Monitoring Electronic Communications in the Workplace

Publication
10.16.01

Within the past few months, virtually every media channel has reported on the use and abuse of electronic communications in the workplace. Among others, mainstream publications such as *The Wall Street Journal* and *Reader's Digest* featured such stories. Television networks such as *Fox News* have done investigative reports, and Atlanta's own Clark Howard has also opined on the subject.

This article sets forth some background facts about the explosion in the use of electronic communications systems in the workplace, briefly summarizes applicable laws, and provides a 10-step action plan for employers to monitor such systems in the workplace.

Background
According to a recent survey conducted by the American Management Association, 67.3% of all employers monitor one or more forms of their employees' electronic communications. Reportedly, 38% of employers monitor employees' telephone use and 27% monitor e-mail messages. These percentages are increasing daily.

The more than 100 million American adults who are on-line send approximately 2.2 billion e-mail messages each day. By comparison, only 293 million first-class letters are mailed each day. The average employee reportedly spends six hours per week surfing the Internet while at work. Employees search for new jobs, review financial markets, purchase goods and services and, at 62% of the companies surveyed, they surf sexually explicit material.

Abuse of electronic communications causes a myriad of problems for employers, including: 1) loss of productivity; 2) claims of harassment or discrimination; 3) breaches of their employers' confidences or trade secrets or those of others for which their employer may be liable; 4) copyright violations or other infringement of intellectual properties; 5) civil and criminal liability for industrial espionage or other new computer crimes; and 6) increased vulnerability to union organizing efforts. Left neglected, these problems pose an immediate and significant threat to employers.

The Law
Contrary to common belief, the U.S. and Georgia Constitutions do not grant employees of private, non-governmental employers any quote "right to privacy." By words and actions, however, an employer may create an employee "expectation of privacy," which can form the basis of privacy

lawsuits. With the increased use and monitoring of electronic communications, invasion of privacy claims have increased 3000% in the past 10 years.

Additionally, several federal and state laws regulate communications and various computer crimes. These statutes, however, actually serve more to protect employers than to limit their rights to regulate the use of electronic communications systems by their employees. For example, the federal law covering "fraud and related activity in connection with computers" prohibits, among other things, fraud, unauthorized access, and computer extortion. Likewise, the Georgia Computer Systems Protection Act prohibits computer theft, computer trespass, computer invasion of privacy, computer forgery, and computer password disclosure. Under both these federal and state statutes, offenders are subject to civil and criminal liability. Thus, Georgia employers have recourse against disgruntled employees who sabotage their electronic communications systems, threaten to destroy important computer files in exchange for severance pay or continued pay, or "snoop" in files where they have no access authority.

10-Point Action Plan

To minimize the problems caused by abuse of electronic communications systems, employers should implement the following 10-point action plan:

1. Audit use of eCommunications: Employers must consider what types of communications are used, such as voicemail, faxes, telephones, pagers, e-mail, personal digital assistants, video surveillance, or Internet and Intranet connections. Next, they must ask questions such as: Who are the users?; What is their culture?; For what business purposes are the systems used?; Is monitoring necessary for quality?; To what extent is security necessary?

2. Develop written policies on electronic communications, software licensing, and no harassment: Among other things, an electronic communications policy should set forth the basic definitions, scope of coverage, acceptable uses of the employer's systems; that the Company has an absolute right of access and employees have no expectation of privacy; that employees either should not use or should limit their use of the systems and that certain uses of the systems are prohibited. Prohibiting gossip, personal or embarrassing information, emotional or knee-jerk communication, non-work related solicitations or other communications is also essential. Additionally, the policy should specifically prohibit the use of material that is discriminatory, harassing, insulting, disruptive, offensive, obscene, or harmful to morale. The policy should also prohibit violation of any intellectual property agreements, laws, or other licenses regulating use of such systems.

3. Train employees and managers about policies: Employers should communicate their policies through stand-alone and handbook statements, Internet or Intranet notices, new employee orientation and employee training. Training for employees should include a review of the policies, the rationale of the policies, the employer's intended procedures for use, access, monitoring, enforcement and inquiries about the policies, and disciplinary and legal consequences of violation. In addition to those matters about which employees are trained, employers should train their

supervisors about the employers' rights, what they should and should not say to employees, when to monitor, intercept or record electronic communications, and proper procedures for investigating alleged policy violations.

4. Avoid words or actions that may tend to create an expectation of employee privacy in employer electronic communications systems: Employers should state that electronic communications on the employers' systems are not personal, confidential or private. They should explain to employees that the employer retains the right of access to the systems at any time, and they should educate employees about the legitimate business reasons for monitoring electronic communications.

5. Monitor electronic communications in the workplace: To ensure compliance with established policies, employers should use a current and effective system for monitoring electronic communications. Programs such as MimeSweeper, Eltron's Internet Manager, Surf Watch, and Websense are appropriate for monitoring electronic communications in the workplace.

6. Uniformly enforce policies relating to electronic communications: Uniform enforcement of policies maintains management credibility, avoids discrimination and harassment claims, protects trade secrets, prevents copyright violation, and minimizes an employer's vulnerability to union solicitations.

7. Protect trade secrets and confidential information, both on-line and in its other systems: Confidential information and trade secrets should be treated with care on-line and off-line to establish that they are in fact secret or confidential. Limiting access or distribution, requiring return of extra or outdated copies, requiring on-site review, or special markings can help protect these things.

8. Be aware of how unions can use electronic communications to the employer's detriment: Unions are adopting progressive, non-traditional methods of organizing employees, such as conference calls, e-mail, and web sites. These methods can be effective in reaching and persuading employees that may not have been otherwise exposed to unions.

9. Establish a crisis management team: Employers should have a crisis management team and a contingency plan for responding to violations of their electronic communications policies or other intrusions into their systems. The team should include a manager, assistant administrator, technical expert, investigation personnel, and perhaps even a media relations specialist.

10. Be aware of the potential litigation risk caused by electronic communications systems: E-mail is written, may not be private, and is frequently retained in computer systems long after deletion by users. These features can cause problems for unwary employers.

Conclusion

Because of the exploding growth in the use of electronic communications in the workplace and the myriad of problems of not regulating such communications, employers should quickly implement the 10-step action plan outlined in this article.

Related People

D. Albert Brannen
Partner
404.240.4235
Email