Steven Gutierrez

Partner
303.295.8531
Denver
sgutierrez@hollandhart.com

Blogging in the Virtual Age

Blogging in the Virtual Age

Insight — 4/1/2008

What can an employer do to regulate the widespread use of these new technologies and what should you be aware of in your effort to regulate use?

Making Employment Decisions In A Virtual Age

Ellen Simonetti, a Delta Air Lines' flight attendant, maintained a personal blog, "Queen of the Sky: Diary of a Flight Attendant." Ms. Simonetti was allegedly fired by Delta for posting photos of herself in uniform on an airplane and for comments posted on her blog which her employer deemed inappropriate.[1] Ms. Simonetti sued her former employer for wrongful termination, discrimination and defamation. Although the merit, if any, of Ms. Simonetti's claims is still unresolved,[2] the time and fees expended by an employer when defending employment-related litigation can be financially crippling and virtually irrecoverable.

Avoiding such litigation and its associated costs is what motivates employers to create, publish and update employee policies and procedures and to invest in training their employees regarding avoiding discrimination and harassment – and with good reason. One survey reported that "labor and employment" litigation was the category with the most numerous litigation matters pending against companies in the past year.3] Such costs can be difficult for an employer to bear and are sufficient incentive alone to examine whether an employer can or should discipline an employee for the employee's virtual activities.

Computer-Use Policies

Written employee policies notify employees regarding their rights and obligations with regard to their employment. Thus, an employee's expectation of privacy in the employee's office, desk, physical and electronic files and email may be reduced or eliminated by way of employer policies and actual practices.[4]

Clear company policies can also reduce the risk of employee theft, leak of confidential information, and employer liability for employee email and Internet abuse by notifying employees that their e-activities will be monitored. At the same time, it should be noted that if an employer fails to enforce its computer use policy or has knowledge of illegal or wrongful acts and fails to take prompt action, a policy might be used against the employer in the litigation context.

A company's computer and communication systems' policy should be in writing and distributed to all employees. It should warn employees that any violation could be grounds for disciplinary action up to and including

termination of their employment. The policy should also inform that there is no expectation of privacy in the employee's use of the computer, Internet, email or IM communications or functions.

Courts generally consider four factors in determining an employee's expectation of privacy in the employee's computer files and emails:

- Whether the employer maintains a policy banning personal or other objectionable use;
- Whether the employer monitors the use of the employee's computer or e-mail;
- Whether third parties have the right of access to the employee's computer or email; and
- Whether the employer notified the employee, or whether the employee was aware of any use and monitoring policies.[5]

Employers should publish their policies related to computer and communications systems' use in their employee handbooks. Moreover, best practices indicate that employees should be required to read the policy and sign an acknowledgement that they understand and will abide by such policies. Additionally, employers are prudent to incorporate their computer-use policies into employee training sessions, which further prevent employee misuse of the employer's systems.

Security Issues

Although an employer's efforts to enforce its computer-use policy and to monitor employee computer and Internet use can lead to an increased risk of litigation when employment decisions are based thereon, it is in the employer's interest to know about its employees' e-activities for many reasons.

Often employers invest substantial financial resources into developing its products, services, processes, systems and methods. Such confidential information is of the utmost importance to companies and can be financially devastating to an organization if revealed to a competitor or the public at large. Many thefts of confidential information are committed by company employees. Monitoring employees' communications on the internet can guard against theft of confidential information.

On January 28, 2005, Mark Jen was fired from Google after just 11 days of employment for allegedly blogging on his personal website regarding Google products.[6] Eli Lilly & Co., a drug company, recently learned that a slip-of-the-click can be incredibly devastating to a company.[7] Eli Lilly was in confidential settlement talks with the government regarding allegations of marketing improprieties concerning its most profitable drug, Zyprexa, to the tune of $1 billion. So when New York Times reporter Alex Berenson reported about the negotiations in surprising detail, Eli Lilly was understandably disturbed, accusing the government of leaking the information. It was reported however that Eli Lilly's outside lawyer had wanted to send an email to her co-counsel *Bradford* Berenson. Instead *Alex* Berenson popped up from her email contacts and, with just a click of

the mouse, a confidential and comprehensive document regarding the settlement negotiations was sent to the New York Times.

The advent of the Internet democratized the nature of public speech by allowing a relatively inexpensive and extremely wide-reaching medium of communication. Freedom of the press, as one court noted, "is [no longer] limited to those who own one." The Internet now allows anyone with a phone line to "become a town crier with a voice that resonates farther than it could from any soapbox."[8] Meanwhile, a company's reputation in the community – for quality of work, timeliness or efficiency (good will) – can be as valuable an asset as any of its confidential information. Good will adds tremendous value to a company. Therefore, an employer has a substantial interest in knowing what its employees may be saying about the company on the Internet that may impact how its products or services are viewed.

In the case of *HealthSouth v. John Doe*, which later became *HealthSouth v. Krum*, a disgruntled former employee of HealthSouth, a publicly-traded corporation operating rehabilitative healthcare facilities, posted several scathing and ad hominem allegations on a Yahoo! Finance message board.[9] Krum posted under the name "I AM DIRK DIGGLER," a reference to the male porn star in the movie, Boogie Nights. Krum accused HealthSouth's CEO, Richard Scrushy, of inappropriate actions with regard to Medicare reimbursements. He also described, in detail, an alleged affair he was having with Scrushy's wife.[10] Krum's postings fit the model for defamatory statements – that is, a false statement that harms or tends to harm an individual's reputation or standing in the community.[11]

Trade disparagement arises when one, with reckless disregard of the truth, makes a false statement that is harmful to the interests of another, that causes pecuniary loss.[12] In Malaysia, in June 2004, eight Royal Dutch Shell Group companies collectively obtained an Interim Injunction and Restraining Order against a Malaysian geologist and former Shell employee, Dr. John Huong.[13]

Additionally, employees often use employers' online and email services to pay bills, email family and friends, shop for gifts or other personal items, chat with office colleagues, etc. According to a survey by America Online and Salary.com, the average worker admits to wasting 2.09 hours per 8-hour workday – with 44.07% of the people citing web surfing as their top time waster.[14] Employees may be using work hours to write posts on their personal blogs or send personal emails that could contain statements about the company or its products or services.

Monitoring Methods

Aside from the issues discussed above, one of the reasons employers are monitoring their employees is because the technology associated with monitoring is advancing at the same rate as the technology associated with employee communication systems. Most employees are now aware that images, documents, and websites created or access on a company's computer cannot be deleted entirely. Programs are available to allow employers to retrieve documents and emails with surprising

effectiveness. Moreover, footprints and metadata are created when employees access websites, and these footprints can be retraced to determine which websites an employee has visited, when the sites were visited and how often.

Additionally, Global Positioning System (GPS) tracking is becoming an important tool for employers seeking to monitor their employees' activities. GPS is becoming more available in cell phones, vehicles and even security badges. In August 2007 an employee sued his employer after he was terminated – his employer-issued cell phone revealed that he was leaving work early.[15] The New York State administrative law judge upheld the termination on the grounds that the employee was falsifying time cards.

Similarly, employers are now using radio frequency identification devices (RFID) for identifying an employee's location. A RFID tag is an object that can be applied to a product, animal, or person for the purpose of identification using radio waves. RFID tags have practical ranges of hundreds of meters, and a battery life of up to 10 years. In the employment context, RFID tags are being applied to employee badges providing the ability to locate the employee (or at least his or her badge) at all times in a facility.

Locating technology will likely not be the last area of development with regard to employee monitoring. Biometric hand-scanners are now being used for security access as well as time-clock systems. As additional monitoring methods are developed, society will need to address the issue of where the line should be drawn between employee monitoring and employee privacy.

Conclusion

Legislation will likely not catch up with technology any time soon, as technology continues to grow and change at ever-increasing rates. Not long ago the first computer weighed 27 tons and filled an entire room – whereas, today, employees communicate to clients through cordless earpieces and carry computers in their phones weighing three to four grams. For this reason, employers may not have a tremendous amount of guidance today, or in the future, when trying to make employment decisions related to employee use of technology or based in information learned about employees through ever more sophisticated means. Thus, the best practice in this virtual age is to make employment decisions based on a timeless guiding factor: fairness. In other words, employees should know, based on their training and the employer's policies, procedures and past actions, that the employee's conduct is inappropriate and lead to his or her discipline. As always, employers should base decisions solely on business-related criteria, act consistently, and follow their policies.

1 "Delta employee fired for blogging sues airline (http://www.usatoday.com/travel/news/2005-09-08-delta-blog_x.htm)", *USA Today*, 2005-09-08.

2 Ms. Simonetti reported in her blog on February 22, 2007 that her case

had been stayed while Delta Air Lines is in bankruptcy proceedings (http://queenofsky.journalspace.com/?cmd=displaycomments&dcid=923&entryid=923).

3 2007 Litigation Trends Survey – Fullbright and Jaworski.

4 *McLaren v. Microsoft Corp.*, 1999 WL 339015 (Tex. App. May 28, 1999).

5 *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005).

6 http://www.news.com/Google-blogger-I-was-terminated/2100-1038_3-5572936.html. Published February 11, 2005. Retrieved on 2/7/2008.

7 http://www.portfolio.com/news-markets/top-5/2008/02/05/Eli-Lilly-E-Mail-to-New-York-Times.

8 *Reno v. American Civil Liberties Union,* 521 U.S. 844, 896-97 (1997).

9 Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 Duke L.J. 855, 866 - 68 (2000).

10 *Id.*

11 Matthew W. Finkin, Privacy in Employment Law, at 91-92, Ch. 2.III.C.3.a. (2d Ed. 2003).

12 Restatement (Second) of Torts § 623A (1977); W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 128, at 962-64 (5th ed. 1984).

13 http://www.royaldutchshellgroup.com/2006affidavit/shellnewsnetaedaffidavitmay2006.htm; http://en.wikipedia.org/wiki/Blog.

14 Internet Use, Socializing Costs Businesses Billions, 25 NO. 5 Legal Mgmt. 10 (2006).

15 *Department of Education v. Halpin*, OATH index No. 818/07 (August 9, 2007).

---

depending on the jurisdiction or circumstances. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.