Social Media, Employee Privacy and Concerted Activity: Brave New World or Big Brother?

By Jeffrey A. Mello

I. Introduction

Advances in technology which allow tremendous portability and affordability of personal computers, personal digital assistants and tablet devices combined with the proliferation of social media networking sites have changed the way in which we communicate, both privately and publically. Individuals are now afforded the means to communicate with friends, co-workers and even strangers via networks that until very recently were not available. While e-mail has existed for several decades, new social media, particularly Facebook and Twitter, have not only greatly altered how both individuals and organizations communicate, but also changed the ways in which business is conducted as well as how people interact with each other in many of their personal and professional dealings.

As of December 2011, Facebook had more than 800 million active users, half of whom log on to the site on a daily basis and half of whom access Facebook through their mobile devices.[1] Roughly 200 million of these members are in the United States, representing two-third of the population.[2] Facebook is currently available in more than 70 languages around the world[3]and is estimated to reach 30 percent of global internet users.[4] Twitter has approximately 300 million users,[5] although participation in both sites continues to expand in both numbers of members and volume of communications.

The use of social networking is not limited to personal communications. 46 percent of information technology professionals believe that online social networking is

The author is the Dean of the School of Business and Professor of Business Law and Management at Siena College in Loudonville, New York. He received a B.S., summa cum laude, from Boston University and an M.B.A and Ph.D. from Northeastern University.

an important business tool and 31 percent of that number considered it to be essential to contemporary business. More than 25 percent of organizations with 500 or more employees have developed some sort of social networking presences as a business tool.[6] A recent poll conducted of human resource professionals by the Society for Human Resource Management found that 68 percent of organizations were using social media for external communications, recruiting and marketing to engage customers, potential customers and potential employees.[7] Employers see tremendous benefit from social networking which include facilitating collaboration among employees, improved efficiencies in operations, facilitation of orientation and learning, internal brand building, employee and organizational development and faster development of new products and services.[8] However, 85 percent of IT professionals acknowledge that they are aware of employees visiting social networking sites for personal usage while at work.[9] The use of online social media has contributed to the further blurring of the separation between employees' work and personal lives.

II. Traditional Employer Monitoring — E-mail and Internet Usage

A significant number of employers monitor the communications and online activities of their employees in the workplace.[10] In fact, 43 percent of employers were actively monitoring their employees' internet use in 2007, the most recent year in which a reliable widespread survey was administered.[11] Most large employers have electronic communications policies that alert employees that the employer reserves the right to conduct such monitoring. E-mail activity is also widely monitored.[12] Most of this monitoring is accomplished not manually but electronically via software programs which can track time, content, size, attachments and recipients.[13] This tracking can also be used on personal e-mail accounts (such as those from AOL, yahoo and Google) which are accessed from the employer's network.[14] 96 percent of employers who monitor their employee e-mails track incoming as well as outgoing messages.[15] It is, however, more difficult for employers to monitor text and e-mail messages sent from employees' personal personally-owned communication devices than from those provided by the employer.

There are many reasons why employers engage in monitoring the electronic communications of their employees. The first is to protect the employer from a variety of legal liabilities which could come about as the result of the content of such communications. Reporting requirements imposed under the Sarbanes-Oxley require the retention and storage of all e-mails related to financial transactions.[16] In the event of any kind of employee misconduct, the employer can be held liable if the employer knew of the conduct and did nothing about it as well as if the employer was unaware of the conduct but was presumed that the employer "should have known" about the conduct.[17] Such an obligation on the part of employers requires a heightened level of sensitivity toward the activities of individual employees which might necessitate the monitoring of communications taking place at work, on employer-owned equipment and networks and within the context of an employee's job. Additional liability can be incurred through the sending and transmission of sexually explicit or provocative e-mails, with or without graphic images, and display of materials on pornographic websites which can serve as a basis for a sexual harassment lawsuit.[18]

Second, employers also might engage in employee monitoring to determine the extent to which employees are actually doing their jobs during work hours and not engaging in distracting personal business. In addition to paying employees for work which is not being performed during regular working house, excessive personal use of employer networks and servers can result in lost productivity and efficiency for a work unit, data storage problems and/or slower network operations.[19]

A third reason for employer monitoring rests with the fact that electronic media can be a means for disgruntled employees to transmit confidential files or provide access to secure parts of the employer's website or intranet.[20] Employ-

ers need to ensure that confidential documents, files, information and/or trade secrets are not disseminated to those outside of the organization who have no legitimate business interests in accessing such information.[21] The challenge here is that electronic transmission of proprietary information is quick and relatively easy but can also be "undone" if detected in a timely manner, justifying the need for vigilant monitoring.

How widespread are these alleged transgression activities? A recent American Management Association survey found that 14 percent of employees admitted to e-mailing confidential or proprietary information about their employer its people, products and services to outside parties; 14 percent admitted to sending third parties potentially embarrassing and confidential company e-mail that is intended strictly for internal readers; 89 percent of employees admitted to using the office system to send jokes, gossip, rumors or disparaging remarks to outsiders; and 9 percent admitted using company e-mail to transmit sexual, romantic or pornographic text or images.[22]

Despite the justifications for employer monitoring, there can be a significant downside to this activity. Employees can often view electronic monitoring by employers as an invasion of their privacy which serves to erode any trust relationship which exists between employees and employers. Eroded trust can have detrimental effects on employee morale, commitment, performance, retention and self-esteem.[23] Employees, however, can and do circumvent employer monitoring though the usage of personal e-mail accounts, rather than those of the employer, and/or use a variety of personal communications devices, such as their own laptop computers, cell phone, Blackberrys, i-Phones or other portable digital assistant devices to communicate during work hours for personal communications, web browsing, shopping, checking sports scores, pleasure reading or any other kind of personal activity. A typical supervisor may not have the time to monitor each subordinate to determine whether the device being used is owned by the employer or the employee. In addition, the portability of such devices can make them difficult to conceal and their similarity to the typical hardware provided makes personal usage difficult to determine.

28 percent of employers who monitor employee e-mail admit to having terminated one or more employees due to what was discovered as a result of monitoring.[24] In two –thirds of these cases the terminations were the result of inappropriate or offensive language, content or both. In other cases the dismissal was attributable to excessive personal use of the internet during working hours.[25]

III. Legality and Privacy

Generally speaking, employer monitoring of employee communications is not only legal but also practical, given the nature and reach of electronic communications. E-mail monitoring has not been found to be unlawful, regardless of whether or not employees had been informed of company policy,[26] mainly because the employer usually owns the hardware that is being used for communications as well the network access on which the e-mail has been sent and received. Employer internet monitoring is generally protected because employees cannot expect any reasonable expectation of privacy relative to websites they visit while they are at work and being paid by the employer for their services.[27] In short, there is no statutory right to privacy afforded to employees regarding their employment-related electronic communications.

To date, courts have consistently held that employees do not have any reasonable expectation of privacy regarding online communication, including internet usage and work e-mail systems.[28] The early precedent-setting case regarding e-mail monitoring, *Smyth v. Pillsbury*,[29] was heard in 1996. The court found that employees have no reasonable expectation of privacy because e-mail communications are voluntary and employer's interests in maintaining professionalism and preventing harassment in the workplace take precedent over any privacy expectations of employees. This reasoning was extended in another case, *McLaren v. Microsoft*,[30] where Michael McLaren, a Microsoft employee, had labeled some fold-

ers as "personal" on his computer and created private passwords by which he accessed them. The court found that the employer's ownership of the computer and the network preempted any presumption or expectation of privacy on the part of the employee. The court further held that any alleged privacy claims were rendered moot when an e-mail was transmitted to another person, hence becoming public.[31]

IV. The Next Wave of Monitoring — Social Networking Sites and Search Engines

Social networking, as noted above, is the latest significant trend in personal communications. However, a significant number of businesses have embraced social networking sites as a critical means of communication, public relations, promotion and marketing and branding. Social media is also being used to communicate with employees as well as with prospective employees about job opportunities and the employment relationship in general.

The combination of employer business use of social networking combined with its popularity among individuals who use it for personal reasons creates two strong simultaneous forces driving the proliferation of social networking. Use of social networking sites by employees is easy and inexpensive. Similarly, monitoring of employees' social network activities by employers is easy and inexpensive. No special technology or customized software program is needed for such monitoring. To conduct any kind of monitoring activity, an employer would only need to create a free account, even under a disguised identity, on a social networking site to gain access to the activities of any or all of its employees. Unless users of a social networking site restrict their personal account to "friends only," the accounts they create and their content are publically available. Some employees are aware of the possibility of employer monitoring as 29 percent of employees report having become both more private and conservative in their social networking endeavors for fear of employer discovery and retribution.[32] This is an especially risky issue for employees as an employer can shield their identity by using a pseudonym allowing them to learn about employee's off-work, personal life in a manner that the employee may not know who has actually gained access to the information the employee has posted.

Monitoring through the use of search engines is as equally quick, easy and inexpensive. Google or Yahoo searches, for example, can turn up information about employees which they employee may not have personally chosen to make public and/or information which was posted by others. Much of this information can be potentially embarrassing, such as information about legal proceedings.[33] However, it is probably much easier for an employer to find discomforting information about an employee on a social networking site as the purpose of such sites is to share information which is personal and sites such as Facebook seem to encourage individual self-expression.

Employers face an ethical question relative to whether, as part of due diligence in the hiring process, they should scour online networks and sources to discover information about prospective hires. A 2011 survey of HR executives conducted by the Society for Human Resource Management found that 26 percent of organizations were using search engines and 18 percent were using social networking sites to *screen*, rather than recruit,[34] applicants for employment. Of this group, 15 percent were using information gathered via search engines to disqualify candidates and 30 percent had used information found on social networking sites to disqualify an applicant.[35] However, a more general survey found that 95 percent of employers admitted to using social media sites to discover additional information about job applicants.[36] A third survey found that 45 percent of employers research social media sites as part of the routine screening of job applicants.[37]

While the survey results vary, it is very clear that employers are utilizing search engines and social media to discover information about job applicants and, in some cases, use this information to screen out applicants. Arguments in favor of utilizing such practices would include

the desire to ensure that the applicant provides the best "fit" with the company, particularly in light of how expensive recruiting activities can be. Many employers condone, if not encourage, hiring managers and human resources personnel to conduct such due diligence, feeling that the practice is certainly not unlawful and, given potential costs and risks associated with hiring the wrong candidate, an ethical if not necessary practice. Privacy advocates would argue that visiting the Facebook profile of a job applicant as part of the employer's screening of potential employees is both unnecessary and an invasion of privacy.

Once a job applicant becomes an employee, the appropriateness of such searches becomes even more ambiguous. While the same information obtained via social networking and search engine monitoring may be available post –hire as well as pre-hire, one could question the motivation of an employer's searches into existing employees' private personal lives outside of work. Once the practice became public within the workplace, such post-hire searches might greatly affect employee morale and trust[38] as in most cases an employer might monitor an employee's social networking activities and posts as a means of collective evidence to use against an employee for disciplinary purposes rather than simply wanting to get to know the employee better.

Issues related to work and employment which were previously "vented" among co-workers at the water cooler, in the cafeteria or in the rest room and now being vented publically online.

A number of recent situations have illustrated the consequences for employees of employer monitoring of employee activity online. After thirteen members of the Virgin Atlantic Airlines cabin crew expressed their impressions of employer, its planes and passengers as part of a Facebook group Virgin terminated them.[39] The airline could not find any "justification for using [Facebook] as a sounding board for staff of any company to criticize the very passengers who ultimately pay their salaries." When Boston-based Anglo Irish Bank employee Kevin Colvin told his supervisor he had to miss work due to a family emergency in New York, his supervisor checked his Facebook page the following day and discovered that Colvin had posted Halloween party pictures from the previous night with Colvin dressed as a green fairy holding a wand and can of beer. Colvin was fired for lying after his supervisor forwarded the photo to everyone in the office.[40]

Mario County FL Sherriff's office fired deputy Brian Quinn after Quinn posted a picture of himself on his MySpace page in full uniform with comments about women's breasts, binge drinking and nude swimming for "conduct unbecoming of an officer."[41] Dan Leone, a Philadelphia Eagles parking lot attendant, was terminated after six years of service when he posted derogatory comments on his Facebook page which criticized the Eagles for their failure to resign a player.[42] In yet another case, a server at Brixx Pizza in North Carolina berated a couple who left her a small tip on her Facebook page, mentioning her employer (Brixx) by name, and was fired as a result. In defending its action, Brixx claimed a violation of company policy against disparaging customers and criticizing the restaurant.[43]

These incidents illustrate the fact that issues related to work and employment which were previously "vented" among co-workers at the water cooler, in the cafeteria or in the rest room and now being vented publically online for a much wider audience. A disgruntled employee doesn't have to wait to get back to the office to express her or his feelings. Online networks provide an immediate opportunity to deal with issues and express feelings. While such public venting allows for spontaneity of expression, posts also cannot often be retracted and may continue to exist and be accessed long after the employee has "calmed down" or even had a change or heart about any specific incident. More so social network monitoring of existing

employees can allow employers to monitor activities and discover personal information which may or may not be work-related. The ethical issue for employers is that much of which may be discovered online is not related to job performance and how is such information to be used once it is discovered.

V. Where We Stand

As the above discussion illustrates, the American legal system has not kept up with the technological advances which have greatly altered how we communicate. The creation of new communication media which were previously unavailable and the availability of the means to monitor the usage and content by which people communicate raise the issue of the appropriateness of employer monitoring.

The only existing law which impacts communications, the Electronic Communications Privacy Act (ECPA),[44] was enacted in the 1980s in response to the kinds of electronic communications which were being utilized at that time. Title I of the EPCA[45] addresses electronic communications solely from the perspective of the interception of wire and aural messages. Despite the fact that e-mail was in its earliest stages of development at the time the EPCA was passed and social networking as we know it was non-existent, federal court decisions have applied the terms and conditions of the EPCA to e-mail. However, Title I provides for the express exemptions from the statue communications related to the normal course of business as well as those conducted on proprietary communication networks and systems. Consequently, employers have prevailed in every case in which employees have objected to monitoring as a violation of their privacy rights.[46]

Hence, employees currently enjoy no specific privacy rights in their communications and very limited protection against employer monitoring (unless such monitoring was targeted at a specific employee who alleges the monitoring was based on protected class status) and the possible consequences employers take in response to what they discover as part of any monitoring. Courts have also not overturned firings which have been based solely on derogatory postings on social networking sites. Employers have generally not been liable for adverse employment actions resulting from employee postings on social media sites unless the employer gained access to the information in violation of the website's agreed terms of usage or without consent.[47] However, because social networking is still a relatively new phenomenon in personal, mass public communication, it is understandable that no specific laws have yet been developed regarding employee and employer rights and responsibilities.

VI. National Labor Relations Act and Concerted Activity

Prior to the advent of social networking, the first case which tested the extent to which electronic communication by employees was protected under any federal law involved an online bulletin board system. In *Konop v. Hawaiian Airlines*,[48] the Ninth Circuit Court of Appeals held that an online bulletin board, established and maintained by a company pilot, used to discuss and criticize the employer's relationship with the employee union was protected concerted activity under the Railway Labor Act (RLA). Because the *Konop* court relied upon National Labor Relations Act (NLRA) in reaching its decision, which is typical in RLA cases, the *Konop* holding was considered precedent for interpretation of the NLRA relative to this issue.[49]

Given the advent of social networking and online employer monitoring of employees, the question has been raised as to whether the NLRA might provide employees some kind of protection against employer actions taken in regard to employee postings online. At this juncture, several complaints have been filed with the National Labor Relations Board (NLRB).

The first complaint was filed with the NLRB in November 2010. Danwmarie Souza, a union member/employee of the American Medical Response of Connecticut (AMR) ambulance service, posted negative comments about her supervisor on her Facebook page from her home computer after a work request she submitted had been denied. When some of her co-workers post-

ed supportive comments in direct response to her post, Souza posted further negative comments and was subsequently fired for alleged violation of the AMR's internet policy which prohibits employees from posting anything about AMR without express permission. While the employer stated that Souza was fired due to "multiple, serious complaints about her behavior," the NLRB reasoned that because Souza was communicating with her co-workers about her supervisor, even though it was in a public forum which could be accessed by others, she was engaging in concerted activity rather than being disloyalty to her employer. Concerted activity is protected under Section 7 of the NLRA, which prohibits employers from interfering with employees' efforts to work together to improve the terms and condition of their workplace and their employment. There was no court ruling in the case as the parties settled in February 2011. As part of the settlement AMR agreed to revise its company policies regarding employees' rights to communicate with each other about work-related matters.[50]

Protected concerted activity could include online discussion boards, or even the case of a single employee who discusses issues related to supervision.

However, in April 2011, the NLRB did not find unlawful another employer's decision to fire an employee because of inappropriate post to his Twitter account. When the Arizona Daily Star newspaper discovered tweets from one of its reporters which made sarcastic and derogatory comments about copy editors the employee was told by the managing editor that he was prohibited from airing grievances or commenting publically about the Daily Star. Subsequent to this incident the reporter posted additional sarcastic tweets which criticized both the Tucson police and the reporting of a local television station. When the reporter was terminated he filed a complaint with the NLRB who held that the reporter's behavior was neither protected nor concerted activity under the NLRA because it did not related to terms and conditions of employment nor did it seek to involve other employers on matters related to employment. While the associate general counsel of the NLRB recommended that the charge be dismissed, he did note that the employer had made statements which could be interpreted as impeding employees' Section 7 rights, specifically noting that the managing editor had told the employee that he was not allowed to tweet about anything related to work.[51]

In the AMR example, it is noteworthy that Souza was part of a unionized workplace. Employers need to remain cognizant, however, of the fact that nonunionized employees enjoy the same rights under the NLRA as those who already belong to unions, including the right to communicate with coworkers about working conditions in a concerted manner. In May 2011, the NLRB announced that it was suing Hispanics United of Buffalo, a nonprofit agency which provides various social services to low-income clients. After an employee of Hispanics United alleged that the organization's employees did not do enough to assist its clients, five co-workers responded to this statement, through Facebook postings, by criticizing their workloads and working conditions. Hispanics United terminated the Facebook-posting employees on the grounds of harassment of their co-worker who made the initial statement. The NLRB argued that the Facebook postings constitute protected concerted activity under Section 7 because they pertain to terms and condition of employment. In September 2011 an NLRB administrative law judge ruled against the employer, accepting the MLRB argument, and ordered that the five employees be reinstated with back pay.[52]

Section 7 of the NLRA provides all covered employees the right to engage in "concerted activities for the purpose of collective bargaining or other mutual aid or protection." It is critical however, that in order to receive protection that the employee's actions or communications not be simply on her or his own behalf nor should the employee disparage the employer, display blatant insubordination or distribute or publicize confidential information to which the employee

is privy.[53] Section 7 protection would not be afforded in such instances.

Regardless of whether a workplace is unionized or non-union, any employer policy which attempts to impede employees' abilities and rights to communicate outside of the workplace regarding wages, hours, supervision or working conditions would be subject to a Section 7 challenge. Such protected concerted activity could include online discussion boards, as noted in the *Konop* case, or even the case of a single employee who discusses issues related to supervision. Although there has been little commentary about how social media could be used as a means of organizing workplaces, the NLRB interpretation issued in AMR could easily be seen by union organizers as a new means to communicate with workers who are being recruited by the union for representation. Both pro-union employees and organizers themselves are afforded opportunities to communicate with workers via social media and networks that were previously unavailable, more cumbersome and/or more costly. Social networking has changed the way in which we communicate and this is particularly so for employees who wish to express themselves about working terms and conditions which apply to others. Given the above discussion it seems inevitable that social media will be embraced by labor unions as a means and strategy for not only communicating with existing union members but, perhaps more important, a means to communicate with employees of companies which are being targeted for organization.

VII. Summary

Social networking is here to stay as not only have individuals embraced it as a vital means of communication, organizations have similarly embraced it as a vital 21st century means of marketing and promotion and conducting business. The question remains as to whether employees are entitled to a reasonable amount of privacy in their personal, public communications on social networking sites. At this juncture, unless such postings can be considered concerted activity, employers are free to take action against employees based on postings which do not sit well with the employer. However, the NLRB is apparently readily to vigorously investigate any allegations of alleged suppression of or intimidation related to concerted activity but even then there is some presumption of a duty of loyalty to the employer and limitations as to how far an employee can go.

While numerous states have passed laws which restrict employer actions which are the result of an employee's legal off-duty conduct, there is no body of law which addresses the issue of employer monitoring of and resultant discovery of information posted on social networking sites. Employers can be fair-minded in developing policies which balance business needs and any reasonable perceived privacy expectations employees could have but in the interim, until such case law is developed, the only protection employees potentially have against employer actions based on discovery of social networking posts is the defense of protected concerted activity under the NLRA. However, while the NLRB has been quick to file suit in such cases, no court has yet to rule on this interpretation. In the meantime, employees need to use discretion and judgment with their posts, realizing the perpetuity issue associated with hitting the "send" or "enter" button on the keyboard. ■

ENDNOTES

1 Wikipedia, http://en.wikipedia.org/wiki/Facebook, retrieved 6 January 2012.

2 New York Times, http://topics.nytimes.com/top/news/business/companies/facebook_inc/index.html, retrieved 6 January 2012.

3 Wikipedia, *supra* note 1.

4 Jeremiah Owyang, *A Collection of Social Networks Stats for 2010*, http://www.web-strategist.com/blog/2010/01/19/a-collection-of-social-network-stats-for-2010/, retrieved 6 January 2012.

5 Wikipedia, http://en.wikipedia.org/wiki/Twitter, retrieved 6 January 2012.

6 Lauren Leader-Chivee and Ellen Cowan, *Networking the way to success: online social networks for workplace and competitive advantage,* http://findarticles.com/p/articles/mi_6768/is_4_31/ai_n31909656/, retrieved 6 January 2012.

7 Society for Human Resource Management, *SHRM Survey Findings: The Use of Social Networking Websites and Online Search Engines in Screening Job Candidates*, 25 August, 2011.

8 Leader-Chivee, *supra* note 6.

9 Sarah Perez, *A Growing Acceptance of Social Networking in the Workplace,* http://www.readwriteweb.com/enterprise/2009/07/a-growing-acceptance-of-social-networking-in-the-w.php, retrieved 6 January 2012.

10 See Am. Mgmt. Ass'n & The ePolicy Inst., *2007 Electronic Monitoring & Surveillance Survey 4* (2008), *available at*http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf (surveying employer monitoring

practices in various areas such as the Internet, e-mail, computer usage, etc.)

[11] *Id.* at 1.

[12] *Id.* at 5 (stating that twenty-six percent of employers monitor all employees' e-mail accounts and seventeen percent of employers only monitor the e-mail accounts of employees in selected job categories).

[13] *Id.* (reporting that seventy-three percent of all employers that monitor employee e-mails do so via software monitoring programs).

[14] *Online Spying: Remote Computer Spyware Software*, Online-Spying.com, http://www.online-spying.com/webmail-spy.html (last visited Oct. 7, 2010). *See also* Rachel Konrad & Sam Ames, *Web-Based E-mail Services Offer Employees Little Privacy*, cnet News (Oct. 3, 2000), http://news.cnet.com/2100-1017-246543.html (stating that, "unfortunately, security experts say many employees would be surprised to know that Web-based email services also offer little privacy. Messages sent via a Yahoo or Hotmail account … are just as accessible [as employer-created e-mail accounts] to nosy employers.").

[15] Am. Mgmt. Ass'n & The ePolicy Inst., *supra* note 10, at 1.

[16] Carolyn Holton, *Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem,* 4 Decision Support Systems, 46, 853-864 (2009).

[17] Christopher Pearson Fazekas, *1984 Is Still Fiction: Electronic Monitoring In the Workplace and U.S. Privacy Law,* 15 Duke L. & Tech. Rev. 1-16 (2004).

[18] *See, e.g.*, Blakey v. Cont'l Airlines Inc., 751 A.2d 538, 543–44 (N.J. 2000) (discussing the facts of a sexual harassment case filed by a female airline pilot claiming, among other things, that her coworkers posted sexually explicit comments about her on Continental Airlines' online bulletin board).

[19] *See, e.g.*, Lisa Scott & Ross Tate, *Monitoring Internet Usage—Spring 2010,* Ass'n of Local Gov't Auditors (2010), http://www.governmentauditors.org/index.php?option=com_content&view=article&catid=47:accounts&id=594:monitoring-internet-usage-spring-2010&Itemid=123 (reiterating that employee Internet use for personal reasons can cause "[b]andwidth and storage shortages [sic] [particularly] from peer to-peer [sic] file sharing and audio/video streaming."); and William P. Smith and Filiz Tabak, *Monitoring Employee E-mails: Is There Any Room for Privacy?* 23 Academy of Management Perspectives, (4), 33-48 (2009).

[20] *See, e.g.*, Jared A. Favole, *Ex-Bristol-Myers Employee Charged with Stealing Trade Secrets*, Barclays Latitude Club (Feb. 3, 2010), http://www.barclays.com/latitudeclub/er_gr_global_news_article.html?ID_NEWS=133949142 (discussing accusations against a Bristol Myers' technical operations associate for allegedly stealing company trade secrets in order to form a competing company in India); Elinor Mills, *Microsoft Suit Alleges Ex-Worker Stole Trade Secrets*, cnet News (Jan. 3, 2009), http://news.cnet.com/8301-10805_3-10153616-75.html (stating that an ex-employee "allegedly downloaded confidential documents onto his company-issued laptop … and then allegedly used a file-wiping program and a 'defrag' utility designed to overwrite deleted files in order to hide the tracks.").

[21] Smith and Tabak, *supra* note 19, at 34.

[22] Laura P. Petrecca, *More employers use tech to track workers,* USA Today, 17 March, 2010.

[23] *See, e.g.*, Mia Shopis, *Employee Monitoring: Is Big Brother a Bad Idea?*, SearchSecurity.com (Dec. 9, 2003), http://searchsecurity.techtarget.com/news/interview/0,289202,sid14_gci940369,00.html (quoting an expert in electronic monitoring who stated that "[e]mployee monitoring is a bad idea … when it's used for Big Brother and micromanagement purposes. Organizations would be better off not doing it if they're going to scrutinize their employees' every move. If it creates a morale problem (and it will if it's not handled properly) all of its value is diminished."). More generally, employee monitoring can have the following negative effects: 1. An employee may suffer loss of self-esteem if she interprets the monitoring to indicate a lack of trust in her.; also, Smith and Tabak, *supra* note 19, at 43.

[24] Am. Mgmt. Ass'n & The ePolicy Inst., *supra* note 10, at 1.

[25] *Id.* at 8–9.

[26] Encouragingly, seventy-one percent of employers monitoring employee e-mail notify such employees prior to any monitoring. *See id.* at 5 (stating that eleven percent of employers do not notify employees while another eighteen percent do not know whether e-mail monitoring took place).

[27] *See, e.g., Doe*, 887 A.2d at 1167 (upholding an employer's Internet monitoring policy, questioning whether, "with actual or imputed knowledge that Employee was viewing child pornography on his computer, was defendant under a duty to act, either by terminating Employee or reporting his activities to law enforcement authorities, or both?" and concluding that such a duty exists).

[28] Tanya E. Milligan, *Virtual Performance: Employment Issues in the Electronic Age*, 38 Colorado Lawyer (2), 29-36 (2009).

[29] 914 F. Supp. 97, 100 (ED Pa. 1996).

[30] 1999 WL 339015, 1999 Tex. App. LEXIS 4103 (Tex. App.-Dallas May 28, 1999).

[31] Michael Rustad and Sandra R. Paulsson, *Monitoring Employee E-Mail And Internet Usage: Avoiding The Omniscient Electronic Sweatshops: Insights From Europe*, 7 University of Pennsylvania Journal of Labor & Employment Law, 829-904 (2005).

[32] *See, e.g., Deloitte, Social Networking and Reputational Risk in the Workplace 4* (2009), *available at*http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_2009_ethics_workplace_survey_220509.pdf., at 12.

[33] *See, e.g.,* Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring,* 48 American Business Law Journal, (2), 285-369 (2011).

[34] A different survey, also conducted by the Society for Human Resource Management in 2011, found that 56% of organizations use social media sites to *recruit* applicants, with 95% using Linkedin, 58% using Facebook and 42% using Twitter. This 56 % represented an increase from 34% just three years earlier in 2008. SHRM Research Spotlight: Social Networking Website and Staffing, http://www.shrm.org/Research/SurveyFindings/Documents/Social%20Networking%20Flyer_FINAL.pdf, retrieved 6 January 2012.

[35] Society for Human Resource Management, *supra* note 7.

[36] Alexis Madrigal, *What You Shouldn't Post on Your Facebook Page If You Want A Job*, http://www.theatlantic.com/technology/archive/2011/10/what-you-shouldnt-post-on-your-facebook-page-if-you-want-a-job/246093/, retrieved 6 January 2012.

[37] Damian R. LaPlaca and Noah Winkeller, *Legal Implications of the Use of Social Media: Minimizing the Legal Risks for Employers and Employees*, 5 J. Bus. Tech L. Proxy 1 (2010), http://www.law.umaryland.edu/academics/journals/jbtl/proxy/5/5_001_LaPlaca.pdf, at 8.

[38] Ciocchetti, *supra* note 33.

[39] John Browning, *Employers Face Pros, Cons with Monitoring Social Networking*, Houston Bus. J. (Feb. 27, 2009), http://www.bizjournals.com/houston/stories/2009/03/02/smallb3.html.

[40] *Id.*

[41] *Id.*

[42] Kabrina Krebel Chang, *Facebook Got Me Fired*, Builders and Leaders, http://www.bu.edu/builders-leaders/2011/05/18/facebook-got-me-fired/ 34-35, retrieved 6 January 2012.

[43] *Id.*

[44] Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. § 2510-2522.

[45] Stored Communications Act, 18 U.S.C. §§ 2701-12

[46] Smith and Tabak, *supra* note 19, at 38.

[47] LaPlaca and Winkeller, *supra* note 36, at 7.

[48] 236 F.3d 1035 (9th Cir.2001).

[49] Scott Grubman, *Think Twice Before You Type: Blogging Your Way to Unemployment*, 42 Georgia Law Review 615 (2008); Carson Strege-Flora, *Wait! Don't fire that blogger! What Limits Does Labor Law Impose on Employer Regulation of Employee Blogs?*, 2 Shidler J. L. Com. & Tech. 11 (Dec. 16, 2005), *at* <http://www.lctjournal.washington.edu/Vol2/a011Strege.html>

[50] Chang, *supra* note 41, at 35.; Maria Greco Danaher, *NLRB Settles Complaint Based on Facebook Posts as 'Concerted Activity'*, http://www.shrm.org/LegalIssues/FederalResources/Pages/NLRBSettlesComplaintFacebook.aspx, 9 February 2011, retrieved 6 January 2012.

[51] Allen Smith, *NLRB: Discharge of Employee for Inappropriate Tweets Was Lawful,* http://www.shrm.org/LegalIssues/FederalResources/Pages/NLRBInappropriateTweets.aspx**,** 13 May 2011, retrieved 6 January 2012.

[52] Maria Z. Stearns, *NLRB Actively Engaged in Examining Employee Social Media Use*, http://www.rutan.com/files/Publication/46b9dcfa-2034-4c1f-a7ce-5907c824a6de/Presentation/PublicationAttachment/e806e8b8-2e0d-48ae-9ed3-5f095a222d18/Society%20for%20Human%20Resource%20Management.pdf, 16 September 2011, retrieved 6 January 2012

[53] Nancy King, *Labor Law for Managers of Non-Union Employees in Traditional and Cyber Workplaces*, 40 American Business Law Journal, (4), 827-883 (2003); Robert Sprague, *Fired for Blogging: Are There Legal Protections for Employees Who Blog?*, 9 U. Pa. J. Lab. & Emp. L. 355 (2007).