PRIVACY AND TODAY'S TECHNOLOGY IN THE WORKPLACE

Brian J. Moore and Samuel T. Long
Dinsmore & Shohl LLP
707 Virginia Street East
Suite 1300
Charleston, WV 25301
Ph: (304) 357-0900
Fax: (304) 357-0919
brian.moore@dinsmore.com
samuel.long@dinsmore.com
www.dinsmore.com
www.wvlaborandemploymentlaw.com

Introduction

It is becoming increasingly common for employers to provide employees with computers, cell phones, and wireless networks, presumably, for business use. Studies have shown, however, that employees spend a significant amount of time engaging in personal use of technology in the workplace. Thus, it is no surprise that 83% of surveyed employers report having a policy governing personal use of employer e-mail accounts. What is somewhat surprising, however, is that of the 586 employers surveyed by the ePolicy Institute, only 43% reported having a policy governing the use of personal cell phones use during working hours, and only 33% reported having a policy governing the use of personal text messaging tools during working hours. Similarly surprising is the fact that only 43% of surveyed employers reported having a policy governing visits to personal social networking sites or video sharing sites during work hours. These figures have undoubtedly increased since this report, but even those employers who do have policies are often faced with questions regarding the legality of these policies.

A. Balancing an employer's right to know vs. employee's privacy

In the modern workplace, employers are presented with the difficult question of whether employees have a right to privacy and/or reasonable expectation of privacy in the workplace. This issue is particularly complex in the area of social media and other electronic communications. Employers must be cognizant of invading employees' privacy through monitoring the use of these sites. Employees have a privacy interest in the content of information if the employee has taken reasonable efforts to keep the information private and the employee derives economic, personal, emotional, or other

value in keeping the information private. An employer infringes upon this employee privacy if the employee's interest in keeping the information private from the employer outweighs the employer's interest in obtaining the information and the employer nevertheless requires that the employee provide the information to the employer.[1]

In order to have a privacy interest in the information, an employee must take reasonable efforts to keep the information private. If an employee has not restricted access to the information, then the employee arguably did not take reasonable steps to keep the information private from the employer. For example, if an employee has a web page that is accessible and open to internet users, the employee has not taken reasonable steps to keep posted information private. In contrast, if an employee has a personal web page that is accessible only to those who enter a proper username and a password, and the employee only provides passwords to her friends and family, then the employee has taken reasonable steps to keep the information private. Therefore, in the second example, the employee has a privacy interest in the information on her web page.[2]

Along with common law privacy, the Stored Communications Act ("SCA") also comes into play for employees' use of social media sites. The SCA is a federal statute that prohibits third parties from accessing electronically stored communications (*e.g.,* e-mail or Facebook entries) without proper authorization.[3] Pursuant to the SCA, an offense is committed by anyone who: "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided;" or "(2) intentionally

---

[1] Restatement of Privacy, § 7.03 Privacy Interests in Content Information.
[2] *Id.*
[3] 18 U.S.C. § 2701.

exceeds an authorization to access that facility; and thereby obtains . . . [an] electronic communication while it is in electronic storage in such system."[4] "Electronic storage" is defined in an earlier part of the Wiretap Act as: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[5] The SCA aims to prevent hackers from obtaining, altering, or destroying stored electronic communications.[6]

Konop v. Hawaiian Airlines, Inc. provides an example of the applicability of this statute to this issue. *Konop*, a case from the United States Court of Appeals for the Ninth Circuit, concerned the denial of summary judgment to an employer on the employee's SCA claim.[7] In *Konop*, an airline pilot sued his employer, alleging that the airline viewed the pilot's secured website in violation of the SCA. The pilot maintained a website, in which he criticized the airline, the airline's officers, and the union. Airline employees were eligible to access the site by logging in with a username and password created by the individual employees. Management employees were expressly excluded and were not eligible to create usernames or access the site.[8]

The vice president of the airline was concerned that the pilot was making untruthful allegations on the website. The vice president asked an eligible employee to assist him with accessing the website. The vice president was upset by the pilot's

---

[4] *Id.*
[5] 18. U.S.C. §§ 2510(17), 2711(1) (definitions of Wiretap Act are applicable to Store Communications Act).
[6] *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp.2d 497 (S.D.N.Y. 2001).
[7] *Konop v. Hawaiian Airlines*, 302 F.3d 868 (9th Cir. 2002).
[8] *Id.* at 872-73.

accusations on the website and contacted the union regarding the website.[9] Regarding the pilot's SCA claim, the Court found that there was an issue of fact as to whether the eligible employee was a "user" of the website -- in other words, whether the eligible employee has the power to "authorize" the vice president, a third party, to access the website. If the vice president is authorized to access the website, then the employer would be exempt from liability under the SCA.[10]

In addition to the SCA, employers also need to recognize potential issues under the National Labor Relations Act ("NLRA").[11] An employer monitoring employees' social media sites may have a chilling effect on employees' communications regarding the terms and conditions of their employment. In *Endicott Interconnect Technologies, Inc.*, the National Labor Relations Board ("NLRB" or "the Board") found that the company had violated Section 8(a)(1) of the NLRA. In *Endicott*, the NLRB found an employee's posting on a public-forum website -- in favor of union representation at the company, and criticism of recent management of the company -- was protected conduct under the NLRA. The company was found to have violated Section 8(a)(1) by threatening, and then discharging, the employee for his statements on the website.[12]

---

[9] *Id.* Note that the Court first dismissed the pilot's claim under the Electronic Communications Protection Act ("ECPA"), known as the Wiretap Act, because the vice president's act of logging into the site did not constitute an "interception" of an electronic communication and was therefore not prohibited by the ECPA. *Id.* at 879.

[10] *Konop, supra* note 11, 302 F.3d at 880; *See also Pietrylo v. Hillstone Restaurant Group d/b/a Houston's*, No. 06-5754, 2008 U.S. Dist. LEXIS 108834 (D.N.J. July 25, 2008) (upholding a jury verdict with punitive damages in which the company was held liable under the SCA for intentionally accessing a chat group on an employee's Myspace account without having received authorization from the Myspace member to join the group).

[11] 29 U.S.C. § 157.

[12] 345 NLRB No. 28 (Aug. 27, 2005).

In a similar case, the NLRB held that the company's policy prohibiting employee use of the company e-mail system for "non job-related solicitations" did not violate Section 8(a)(1) of the NLRA. In *The Guard Publishing Company d/b/a The Register-Guard*, the company implemented a policy that communications systems, including e-mail, are not to be used for non job-related solicitations. The company was aware that employees sent personal e-mails such as baby announcements, party invitations and sports tickets, but there was no evidence employees used e-mail to solicit support for any outside cause or organization other than the annual United Way fundraiser. An employee received two written warnings for sending e-mails to employees at their company e-mails soliciting union support.

The union filed a charge alleging the company violated Section 8(a)(1) by maintaining its policy and discriminatorily applying it against union-related e-mails. The Board compared e-mail systems to other types of employer-owned property -- such as bulletin boards, telephones and televisions -- and found that there was no statutory right to use an employer's equipment or media as long as the restrictions are not discriminatory. The Board also found that the employee's e-mails soliciting union support were different than the occasional e-mails about baby announcements, and that the e-mails supported an outside group or organization. Ultimately, the Board found that employees have no statutory right to use the company e-mail system for Section 7 purposes under the NLRA (the rights of employees to form, join, or assist labor organizations, and other concerted activities for other mutual aid or protection).[13]

[13] 351 NLRB No. 70 (Dec. 16, 2007).

Along with these potential legal issues, employers must be aware of issues that arise during litigation after accessing information from employees. Some courts have found that employers violate state professional conduct ethics rules by retaining and using e-mails protected under the attorney-client privilege doctrine.[14] For example, in *Nat'l Econ. Research Assoc. v. Evans*, a Massachusetts Superior Court ruled that an employee did not waive the attorney-client privilege for personal e-mails sent and later accessed by his employer.[15] The court denied the company's motion to compel disclosure of attorney-client communications between a past employee and his attorney.

Many of these e-mails were on the employee's work computer using his personal e-mail account, not his company account. The court held that the employee did not waive the attorney-client privilege because he did not use the company intranet or e-mail, and he did not forward the communications to his company intranet or save them in a file on his company laptop. Therefore, the court found that the employee took adequate steps to protect the confidentiality of his privileged communications.[16] The law on this issue depends on the employer's specific jurisdiction. However, the lesson for employers is to have a properly drafted e-mail policy that is clearly disseminated to employees and updated as appropriate.[17]

---

[14] Sean Carnathan, *Attorney-Client Privilege Trumps Workplace Regulations*, ABA Section of Litigation, Fall 2009, Vol. 35 No. 1.
[15] No. 04-2618 BLS2, 2006 Mass. Super. LEXIS 371 (Mass. Super. Aug. 2, 2006).
[16] *Id.* at *11.
[17] Carnathan, *supra* note 15.

B. Wireless devices: monitoring and creating policies regarding electronic communications, data security

Many employers supply certain employees with cell phones to use in the performance of their job duties. Unsurprisingly, however, these devices are also frequently used for non-business purposes. Thus, employers must make the decision whether to monitor its employees' use of these devices and whether to reprimand employees for improper use. Moreover, it is unclear under what circumstances it is appropriate to discipline employees for improper use of these devices.

Employment lawyers hoped to receive some clarity on this issue several years ago when the U.S. Supreme Court considered the case of *City of Ontario, California v. Quon*.[18] In that case, the employer terminated an employee for transmitting sexually-explicit text messages on an employer-owned pager. The employer paid for the pager's service plan, but the employee reimbursed the employer for his personal use of the pager beyond the allotted minutes of the plan. When the employer performed an audit of pager use, to see if the service plan needed changed, it discovered the explicit messages and terminated the employee. The trial court upheld the termination, but the Ninth Circuit Court of Appeals reversed. Both courts ruled that the employee had a reasonable expectation of privacy, but disagreed on whether the employer's interests were sufficient to override the employee's right. During the subsequent appeal, many hoped that the Supreme Court would shed some light on how to balance an employee's right to privacy with an employer's right to run its business. The first warning sign that this would not happen occurred during oral argument of the case. In discussing the concept of text-

[18] 130 S. Ct. 2619 (2010).

messaging, Chief Justice Roberts commented "I thought, you know, you push a button; it goes right to the other thing." Justice Scalia replied "You mean it doesn't go right to the other thing?"

Indeed, the Supreme Court eventually ruled that the case could be resolved without determining the extent of the employee's privacy rights. Assuming that the employee did have a reasonable expectation of privacy, the Court held that the employer's interest in auditing the pager records overrode that right. Thus, the Court declined to rule on what it called an issue of "far-reaching significance," stating that such a decision would be premature because it is "uncertain how workplace norms, and the law's treatment of them, will evolve." According to the Court:

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. ***The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear***. . . . ***Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices***. . . . Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are communicated. . . . ***A broad holding concerning employees' privacy expectations vis-à-vis employer-***

> ***provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds.***[19]

Consequently, the *Quon* decision shed little light on the extent of an employee's privacy rights when texting on an employer-owned device. However, this decision informs employers that they need well-conceived policies establishing expectations for employees with respect to digital privacy in the workplace. Further, employers must also be familiar with existing and emerging digital technologies to identify and address potential privacy issues before they present legal problems.

Data Security

There have been numerous incidents in recent years which highlight the need for employers, and their employees, to vigilantly protect company data. For example, in December 2013, Target discovered a security breach in which the credit card information for approximately 40 million customers was stolen. In addition to credit card numbers, information stolen included names, mailing address, email address and phone numbers for up to 70 million customers. In 2014, Verizon issued its Data Breach Investigations Report in which it analyzed more than 63,000 security incidents and nearly 1,400 confirmed breaches. It found that three out of four of network intrusions exploited weak or stolen credentials. Moreover, nearly one in three of these attacks utilized social tactics (information gained via e-mail, phone calls, and social networks) to assist with gaining access. Thus, a company's data must is particularly susceptible to breach when its

[19] *Quon,* 130 S. Ct. at 2629-30 (emphasis added).

employees leave devices, such as laptops or cell phones, unattended or in an unsecure location.

To avoid costly data breaches, employers should adopt the following best practices. First, employees must be required to use strong passwords and, if possible, require two-factor authentication on remote access accounts. Second, every employee device must be equipped with the latest antivirus, firewalls, and intrusion detection software. Third, companies must implement monitoring and auditing processes to review potential security risks before they become an issue. Finally, and perhaps most critically, employers must educate their employees on their duty to protect company data. An informed user is more likely to use company devices responsibly and take fewer risks with valuable company data, including e-mail.

C. Use of social networking sites in the employment context: risks, best practices, and policies

Social Media in the Workplace

Social media sites are great employer tools for marketing and advertising purposes. Additionally, social media sites provide a good resource for recruiting. Employers are able to easily research applicants online. Social media can provide useful insight into whether a candidate will fit with the company culture. The list of justifications for screening applicants through social media is extensive and the number of employers who are taking advantage of it continues to grow. Even the Obama administration required candidates seeking positions in the administration to disclose any potentially damaging or embarrassing e-mails, blogs, and text messages they had

produced, as well as provide a link to their social media sites so that they could be inspected.

A story reported on NBCNEWS.com provides a real world example of social media as a tool in recruitment. The story concerned a corporate recruiter charged with hiring physicians. The recruiter would log into Facebook to view a candidate. In one particular incident, the recruiter found pictures of a candidate taking her shirt off at parties, and called the candidate to request an explanation. He was unimpressed and did not offer her the position, stating "[H]ospitals want doctors with great skills to provide great services to communities. They also don't want patients to say to each other, 'Heard about Dr. Jones? You've got to see those pictures.'"

Employers have also found social media useful during litigation and in conducting investigations. In addition, there are sometimes advantages to allowing employees to use social media in the workplace – some employers even encourage it. Business justifications for allowing on-the-clock use of social media include (1) strengthening of professional relationships; (2) promoting the company; and (3) allowing employees to share information with each other.

Along with the benefits, there are disadvantages to using social media in the workplace. One disadvantage for employers is in the form of lost productivity resulting from the time employees spend on these sites, which is hard to track given the prevalence of mobile devices. Of course, employers have disciplined and discharged employees based on their use of social media. For example, in March 2009, the Philadelphia Eagles fired an employee for criticizing the Eagles on his Facebook page. Dan Leone, a gate

worker at the team's stadium, posted an angry, expletive-laced complaint about the team's failure to re-sign safety Brian Dawkins. Management found out and fired him for making the team look bad.

Legal Issues Surrounding Social Media in the Workplace

There are, of course, a number of legal issues that may arise with the use of social media in the workplace. In addition to the privacy concerns addressed above, one issue that arises with using social media to pre-screen candidates is the possibility of discrimination claims. By screening an applicant's Facebook page, for instance, an employer may become aware of a candidate's race, religion, gender, sexual preference, age, nationality, marital status, and/or disability. Through these searches, employers may become aware of information which they would not have otherwise known - or be legally entitled to know - through a simple interview. The issue then becomes proving that this information was not the basis for the employer's decision not to hire a candidate.[20] Employers can take actions to protect themselves from these types of discrimination claims, however. First, they should have in place a policy regarding the use of social media in conducting background checks. Second, they should consistently apply the policy. Third, they should limit such screenings to a few well-trained individuals and have non-decision makers search and filter the information.

[20] This pre-screening issue potentially implicates a number of federal employment statutes including the Americans with Disabilities Act ("ADA"), Title VII of the Civil Rights Act of 1964 ("Title VII"), the Age Discrimination in Employment Act ("ADEA"), and the Uniformed Services Employment and Reemployment Rights Act ("USERRA"), among other statutes providing protection for employees and applicants.

D. Off the job behavior, e.g., blogging and dating

As is appropriate, employers have limited ability to control the behavior of employees outside of the workplace. The distinction between on and off the job activity becomes blurry, however, in the digital medium. Employers should adopt policies regarding employee use of the internet, and, in particular, social media, to outline the scope of acceptable behavior. To address this issue, the NLRB has provided guidelines on the scope of permissible restrictions on employee use of social media.

The following are some specific examples of the NLRB's views on particular language:

(1) *A ban on posting "confidential" or "non-public" information.* The NLRB believes this language is improper because employees could construe it as prohibiting them from discussing information regarding the terms and conditions of their employment.

(2) *A ban on posting "proprietary," "trade secret," or "attorney-client privileged" information.* This is permissible because it is more specific, and is "clearly intended to protect the employer's legitimate interest in safeguarding its confidential proprietary and privileged information."

(3) *A prohibition on "inappropriate" or "unprofessional" comments.* According to the Board, "this provision improperly proscribes a broad spectrum of communications that would include protected criticisms of the employer's labor policies or treatment of employees."

(4) *A prohibition on "harassing, threatening, intimidating, bullying, or discriminatory" comments.* This is permissible because it is more specific, and limited to comments that are clearly unlawful, and not protected by the Act.

(5) *A ban on "disparaging" or "misleading" comments.* This would include criticism of the employer or management concerning the terms and conditions of employment and is, therefore, overly broad.

(6) *A prohibition on "harassing, threatening, intimidating, bullying, or discriminatory" comments.* This is permissible because it is more specific, and limited to comments that are clearly unlawful, and not protected by the Act.

(7) *A ban on "disparaging" or "misleading" comments.* This is overly broad because it would include criticism of the employer or management concerning the terms and conditions of employment.

(8) *A ban on "slanderous" or "maliciously false" comments.* This is permissible because it is more specific, and focused on comments that are unlawful and therefore not protected.

(9) *A ban on employees identifying themselves as employees on social media.* This could prohibit legitimate discussion of the terms and conditions of employment and is, therefore, overly broad.

(10) A *ban on posting comments in the name of the employer or in a manner that could reasonably be attributed to the employer, without prior written authorization.* This is permissible because it is more specific and aimed directly at the employer interest.

(11) *Encouraging employees to resolve conflicts by speaking directly with another employee, rather than posting complaints online.* According to the Board, an employer cannot tell employees to use internal resources rather than airing grievances online because it will preclude or inhibit employees from protected activity seeking redress through alternative forums.

(12) *Suggesting that employees resolve conflicts in person.* This is permissible because it does not direct employees to do anything.

(13) *A policy relating to exercising good judgment and requiring employees who disclose affiliation with the employer to make posts "completely accurate and not misleading."* This is overly broad and could be interpreted to apply to protected discussions and criticisms of the employer's policies and treatment of employees.

(14) *"When in doubt, check with the employer."* This is overly broad. Any rule that requires an employee to secure permission from an employer as a precondition to engaging in Section 7 activities violates the Act.

(15) *A policy relating to "friending" co-workers.* This is overly broad because it would discourage communications among co-workers, and thus it necessarily interferes with Section 7 activity.

(16) *"The employer's social media policy will be administered in compliance with applicable laws and regulations (including Section 7 of the National Labor Relations Act)."* Generally speaking, a savings clause will not cure the ambiguities in a social media policy that contains overbroad rules.[21]

[21] *General Motors*, Case 07-CA-053570.

Accordingly, employers should implement restrictions on employee activity outside the workplace which conforms with these guidelines, as discussed further below.

E. Privacy issues and information disclosure

It is essential for employers to develop a social media policy to establish expectations for employees with respect to digital privacy in the workplace. Employers must consider the many goals that the policy intends to cover, such as:

- Protecting the company's trade secrets, confidential, proprietary and/or privileged information;
- Protecting the company's reputation;
- Protecting the privacy of employees; and
- Establishing guidelines for whether use of social media sites during working hours is permitted, and if so, under what circumstances.

Employers must also consider the parameters in developing a new policy, such as:

- Setting forth the potential for discipline, up to and including termination, if an employee misuses social media sites relating to employment;
- Establishing a reporting procedure for suspected violations of the policy;
- Enforcing the policy consistently and with regard to all employees;
- Reiterating that Company policies, including harassment and discrimination policies, apply with equal force to employees' communications on social media sites;
- Reminding employees that the computers and e-mail system are Company property intended for business use only, and that the Company may monitor computer and e-mail usage; and
- Arranging for employees to sign a written acknowledgment that they have read, understand, and will abide by the policy.

F. Case law studies

The NLRB's Views on Social Media

The NLRB has issued several decisions focused on employer social media policies since 2010, when the NLRB's regional offices first began receiving charges related to specific instances of discipline related to employees' Facebook postings. In particular, the question often arises of whether an employee's activity on social media is protected under the NLRA. The NLRA is typically thought of as an Act governing unionized operations. Certain provisions of the Act, however, apply to both union and non-union employers. Specifically, Section 7 of the Act protects concerted activity by employees:

> Employees shall have the right to self-organization, to form, join or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, and shall also have the right to refrain from any or all such activities except to the extent that such a right may be affected by an agreement requiring membership in a labor organization as a condition of employment as authorized in section 8(a)(3) of this Act.[22]

Concerted activity must normally involve two or more employees. Thus, the NLRB has focused on two primary issues: (1) employers who terminate employees for their social media activity and (2) employer social media policies in general. The Board has reviewed several hundred social media cases in the past few years. A number of those cases have resulted in charges, hearings, and/or settlements with the Board. These cases

[22] 29 U.S.C. § 157.

typically involve either an employee who was disciplined/discharged because of social media activity, or review of an employer policy on the subject.

In order to be protected, social media posts must be about employees' terms and conditions of employment. The most common examples would be wages and benefits, treatment by supervisors, work assignments, and discipline of employees. Again, the posts must involve two or more employees. Typically, a post solely for the benefit of one person would not be protected unless it is a recitation of an issue previously discussed with other employees. Interestingly, the Board has noted that using vulgarity does not remove speech from protected status under the Act. For example, the Board has found calling supervisors "liar and a bitch," "an egotistical f**k," and a "f**king son of a bitch are protected under the Act.

The Board is not just looking for policies that expressly prohibit employees from engaging in protected activity (for example, a policy prohibiting employees from discussing their salary information). If the rule does not explicitly restrict protected activities, it will only violate Section 8(a)(1) upon a showing that: (1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights.

The best guidance as to the NLRB's view on what an employee would reasonably construe as prohibiting Section 7 activity is contained in three Memoranda issued over the past couple of years by the NLRB's General Counsel, most recently on May 30, 2012. The NLRB has invalidated social media policies that employees could potentially

interpret as infringing on Section 7 rights, rather than policies that employees would reasonably interpret that way. For example, the NLRB has declared that a policy encouraging employees "to resolve concerns about work by speaking with co-workers, supervisors, or managers," is unlawful. In contrast, however, the Board later stated that "[a]n employer may reasonably suggest that employees try to work out concerns over working conditions through internal procedures." The most important takeaway point from the NLRB Memoranda, and the one with the most practical application, is that the NLRB's opinion on the validity/invalidity of an employer's social media policy is likely to be based, in large part, on whether the employer has taken steps to avoid "ambiguity" and "overbreadth." The Board frowns upon policies and language that could be interpreted too broadly. The Board has advised that employers draft "rules that clarify and restrict their scope by including examples of clearly illegal or protected conduct, such that they could not reasonably be construed to cover protected activity."

In sum, an employer can glean from the NLRB's statements that (1) rules that are ambiguous as to their application to Section 7 activity and that contain no limiting language or context to clarify that the rules do not restrict Section 7 rights are unlawful and (2) rules that clarify and restrict their scope by including examples of clearly illegal or unprotected conduct, such that they could not reasonably be construed to cover protected activity are lawful.

Conclusion

To compete in today's economy, employers must embrace technology and the efficiencies that it can create. Employers and their counsel must also be cognizant,

however, of the legal issues that arise when taking advantage of these resources. Technology will continue to develop at a quicker pace than the law regarding its implementation in the workplace. Thus, this is one area where it will definitely pay to implement best practices and stay abreast of all legal developments.