Lost in Cyberspace:

Issues Affecting Employers and Employees in Today's Technological World

Blogs, cyber attacks, and social network background checks are just a few of the merging phenomena in the workplace. As laws addressing these technological advances slowly develop, employers and employees struggle with how to deal with these issues as well as their respective rights and duties.

By Angela McCorkle Buckler

We've probably all checked the latest weather forecast or traffic update on our office computers. Technically, this type of searching is not "related to the company's business" as many e-policies provide. Employers know, however, that prohibiting all personal use of a company's computer equipment not only is impossible to enforce but also would result in an available workforce of about 2 percent of the population. But how much is too much, and what are some of the risks employers and employees face as a result of this use of computers in the workplace? This area of the law is still evolving and will continue to do so as technological developments, such as blogging, find their way into the workplace.

To Blog or Not to Blog

Blogging is one of the latest cyber trends and is especially popular with the 30-something and younger generations. A "Weblog" is a Web site that contains an online personal journal with comments and often hyperlinks. A Weblog differs from a regular Web site because it functions as a bulletin board, allowing comments and postings from anyone who visits the blog, not just from the author. Technorati, an organization that currently monitors and organizes 66.6 million blogs, reports that more than 175,000 new blogs are created every day and that bloggers update their blogs with more than 1.6 million postings per day—or more than 18 postings per second. Naturally, some of these bloggers are employees of a company. Because of the widespread reach of blogs, as opposed to e-mail, for example, employers are rightly concerned about defamatory statements, "blog attacks" from disgruntled or former employees, or disclosure of trade secrets and other confidential information. Similarly, employees want to be able to communicate with other bloggers and express themselves online. Even though there is not yet a large body of case law dealing with the blogging phenomenon, there have been highly publicized instances of employees who were terminated or "dooced" for their blogging activities. For example, a flight attendant employed by Delta Airlines was terminated for posting provocative pictures of herself in her flight attendant uniform and a Microsoft employee was similarly fired for posting pictures of Macintosh computers that his employer had apparently purchased.

As it stands, "at will" employees are subject to discipline for posting inappropriate content to a blog. There are some areas, however, where employees' blogging may be protected. For example, the National Labor Relations Act protects employees who "engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection." 29 U.S.C. § 157. Accordingly, employees blogging with one another about terms and conditions of employment, wages, benefits, and the like may be engaging in protected activity, and employers should be cautious about taking adverse action.

Similarly, employees engaging in "whistle-blogging" activities may be protected by state whistle-blowing laws. In Kentucky, for example, a public employee who reports or "otherwise brings to the attention of" certain authorities information about his or her employer's alleged breach of the law may be protected from adverse action. The Sarbanes-Oxley Act of 2002 provides protection for whistleblowers who work for publicly traded companies. Again, the act requires reporting to certain entities, but employers must use caution when dealing with content containing allegations of wrongdoing on the part of the company. It remains to be seen how blogs will figure into the notice requirements under these statutes.

In an effort to encourage "positive" blogging, some companies have set up company-sponsored blogs for use by employees and others. Sun Microsystems and General Motors, for example, have blogs to which the companies' chief executive officers regularly post messages. Other employers are making sure that their e-policies incorporate and cover issues pertaining to blogging, such as discouraging anonymous blogging; banning the use of company logos or trademarks on blogs; prohibiting the disclosure of confidential and proprietary information; requiring employees to take responsibility for statements they make, to include a disclaimer of company approval, and to comply with company policies and codes of conduct when blogging; and informing employees that their blogs may be monitored and that they should have no expectation of privacy.

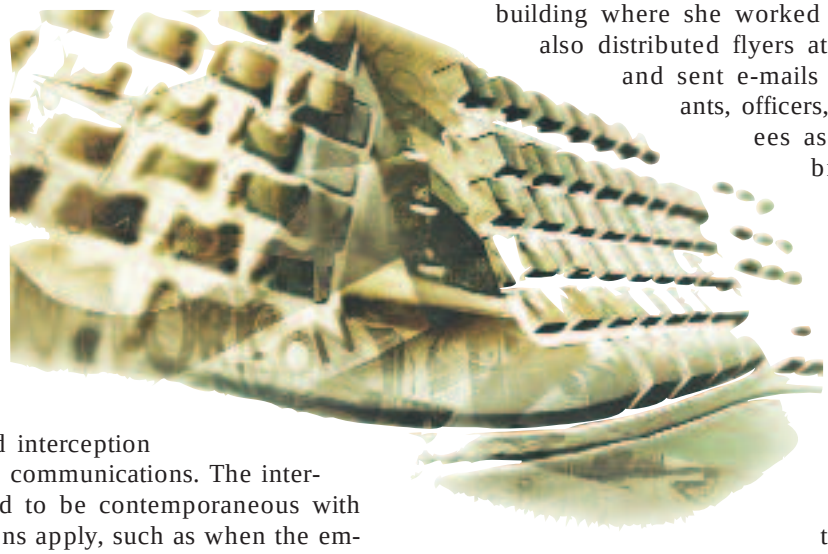
Background Checks on MySpace and Other Social Networks

Another recent cyber-phenomenon is employers' research into applicants' online social networking sites,

such as MySpace and Facebook. Employers are interested in these sites because applicants post pictures, opinions, stories, and other personal information. These "background checks" differ from those that often implicate the Fair Credit Reporting Act because the employer, not a third-party screening company, is doing the online search. Accordingly, when an employer does the Internet search, there is no requirement that prospective employees be told about the search or that the search resulted in disqualifying the candidate. The fact that employers are viewing this information should come as no surprise to job applicants. Generally, when an individual posts information on the Internet for millions to see, he or she is hard-pressed to assert a reasonable expectation of privacy in such information. However, as with any hiring decision, employers may subject themselves to discrimination claims if it is perceived they are gathering or using the information in discriminatory ways.

Privacy Issues

For the most part, employees who use company equipment or the company's Web capabilities will not have a reasonable expectation of privacy in their communications, particularly when employers advise employees that company equipment and systems are subject to monitoring. It is advisable for employers who monitor employees' e-mail or other computer usage to have e-policies because of statutes such as the Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, which prohibits the unauthorized interception of wire, oral, or electronic communications. The interception is usually required to be contemporaneous with transmission, and exceptions apply, such as when the employer has received permission from one of the parties to the communication (that is, signed authorization as part of e-policy), when the employer is the supplier of the system being monitored and the monitoring occurs in the normal course of business, or when the communication is made through a system that makes the communication readily accessible to the general public.



Similarly, the Stored Communications Act prohibits intentional unauthorized access of electronic communications that are stored electronically, including communications in temporary, immediate storage that are incidental to electronic transmission as well as communications stored for backup purposes. However, this act contains several exceptions, including those for service providers, intended users, and individuals authorized to access the information (again, authorization is typically obtained through an employer's e-policies).

Employees' Misuse of Electronic Communications

Employers are not without recourse when an employee or former employee gains unauthorized access to the company's computer system. The Computer Fraud and Abuse Act makes it a crime to access a computer without authorization. Thus, employers may obtain civil and equitable remedies if proprietary information is misappropriated or destroyed. *See International Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (allowing the employer to sue a former employee who deleted data from the company's laptop computer under the Computer Fraud and Abuse Act).

Former employees' activities can be especially troubling for employers. Such problems are illustrated by the case of *Bynog v. SL Green Realty Corp.*, 2005 WL 3497821 (S.D.N.Y. 2005), in which an employee complained to management about alleged threats of physical harm and alleged derogatory remarks involving race and gender. The employer apparently considered the employee (Bynog) to be the source of the problem and ultimately terminated her. Bynog then sought to publicize the situation by creating a Web site that contained a time line of events surrounding her termination, a blog reflecting viewer comments, and testimonials from tenants of the building where she worked as a concierge. Bynog also distributed flyers at SL Green's properties and sent e-mails to the company's tenants, officers, directors, and employees as well as to real estate brokers and analysts. Bynog filed a lawsuit and the defendant moved for a preliminary injunction requiring the plaintiff to cease her cyberattack. The court, however, denied the motion, citing general disfavor of injunctive relief in defamation cases and indicating that the harm did not appear imminent because the activities had been going on for one year and the defendant had produced no evidence of harm the company had suffered as a result.

Employers are also concerned about the ability to determine the identity of anonymous posters to the Internet. Courts have taken varying approaches to this issue, including the following:

- applying a summary judgment standard to the cause of action before allowing a plaintiff to conduct discovery as to the identity of anonymous posters (*see Doe v. Cahill*, 884 A.2d 451 (Del. Super. 2005));
- requiring a plaintiff in a defamation suit to demonstrate that he or she has undertaken efforts to notify the

Lost in Cyberspace continued on page 38

Lost in Cyberspace continued from page 33

anonymous posters that they are the subject of a motion seeking disclosure, to identify statements made by the posters, and to establish a prima facie cause of action for defamation (the court then balances the defendant's First Amendment right to anonymous free speech against the strength of the prima facie case) (*see Dendrite Int'l Inc. v. Doe No. 3*, 775 A.2d 756 (N.J. 2001)); and

- analyzing a defendant's motion for a protective order under existing civil rules, balancing First Amendment rights against a plaintiff's right to the information sought (*see Klehr Harrison Harvey Branzburg & Ellers LLP v. JPA Development Inc.*, 2006 WL 37020 (Pa. Com. Pl. 2006)).

Vicarious liability for employees' misuse of a company's electronic communication poses yet another risk to employers. In *Booker v. GTE.net LLC*, 350 F.3d 515 (6th Cir. 2003), the Sixth Circuit affirmed the district court's dismissal of claims of negligent supervision and vicarious liability for an employee's inappropriate e-mail. Although the court concluded that many of the required elements of the claims had been met, the court dismissed the claim of negligent supervision, because there was no evidence that the employer knew or should have known the employee would send an inappropriate e-mail. The court also dismissed the claim of vicarious liability, because the employee's act was not in furtherance of the company's business. In another recent decision, however, a New Jersey court ruled that an employer may be civilly liable to a victim of child pornography when the employer fails to investigate or stop an employee's use of a workplace computer to view and transmit child pornography. *See Doe v. XYC Corp.*, 2005 WL 3527015 (N.J. App. Div. 2005).

Because employers face risks of such misuse, many companies have increased the level of discipline that corresponds to employees' activities in this area. A survey of employees' use of workplace e-mail, instant messaging, and blogs conducted by the American Management Association and the ePolicy Institute in 2006 indicates that 26 percent of employers have terminated employees for misusing the company's e-mail, 2 percent have dismissed workers for inappropriate instant messaging, and nearly 2 percent have terminated employees for offensive content on blogs.

Conclusion

Electronic communication obviously offers a wealth of benefits for employers as well as for employees. But new risks accompany the benefits offered by today's technology. Both employers and employees have exposure concerning issues of privacy, defamation, and protection of proprietary information, just to name a few. With effective e-policies, employee training, and consistent monitoring and implementation of such policies, many of the pitfalls encountered in cyberspace can be avoided. Those who cannot avoid them, however, have existing and emerging laws that can provide guidance to employers and employees alike. As this area of law continues to evolve, it remains to be seen how the courts will treat issues such as blogging and online social network research. TFL

Angela McCorkle Buckler is a partner at Wyatt, Tarrant & Combs LLP, where she is a member of the firm's employment and commercial litigation practice groups. She is currently vice chair of the Louisville Bar Association's Labor and Employment Section and can be contacted at abuckler@wyattfirm.com. This article was originally published in Louisville Bar Briefs, *the newspaper of the Louisville Bar Association.*

Staying Connected continued from page 36

[40]D.R.I. R. 5072-1(e) (2000).
[41]N.D. Cal. Gen. Ord. 58 (2005).
[42]N.D. Iowa R. 83.5(a)(6) (2006).
[43]D. Neb. R. 1.6(e)(1) (2006).
[44]*Media Guidelines* (N.D. Fla. 2007), available at www.flnd.uscourts.gov/forms/General/mediaGuidelines.pdf.
[45]N.D. Ind. R. 83.3 (2006).
[46]E.D. Tenn. R. 83.1(a) (2006).
[47]General Order *In re: Prohibition of Wireless Communication Devices in Courtroom Facilities* (E.D.N.C. 2005).
[48]D.N.H. R. 83.7(c)(2) (2006).
[49]D. Vt. R. 83.5(b)(2) (2007).
[50]E.D. Okla. R. 83.7(c) (2006).
[51]D.N.M. R. 83.1 (2006).
[52]N.D. Geo. R. 83.4(A) (2006).
[53]Bankr. W.D. Mich. R. 5091(b) (2007).
[54]Gen. Ord. 05-05 (S.D. Ohio 2005).
[55]Bankr. D. Vt. R. 5073-1(b) (2006).
[56]S.D. Ala. L.R. Appendix (2006).
[57]N.D. Iowa R. 83.4(a)(3) (2006).
[58]D. Neb. R. 1.6(f)(1) (2006).
[59]D.N.D. R. 77.3(G) (2000).
[60]Gen. Order 06-15 *In the Matter of Electronic Devices* (N.D. Okla. 2006).
[61]Tim Perrotta, *District May Relax Phone Ban for Lawyers*, N.Y. L.J., Aug. 3, 2006.
[62]E.D. Tenn. R. 83.1(b) (2006).
[63]D.W. Va. R. 83.10 (2006).
[64]Interim Order 2006-11 *In re Cell Phones in U.S. Courthouses* (N.D. Ohio 2006) (affirming that "each Judicial Officer has the authroity to prohibit cell phones, hand-held devices, and/or laptop computers … from their courtrooms and chambers").