she has no prior relationship. Friends can post pictures that may include other people without obtaining the consent of the people in the picture. Quickly, a user loses control over the content that is posted online and made available to other people.

If we do not recognize a realm of privacy to protect these conversations, we are opening Pandora's box to a different world with very little privacy. It would be similar to allowing public restaurants to place bugs under each table and broadcast the hundreds of conversations that occur daily on a public feed for employers to view. In online communities, people are having conversations using a different technology that is easier for them to use. This new technology is also archived, leaving a permanent digital trail. Our traditional conversations are rarely archived unless someone is taping them, a practice often prohibited by law (Clemmitt, 2006).

Many users of SNSs communicate with a false sense that these online communities are safe (Clemmitt, 2006). Others have a belief that the communication one conducts on the Internet is private since it is often done in one's own home (New York Times, 2006). People use the Internet to check their financial records, research sensitive medical issues, and seek advice on topics about which they would be ashamed to ask a friend. Many teenagers post with a belief that no-one is watching. While teenage girls would be horrified if someone read their diary, they are posting so much more personal information online (Clemmitt, 2006).

In the future, online communications and social networking will become even more deeply rooted in our lives. Social networking addresses may be the

most consistent way to reach someone (Clemmitt, 2006). As the flood gates are open, for the good of society, we need to ensure that technology does not strip away our privacy.

Edwards and Kleiner (2002), who wrote an article about conducting traditional reference checks in 2002, cautioned employers to realize "a social responsibility not to invade the privacy of an applicant more than necessary" (p. 146). They argued that employers have access to so much information, that job applicants do not know how much information is being considered, and that employers need to limit their consideration to only job-related information. Miller and Weckert (2000) agree, stating that an employer is buying labor not things outside of work, and privacy is a moral right. Recently, some countries have passed laws to limit the information that may be considered by an employer about a job applicant (Jeffery, 2002a).

Permanency of online communication

A major difference of online communication is that it is a permanent type of communication. Even when a user deletes the information, it remains the property of the SNS and can be recalled at a later time. Sometimes a user's deleted profile is still retrievable upon an Internet search because it exists somewhere online. In contrast, many laws protect the interception of a telephone conversation by a third party or government entity (Jeffrey, 2002a). It is also a violation of most laws for a written letter to be opened by someone other than the intended receiver. Online communication is not afforded similar protection. Because of this permanency, a person's mistakes or misjudgments cannot be retracted and may come back to haunt him or her. This permanency has a greater impact on minors, who are known for making errors of judgment.

Most countries protect minors from the decisions they make when it is believed they lack full mental capacity to assess the risks and consequences of their actions. In some jurisdictions, minors who commit crimes are prosecuted and punished in a separate juvenile system, and their records are sealed and purged when they reach the age of majority (Junger-Tas and Decker, 2006).

New technologies are developing all the time and are creating a generational divide. Young adults and teenagers have grown up with technology and have done most of their communication through computers. They have learned to multitask while communicating with several people at the same time (Sherman, 2008). Teenagers are quick to jump on-board with the new technology, making it hard for legislators, parents, and others to stay on top of it (Clemmitt, 2006). Most cyber social network users are aged between 12 and 25 years (Clemmitt, 2006). Although SNSs may restrict accounts to users of certain ages, often teenagers are allowed on the sites legitimately; thirteen-year-olds are allowed an account on MySpace. Since there is no good way to verify a user's identify or age, much younger users are online.

Eighty-three percent of teenagers surveyed about MySpace said they believe it is safe (Clemmitt, 2006). College students also perceive SNSs, especially Facebook, to be private (Peluchette and Karl, 2008). However, a proposed Facebook change in 2006 made users more aware that whatever they put online remains saved forever (Clemmitt, 2006). Online information cannot be deleted permanently and may remain accessible for years due to caching (Oblinger and Hawkins, 2006). The information one posts online is only as safe as your friends keep it (Clemmitt, 2006).

Teenagers and younger users sometimes use SNSs in a risky manner. However, it is important to remember that a lot of online behavior was happening anyway in teen hangouts but parents and employers did not have access to it (Clemmitt, 2006). In 2006 a survey of US students explored what kind of information they post on their SNS profiles (Peluchette and Karl, 2008). Results indicated that males were more likely to post self-promoting and risqué pictures or comments while females were more likely to post cute or romantic material. Teenagers expressed comfort with family, friends, and classmates seeing their sites, but one in five did not want employers seeing their sites. The study confirmed that students did not realize the consequences of posting such information online (Oblinger and Hawkins, 2006; Peluchette and Karl, 2008).

It is in the public interest to protect the privacy and actions of people in their social interactions. It is

also not in society's interest for employers to have access to the missteps, questionable decisions, or nonmainstream ideologies of job candidates when making employment decisions. Allowing employers access to this personal information may forever impact a person's ability to get a job. It has yet to be established that judgments made based on information from SNSs is related to job performance.

Boundaries between work and private life

Currently, there is a debate about whether there still exists a boundary between work and an employee's private life (Charlesworth, 2003). Such a boundary has not always existed. Conway (2003) notes that it was only with the Industrial Revolution and a change in where work was conducted that such a wall formed. Prior to the Industrial Revolution, it was common for work to be conducted within a person's home. The Industrial Revolution led to people working within factories in cities, and the separation between work and one's home life developed. Now, with the advancement of technology and the desire for flexibility (Cowan and Hoffman, 2007), there seems to be a blurring of the line, as people return to working more at home (Duxbury and Higgins, 2001; Johnson and Chadwick, 2009).

Manning (1997) argues that an employee has a right to liberty, and flowing from liberty is a right to lead one's life separate from work. This freedom is required for private thoughts and development of one's self apart from his or her work identity (Manning, 1997). Others strongly counter that work is not a right but a privilege, and argue that an employer has a right to know whatever it can about a person to protect its property right in the business (Myatt, 2009; Sugarman, 2003). Myatt explains that an employee is a direct representative of the company at all times, on and off work. Manning (1997) makes the point that a person does not have to work for an employer if he or she does not agree with the employer's hiring practices. Often a job applicant or employee is unaware that the employer is conducting an online background check and has made an adverse decision based on that information. Manning's view of employment ignores an employee's

unique contribution and value to the organization and seems to treat employees as a means to an end.

Maintaining a separation between work and life is something that brings value to the organization, the employee, and therefore society. For example, organizations that offer flexibility and work–life balance options provide a mechanism to reduce stress resulting from high work–life conflict (Eos Life~Work, 2007; Van Steenbergen and Ellemers, 2009). It also makes employers more competitive in attracting and retaining employees (Gregory and Milner, 2009; Hakala, 2008).

If the boundary between work and an employee's private life is destroyed, it becomes more likely that employees will modify their behavior for fear of being judged by their employer. Employees may then express religious, political, and other views they believe the employer deems acceptable, resulting in masses of people who act in a cult-like fashion. This type of groupthink can have dire consequences and eliminate originality and creativity (Dvorak, 2001; Whyte, 1989).

While it is true that working for a particular employer is not a right, having the opportunity to work is an economic necessity (Eos Life~Work, 2007). If the boundary between work and family is eroded in part based on this rapidly developing social norm, then some may not be able to work because of the judgment of others (“she is too conservative or too liberal”; “she is a sinner for sexual preference”; etc.). It is important that the line between work and one's private life be clearly marked and preserved (Stross, 2007).

Summary of the potential harm to society

The current practice of employers conducting online character checks that include reviewing information posted on job applicants' SNSs is harmful to society because it allows employers to be undetectable voyeurs to very personal information and make employment decisions based on that information. The acceptance of this practice would have a chilling effect and permanently render a promising communication medium inferior and dangerous for people to use. We believe that society needs SNSs because they are the next step in human social interaction. Currently, within these sites,

people are reconnecting and maintaining daily contact with others across geographical distances. Society needs this communication medium but along with it realms of personal privacy must be protected.

In addition to the potential of damaging an evolving communication medium, the current practice of unfettered checks further destroys a line between what is appropriate for the work realm and what should exist in one's private realm. The current practice attacks a natural right of humans to have a personal space. The practice also has a greater impact on younger generations, as they are the most dominant users of SNSs and are more likely as teenagers to use the sites for boasting, which may haunt them later when they seek employment. These issues are amplified because currently our digital communications remain permanently in digital storage for people to judge years later. For these reasons, we call upon employers to make a practice change that will benefit society by protecting this virtual communication space from their judgment.

Guidance for socially responsible use of online background checks

Employers should cease the practice of informal, online background checks of job applicants and take the necessary time to discuss and establish a policy to guide when and how an employer will use information obtained from online sources in the future (Rifkin, 1991). The first step in developing a policy is for an employer to establish that there is a link between what is contained on applicants' SNSs and on-the-job behavior (Peluchette and Karl, 2008). If this link exists, then an employer should determine for which jobs the employer has a legitimate business interest in gathering this information (Bahls, 1990). Sugarman (2003) provides a more detailed discussion of what a legitimate business interest may include. For those jobs for which there is a legitimate business interest, employers should determine what impact online background checks have on the trust formation between the employer and the future employee. The employer should also weigh the benefits gained against the potential negative consequences from further erosion of the boundary between a person's private and work life.

For those jobs for which there is a legitimate interest to consider the information found on a SNS that outweighs the negative consequences to society at large, the employer should establish guidelines to be sure that the employer is not seeking or using information based on protected class membership (Greenwald, 2008) or in violation of a law or regulation. The employer should weigh whether it is better not to look in order to prevent the inference that a protected characteristic was illegally considered (Greenwald, 2008).

Guidance provided to employers on how to conduct and use information from traditional background checks applies as well to informal online background checks. For example, Bahls (1990, pp. 30–31) provides the following guidance:

- Do not conduct a check unless the information is job related and the employer can justify a legitimate reason in court;
- Provide fair notice to the employee prior to the background check;
- Make sure the information obtained is accurate, complete, and relevant;
- Keep promises of confidentiality;
- Restrict in-house access to information to those with legitimate interest in the information;
- Discard outdated information;
- Avoid intrusive data collection.

Charlesworth (2003, p. 222) provides similar guidance to employers who are considering a measure that intrudes on an employee's privacy:

- Have a legitimate purpose for the intrusion;
- Ensure that the intrusion is offset by a greater utility to the employer or society;
- Use the least intrusive measure possible that achieves the desired outcome;
- Ensure that the measure is fair and lawful;
- Apply the measure equally to similarly situated job applicants or employees;
- Be transparent in your use of the measure and the process the employer used to develop the measure.

Conclusions

There appears to be a disconnect between how users of SNSs view the purpose and utility of SNSs and how employers view the sites. Users of SNSs use them mainly for social interaction, whereas employers use a site to gather character information about job candidates without the applicants ever knowing what information was considered. SNSs serve as a local gathering place, albeit online, where people run into each other, make plans, and share news. Unlike a traditional bricks-and-mortar gathering place, online conversations are immortalized in the online gathering place, and others (friends and strangers) can be voyeurs and listen in. The purpose of and activity taking place in these gathering places are the same, but the permanency and judgment of the activities by employers are something very different.

We call upon employers to take a moment to consider the impact these easy, informal background checks have on society. The greatest impact is the chilling effect this practice will have on the quality of human interaction that will occur online. Rather than expecting users of SNSs to change their behavior by not posting anything they do not want an employer to view, we argue that it is better for society for employers not to enter an employee's virtual front door.

Note

¹ The afore-mentioned authors' study was approved by the authors' university's Office of Compliance in accordance with the ethical standards laid down in the 1964 Declaration of Helsinki. All respondents in the study provided their informed consent prior to beginning the survey and identifying information was not collected.

Appendix A

See Table II.

TABLE II
Workplace privacy orientation and laws in selected countries

Country	Workplace privacy orientation and laws
Brazil (Filho and Leonel de Rezende Alvim, 2002)	<p>An employee sells his work time to the employer. The legal system tries to balance the employee's private life and private correspondence with an employer's private property rights and a manager's right to manage. Courts have recognized that employees have a private sphere that is protected from employer intrusion. Employers are required to provide notice before any workplace surveillance occurs. When it comes to personal data, an employee should be able to decide what happens to it (self-determination orientation).</p>
UK (Jeffery, 2002b)	<p>In 1998, a provision was added to the Constitution which protects workers from automation. It called for the development of tools to achieve a balance between workers' productivity and the automation of work. Courts have found that e-mails, even when sent from a company's computer, are private correspondence. Courts have made decisions based on an employer's "(a) respect for the worker's dignity, and (b) consistency between surveillance procedures and their stated purpose" (p. 290).</p> <p>There are several recent laws in UK that address the surveillance of workers and the processing of personal data. The Data Protection Act 1998 was passed to implement European Council directive 95/46/EC. The Human Rights Act 1998 includes "the right to have one's private life respected" (p. 304). The Regulation of Investigatory Powers Act 2000 provides a legal framework for all interceptions of communications on both public and private telecommunications systems (p. 305) and requires that both parties to the communication consent to the communication being intercepted by another party. Laws have required an employee's notice, consent, and fair treatment when specifying what behavior is legal. In summary, these laws required an employee's notice, consent, and fair treatment prior to processing of personal data. These laws are just now being implemented and interpreted by the courts. It is likely that, when in doubt, the courts will interpret the law to provide for individual privacy. Common law has also recognized a right to personal privacy. Initially the laws seemed to weigh in favor of employees and protect personal data from employee surveillance. Recently, laws seem to have been in favor of employers.</p>
Germany (Reinhard, 2002)	<p>Germany has a mixture of laws that provide some workplace privacy and are in compliance with Directive 95/46/EC. Employers have the right to collect some personal data on employees. Surveillance without an employee being given notice can only occur in rare circumstances. Courts have ruled that "the protection of personal data is a fundamental right under the Constitution" (p. 393). The collection of personal data must be authorized by law or when a person consents.</p>

TABLE II
continued

Country	Workplace privacy orientation and laws
Spain (Arranda, 2002)	<p>A 1980s law established a right of the employer to monitor the employee regardless of the methods used. Judicial interpretations of this law have limited the degree to which an employer may monitor. The monitoring must relate to employment. The employee must be informed of the monitoring before it occurs. The courts look to company rules for guidance on whether the monitoring is appropriate. Monitoring must be justifiable and related to its purpose.</p>
USA (Finkin, 2002)	<p>The Spanish Constitution of 1978 included Article 18.4, which states that “the law shall limit the use of computers in order to safeguard the honour and privacy of all its citizens, whether related to the individual or the family, and ensure that they may fully exercise their rights” (p. 449). In 1999, a new law (Ley Orgánica de Protección de Datos de Carácter Personal, referred to as LOPDCP) provided protection of personal data and implemented Directive 95/46/EC. The LOPDCP has two main requirements. First, personal data sought by an employer must have a legitimate purpose. Second, the data sought must be relevant, appropriate, and not excessive with regards to that purpose. In determining whether the purpose is legitimate, the consideration of the personal data cannot lead to unlawful discrimination based on sex, race, ideology, or union membership. Sensitive personal data requires the consent of the data subject prior to its processing.</p> <p>In the USA, the employment-at-will doctrine is strong. Unless there is a contract stating otherwise, the employment-at-will doctrine states that an employer or employee may end the employment relationship for any reason at any time. Very little employee privacy protection exists in federal and state legal codes. Likewise, there is very little workplace privacy protection afforded in common law.</p> <p>The Electronic Communications Privacy Act (1968) provides some protection against wire taps and the release of stored communications, but what is protected is interpreted narrowly.</p> <p>Common law protection against wrongful invasion of privacy requires that a person has a reasonable expectation of privacy and that the nature of the invasion of privacy to a reasonable person is “highly offensive.”</p> <p>In contrast to laws in other countries, recent state legislation has afforded more protection to employers when providing reference information about a former employee rather than limiting what information an employer may consider.</p>

TABLE II
continued

Country	Workplace privacy orientation and laws
France (Vigneau, 2002)	<p>Law and culture in France recognize a sphere of personal privacy. In French law, there are three principles that guide workplace privacy. The principle of transparency requires that prior notice be provided to an employee before workplace surveillance or personal data is processed. The principle of proportionality requires that the means used to gather the information is balanced to the depth or type of information needed. The third principle of relevance requires the employer to justify the need for the information. An employer must notify an employee that personal data will be collected. The employee can challenge its use Article L.121-6 of the French Labor Code requires that "information sought from job applicants and employees must aim exclusively at evaluating their professional abilities" (p. 354). Recent decision by the highest appeal court in France found that an employer did not have the right to open an employee's private e-mail even though it was retrieved using the employer's computer during work hours. An employer can monitor work activities of employees only to the extent that such surveillance does not interfere with the employee's right to privacy.</p>
Italy (Faleri, 2002)	<p>Article 9 of the French Civil Code and Article 8 of the European Convention on Human Rights clarify that an individual has a right to personal privacy. French law also follows European Community Directive 95/46/EC.</p> <p>Italian law seems to ensure a balance between the employer and the employee in contrast to recognizing an employee's right to privacy. The law recognizes an employee's "right to data self-determination" (p. 426). Changes were made to Italian law to comply with Directive 95/46/EC. Sensitive data requires a data subject's consent before it can be processed, and the processing must be authorized by the Guarantor. The Guarantor has provided authorization for many types of data processing through the issuance of a list. Ordinary data does not require the consent of the data subject.</p> <p>An employee's right to privacy is "limited by the Freedom of Economic Initiative, as established by Article 41 of the Italian Constitution" (p. 414). This constitutional provision specifies that any law cannot impose excessive bureaucracy that would impact an employer's ability to run the business efficiently.</p>

References

- Arranda, J. T.: 2002, 'Information Technology and Workers' Privacy: The Spanish Law', *Comparative Labor Law and Policy Journal* **23**(4), 431–470.
- Arrington, M.: 2009, 'Facebook Now Nearly Twice the Size of MySpace Worldwide', <http://www.techcrunch.com/2009/01/22/facebook-now-nearly-twice-the-size-of-myspace-worldwide/>. Accessed 20 June 2009.
- Bahls, J. E.: 1990, 'Checking Up on Workers', *Nation's Business* **77**(12), 29.
- Bebo.com: 2009, 'Bebo', <http://www.bebo.com/c/site/index>. Accessed 4 June 2009.
- Bellis, M.: 2009, 'The History of Communication', http://inventors.about.com/library/inventors/bl_history_of_communication.htm. Accessed 20 June 2009.
- Blackwell, C. W.: 2004, 'Current Employee Privacy Issues', *The Journal of Applied Management and Entrepreneurship* **9**(1), 113–118.
- Brandenburg, C.: 2008, 'The Newest Way to Screen Job Applicants: A Social Networker's Nightmare', *Federal Communications Law Journal* **60**(3), 597–626.
- Business & Legal Reports, Inc.: 2006, 'Employers Check Social Networking Sites', <http://hr.blr.com/news.aspx?id=18685>. Accessed 8 June 2009.
- Campbell, B. A.: 2008, 'Choose Your Online Friends Wisely', <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202426779555>. Accessed 11 Aug 2009.
- Careerbuilder.com: 2008, 'One-in-Five Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder.com Survey Finds', <http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr459&sd=9%2F10%2F2008&ed=12%2F31%2F2008&cbRecursionCnt=1&csid=2e371ebf845fb985c1303f725badf-297778093-JT-5>. Accessed 8 June 2009.
- Charlesworth, A. J.: 2003, 'Opinion. Privacy, Personal Information and Employment', *Surveillance & Society* **1**(2), 217–222.
- Clemmitt, M.: 2006, 'Cyber Socializing', *CQ Researcher* **16**(27), 627–648.
- Colin, T. J.: 2006, 'Cyber Socializing', *CQ Researcher* **16**(27), 625.
- Conway, J. F.: 2003, *The Canadian Family in Crisis*, 5th Edition (James Lorimer, Toronto, Canada).
- Cowan, R. and M. F. Hoffman: 2007, 'The Flexible Organization: How Contemporary Employees Construct the Work/Life Border', *Qualitative Research Reports in Communication* **8**(1), 37–44.
- DeCew, J. W.: 1997, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press, Ithaca, NY).
- Duxbury, L. and C. Higgins: 2001, 'Work-Life Balance in the New Millennium: Where Are We? Where Do We Need to Go?', Canadian Policy Research Networks Discussion Paper W 12, <http://www.cprm.org>. Accessed 22 June 2009.
- Dvorak, J. C.: 2001, 'The Group-Think Phenomenon', *PC Magazine* **20**(12), 75.
- Edwards, R. M. and B. H. Kleiner: 2002, 'Conducting Effective and Legally Safe Background and Reference Checks', *Managerial Law* **44**(1/2), 136–150.
- Eos Life~Work: 2007, 'Managing the Life~Work Boundary', <http://www.eoslifework.co.uk/boundaries.htm>. Accessed 23 June 2009.
- Facebook: 2008, 'More Privacy Options', <http://blog.facebook.com/blog.php?post+11519877130>. Accessed 11 Aug 2009.
- Facebook: 2009a, 'Facebook Factsheet', <http://www.facebook.com/press/info.php?factsheet>. Accessed 4 June 2009.
- Facebook: 2009b, 'Facebook Statistics', <http://www.facebook.com/press/info.php?statistics>. Accessed 4 June 2009.
- Faleri, C.: 2002, 'Information Technology and Workers' Privacy: The Italian Law', *Comparative Labor Law and Policy Journal* **23**(4), 399–430.
- Filho, R. F. and J. Leonel de Rezende Alvim: 2002, 'Information Technology and Workers' Privacy: The Brazilian Law', *Comparative Labor Law and Policy Journal* **23**(4), 281–300.
- Finkin, M. W.: 2002, 'Information Technology and Workers' Privacy: The United States Law', *Comparative Labor Law and Policy Journal* **23**(4), 471–506.
- Freeman, R. E.: 1984, *Strategic Management: A Stakeholder Approach* (Pitman Publishing Inc., Marshfield, MA).
- Friedman, M.: 1962, *Capitalism and Freedom* (University of Chicago Press, Chicago, IL).
- Friendster: 2009, 'About Friendster', <http://www.friendster.com/info/index.php>. Accessed 4 June 2009.
- Gaudin, S.: 2009, 'Facebook Use Jumps – Thanks to Older Users', Computerworld: Networking & Internet, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9129652>. Accessed 20 June 2009.
- Greenwald, J.: 2008, 'Web-Based Screening May Lead to Bias Suits', *Business Insurance* **42**(1), 1–2.
- Gregory, A. and S. Milner: 2009, 'Trade Unions and Work-Life Balance: Changing Times in France and the UK?', *British Journal of Industrial Relations* **47**(1), 122–146.
- Grossman, H. A.: 2005, 'Refining the Role of the Corporation: The Impact of Corporate Social Responsibility on Shareholder Primacy Theory', *Deakin Law Review* **10**(2), 572–596.

- Hakala, D.: 2008, '16 Ways to Encourage Work/Life Balance in Employees', <http://www.hrworld.com/features/encourage-work-life-balance-041608/>. Accessed 23 June 2009.
- Harrington, J.: 2009, July 24, 'Facebook Ads with Your Photos – Steps to Stop', <http://photobusinessforum.blogspot.com/2009/07/facebook-ads-with-your-photos-steps-to.html>. Accessed 2 Aug 2009, from Photo Business News & Forum.
- Hi5.com: 2009, 'About Us', <http://www.hi5networks.com/aboutus.html>. Accessed 20 June 2009.
- Hrtools.com: 2008: 'Social Networking Survey Results by One of Nation's Largest Employment Law Firms', http://www.hrtools.com/staffing/social_networking_survey_results_released_by_one_of_nations_largest_employment_law_firms.aspx. Accessed 8 June 2009.
- Internetworldstats.com: 2009, 'Internet Usage Statistics: The Internet Big Picture', <http://www.internetworldstats.com/stats.htm>. Accessed 20 June 2009.
- Introna, L. D.: 1997, 'Privacy and the Computer: Why We Need Privacy in the Information Society', *Metaphilosophy* **28**(3), 259–275.
- Introna, L. D. and A. Pouloudi: 1999, 'Privacy in the Information Age: Stakeholders, Interests and Values', *Journal of Business Ethics* **22**(1), 27–38.
- Jamali, D.: 2008, 'A Stakeholder Approach to Corporate Social Responsibility', *A Fresh Perspective into Theory and Practice* **82**(1), 213–231.
- Jeffery, M.: 2002a, 'Information Technology and Workers' Privacy: Introduction', *Comparative Labor Law and Policy Journal* **23**(4), 251–280.
- Jeffery, M.: 2002b, 'Information Technology and Workers' Privacy: The English Law', *Comparative Labor Law and Policy Journal* **23**(4), 301–350.
- Jensen, L. C. and S. A. Wygant: 1990, 'The Developmental Self-Valuing Theory: A Practical Approach for Business Ethics', *Journal of Business Ethics* **9**(3), 215–225.
- Johnson, M. and A. Chadwick: 2009, 'Today's Workplace is About Flexibility', *Financial Executive* **25**(3), 34–39.
- Junger-Tas, J. and S. H. Decker: 2006, *International Handbook of Juvenile Justice* (Springer, Netherlands).
- Kazeniak, A.: 2009, 'Social Networks: Facebook Takes Over Top Spot, Twitter Climbs', <http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/>. Accessed 4 June 2009.
- Labott, E.: 2009, 'Officials: Social Networking Providing Crucial Info from Iran', <http://www.cnn.com/2009/TECH/06/16/iran.twitter.facebook/index.html>. Accessed 20 June 2009, from CNN.com/technology.
- LaFerla, B.: 2006, 'Don't Tell Me to Shut Up', *IEE Engineering Management* December/January 2005/06, 1.
- Livingstone, S.: 2008, 'Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression', *New Media & Society* **10**(3), 393–411.
- Manning, R. C.: 1997, 'Liberal and Communitarian Defenses of Workplace Privacy', *Journal of Business Ethics* **16**(8), 817–823.
- McClenahan, J. S.: 2005, 'Defining Social Responsibility: It's Much More than Good Works and Charities', www.industryweek.com. Accessed 19 Mar 2005.
- McWilliams, A., D. S. Siegel and P. M. Wright: 2006, 'Corporate Social Responsibility: Strategic Implications', *Journal of Management Studies* **43**(1), 1–18.
- Miller, S. and J. Weckert: 2000, 'Privacy, the Workplace and the Internet', *Journal of Business Ethics* **28**(3), 255–265.
- Myatt, M.: 2009, 'Employer's Rights vs. Employee's Privacy', http://EzineArticles.com/?expert=Mike_Myatt. Accessed 23 June 2009.
- New Media Consortium: 2007, 'Social Networking, the "Third Place" and the Evolution of Communication', White Paper, <http://www.nmc.org/pdf/Evolution-of-Communication.pdf>. Accessed 4 June 2009.
- New York Times: 2006, 'Online Party Crashers', *The New York Times*, June 18, 2006 (Late Edition – Final), Section 4, Column 1, p. 11.
- Noyes, K.: 2009, 'Facebook Hones Privacy Settings, Scraps Regional Networks', *TechNewsWorld*, December 2, 2009. Accessed 15 Dec 2009.
- Oblinger, D. G. and B. L. Hawkins: 2006, 'The Myth about Putting Information Online', *Educause Review* September/October, 14–15.
- Peacock, L.: 2009, March 17, 'Social Networking Sites Used to Check Out Job Applicants', <http://www.personneltoday.com/articles/2009/03/17/49844/social-networking-sites-used-to-check-out-job-applicants.html>. Accessed 8 June 2009, from Personneltoday.com.
- Peluchette, J. and K. Karl: 2008, 'Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content', *CyberPsychology & Behavior* **11**(1), 95–97.
- Privacy: 2009, 'Merriam-Webster Online Dictionary', <http://www.merriam-webster.com/dictionary/privacy>, Accessed 30 Dec 2009.
- Read, B.: 2007, 'Online', *Chronicle of Higher Education* **53**(19), A31.
- Reid, F. J. M. and D. J. Reid: 2004, 'Text Appeal: the Psychology of SMS Texting and Its Implications for the Design of Mobile Phone Interfaces', *Campus-Wide Information Systems* **21**(5), 196–200.
- Reinhard, H.-J.: 2002, 'Information Technology and Workers' Privacy: The German Law', *Comparative Labor Law and Policy Journal* **23**(4), 377–398.

- Rifkin, G.: 1991, 'Do Employees Have a Right to Electronic Privacy?', *New York Times*, December 8, 1991, Page 8, Col 1.
- Rosenblum, M. F.: 1991, 'Security vs. Privacy: An Emerging Employment Dilemma', *Employee Relations Law Journal* **17**(1), 81–101.
- Samborn, H. V.: 2007, 'Go Google Yourself!', *ABA Journal* **93**(8), 56–57.
- Shaw, W. H.: 2009, 'Marxism, Business Ethics, and Corporate Social Responsibility', *Journal of Business Ethics* **84**(4), 565–576.
- Sherman, R.: 2008, 'Gen Y v. Boomers: Generational Differences in Communication', <http://www.fastcompany.com/blog/ruth-sherman/lip-service/gen-y-v-boomers-generational-differences-communication>. Accessed 27 Feb 2009, from FastCompany.com.
- Simms, M.: 1994, 'Defining Privacy in Employee Health Screening Cases: Ethical Ramifications Concerning the Employee/Employer Relationship', *Journal of Business Ethics* **13**(5), 315–325.
- Sprague, R.: 2007, 'Fired for Blogging: Are There Legal Protections for Employees Who Blog?', *University of Pennsylvania Journal of Labor and Employment Law* **9**(2), 355–387.
- Stross, R.: 2007, 'How to Lose Your Job on Your Own Time', *The New York Times*, December 20, 2007, <http://www.nytimes.com/2007/12/30/business/30digi.html>. Accessed 23 June 2009.
- Sugarman, S. D.: 2003, 'Lifestyle Discrimination in Employment', *Berkeley Journal of Employment and Labor Law* **24**(2), 377–438.
- Thibodeau, P.: 2008, 'The Grill: Marc Rotenberg', *Computerworld*, Feb 18, 2008, 19–20.
- Twitter.com: 2009, 'About Twitter', <https://twitter.com/about#about>. Accessed 12 Aug 2009.
- Van Den Haag, E.: 1971, 'On Privacy', *Nomos* **13**, 147–153.
- Van Steenbergen, E. F. and N. Ellemers: 2009, 'Is Managing the Work-Family Interface Worthwhile?', *Journal of Organizational Behavior* **30**(5), 617–642.
- Vault.com: 2009, 'Social Networking Web Site Survey', <http://www.vault.com/surveys/social-networking/index.jsp>. Accessed 8 June 2009.
- Vigneau, C.: 2002, 'Information Technology and Workers' Privacy: The French Law', *Comparative Labor Law and Policy Journal* **23**(4), 351–376.
- Warren, S. D. and L. D. Brandeis: 1890, 'The Right to Privacy', *Harvard Law Review* **4**(5), 193–220.
- Whyte, G.: 1989, 'Groupthink Reconsidered', *Academy of Management Review* **14**(1), 40–56.
- Wikipedia, 2009: 'List of Social Networking Websites', http://en.wikipedia.org/wiki/List_of_social_networking_websites. Accessed 4 June 2009.
- Williams, C.: 2010, *MGMT 2009–2010 Edition* (South-Western Cengage Learning, Mason, OH).
- Wines, W. A.: 2008, 'Seven Pillars of Business Ethics: Toward a Comprehensive Framework', *Journal of Business Ethics* **79**(4), 483–499.
- Wolgemuth, L.: 2008, 'Stupid Computer Tricks', *U.S. News & World Report* **144**(16), 67.
- Zeidner, R.: 2007, 'How Deep Can You Probe?', *HR Magazine* **52**(10), 57–60.

Middle Tennessee State University,
Murfreesboro, TN, U.S.A.
E-mail: laclark@mtsu.edu

Copyright of Journal of Business Ethics is the property of Springer Science & Business Media B.V. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.