LEGAL RISKS TO THE EMPLOYER IN THE ELECTRONIC WORKPLACE AND HOW TO AVOID THEM

Donald F. Burke

In 2002 nearly 80% of businesses in the United States electronically monitor their employees. Employers' concerns about workplace security, confidential information breaches, liability for so-called "smoking gun e-mails, and workplace harassment issues, among many others, continue to increase. As workplace surveillance proliferates in response to such employer interests, privacy concerns continue to rapidly escalate. While there are both federal and Maryland laws which address privacy there are few which explicitly address privacy rights in today's complex and sophisticated electronic workplace. In fact, it is clear that technology is developing at a far more rapid pace than either corresponding legislation or case law. One result of this ever widening gap is that employers are exposed to legal risks. While these risks are present, they can be successfully avoided by undertaking preventive measures.

Many employees view the use of their employer's e-mail system, for example, as akin to making a telephone call and therefore feel that messages they send on their company's e-mail system should be free from employer intrusion. Employees view surfing the net in the same manner. A recent study of comScore Networks reports that in 2001, 59 percent of sales online were conducted from work. From April through June of 2002, the most frequent online shopping occurred at work between 11 a.m. and noon. Nielsen/NetRatings, another Internet measuring firm, reported that in August 2002, peak Internet access from work was from 10 a.m. to noon. Seattle-based Internet filtering technology firm N2H2, which conducts the surveys and tracks lost

productivity, estimates that for each hour of unnecessary surfing per day, a company with 1,000 employees loses an average of $11 million a year in productivity.[1]

The prevailing trend of judicial decisions in the area of employee use of employer technology suggests that, absent statutory provision, employees lack rights of privacy when using employers' technology. However, an employer can possibly create an expectation of privacy if it is aware of the use of, for example, its e-mail system for personal communications among its employees and allows the system to be used for that purpose. Under these circumstances, an implied agreement is arguably created granting employees the right to expect that their private communications will not be monitored or accessed. On the other hand, an employer can of course also expressly permit its employees to use its e-mail system for personal communications by informing them in policy statements or personnel manuals that this practice is acceptable. Some companies have recognized that employee use of e-mail or the Internet is inevitable and therefore have either impliedly or expressly granted such rights to employees.

Some companies, notably Silicon Valley based tech firms, permit limited private use of the employer's communication technology. Usually a certain portion of the company's communication system is designated for that purpose. The employer informs its employees that it will not monitor electronic communications unless it believes the system is being used for illegal activities or activities harmful to the company.[2] However, such approaches to the use of company communication technology, while well meaning, nearly always fail. They not only fail but often result in liability to the employer since actions of an employee during working hours

---

[1][Detroit News, Oct. 10, 2002].

[2]Various approaches to limited employee use of employer communication technology are suggested by the Electronic Messaging Association in its pamphlet, "Access to and Use and Disclosure of Electronic Mail on Company Computer Systems: A Tool Kit for Formulating Your Company's Policy."

are, in many cases, attributable to the employer under the legal principle of *respondent* superior. Therefore, if liability is to be avoided the line between business and personal use of the employer's technology must be clearly defined. Acknowledging the present unsettled state of the law, an employer can best protect itself by a adopting an "all or nothing policy" with respect to personal use of employer technology.

While given the rapid advances in technology and the considerably slower pace of statutory development, it is vital that an employer adopt and uniformly implement a well drafted communications technology policy. There have, however, been several interesting cases which have interpreted the federal statutes as allowing employer access to employee generated electronic communication without employee consent. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act"), restricts employer monitoring of computer use and electronic mail. The Act prohibits intentional interception or accessing of any wire, oral, or electronic communication during actual transmission (except with consent or using the business extension exception) and was amended in 1986 by the Electronic Communications Privacy Act ("ECPA") to include specifically e-mail, digitized transmissions, and video teleconferences in the definition of electronic communication. 18 U.S.C. §§ 2510, et seq. However, under the Stored Wire and Electronic Communications and Transactional Records Access Act ("SWECTRAA"), the person or entity that provides the electronic communication service may access the communication while it is in electronic storage and without obtaining consent. 18 U.S.C. § 2701. Thus, employers that provide e-mail and voice mail may access the messages stored in their computer and telephone systems without the explicit consent of their employees. See Fraser v. Nationwide Mutual Insurance, 135 F. Supp. 2d 623 (E. D. Pa. 2001) (the employer did not violate the ECPA or the SWECTRAA when it accessed an employee's e-mail after the e-mail had

been transmitted and stored); Bohach v. City of Reno. 932 F. Supp. 1232 (D.Nev. 1996) (the court determined that the city which provided employees with pagers, terminals, software, and computers that made electronic communications possible lawfully accessed electronic messages sent over the pager system once they were stored in the computer).

Increased globalization and availability of World Wide Web access, coupled with a demand to improve employee productivity, has resulted in increased employer reliance on electronic means of communication and transmission and storage of information often at the cost of what some refer to as electronic privacy. Courts have recognized the difficulty of applying existing legal standards to the rapidly-changing technology. One federal District Court has noted in a decision that:

> [t]he Internet may well be the premier technological innovation of the present age. Judges and legislators faced with adapting existing legal standards to the novel environment of cyberspace struggle with terms and concepts that the average American five-year-old tosses about with breezy familiarity. Not surprisingly, much of Internet-related issues focused on seeking a familiar analogy for the unfamiliar. American Library Assn., et al. v. Patake, 1997 U.S. Dist. LEXIS 8793 (S.D.N.Y.6/20/97)

Such legal analogies are often difficult to draw for both courts and employers. Therefore, employers are forced to anticipate legal challenges to their actions in the context of a highly-mobile legal and technological landscape. Largely because of the difficulty of applying today's legal standards to the rapidly-changing electronic workplace, and the uncertainty of how any court may apply legal theories concerning workplace privacy in the future absent sound employer policy and practice, an employer is best served by adopting and implementing a no-nonsense approach with respect to use of technology in the workplace.

Employers should adopt a multidisciplinary or team approach toward developing technology policies. Input should be sought from (1) all affected departments, (2) human resources, (3) information technology, and (4) legal. Critically review any existing policies to determine if they are adequate, need revision, or should be tossed and replaced. Often this partnering brings unique knowledge and experience to enable the employer to develop policies that are as complete, and innovative as the requirements of the developing technology demand.

Development of workplace training programs for management and non-management personnel is an essential element to the success of any technology use policy. The training of managers concerning the proper use and also misuse of company communication and technology is essential to reducing litigation risk. In many cases managers will be initially confronted by affected employees with questions and issues concerning implementation of company policy in this area and they should be able to give a knowledgeable response. Also, the company will rely on managers to consistently and uniformly enforce its policies. To accomplish this requires understanding of the policies and how best to implement them in a uniform fashion.

Training of non-management employees is also desirable in order to reinforce any written policy in this complicated and often confusing area. A record should be kept of all such employee meetings. It is important during these meetings to not only restate the policy and respond to inquiries but to clarify privacy issues, especially for computer files, electronic mail, Internet access, and voice mail. Employees many times incorrectly assume that these are "private" or will remain inaccessible to the employer. Employees should understand that these items are no different from desks or lockers when it comes to the employer's right to access, search, or monitor them. Employers should also discourage employees from keeping private information stored in their computer files and should inform them that deleting electronic files does not

always erase them. To further lessen the expectation of privacy, employees should be required to report all passwords or codes used with communications systems to the security or information technology departments or other appropriate management personnel and should not be allowed to have "secret" passwords.

New and technologically innovative communications systems are an essential tool for doing business and constitute an integral part of the daily work of many millions of employees. The use of such technology affects virtually every organizational function. Employers should adopt a communication or technology use policy that identifies the proper uses of these systems. Since employer discretion does not come without restriction, it is important for employers to take the proper precautions to minimize the likelihood that their actions and policies can be challenged. An employer should therefore implement the following precautions to lessen the possibility of liability in a privacy or other action by an employee: [1] create a detailed e-mail and Internet policy tailored to your organization; [2] inform employees that all communication equipment is the employer's business property and that the employee has no expectation of privacy with respect to usage of such equipment; [3] communication systems are provided for business purposes and their use is limited to that purpose; [4] incorporate a firewall or filter with the ability to screen or collect data on incoming e-mails, and disclose this fact to employees; [5] create automatic warning messages stating company policy concerning the consequences employees face when accessing prohibited websites or sending or receiving e-mail messages with inappropriate or offensive content; [6] prepare an express provision in the policy maintaining the employer's right to monitor company e-mail and Internet use; [7] verbally discuss company e-mail and Internet policy during employee orientation; [8] regularly remind employees about the

company e-mail and Internet policy via paper and electronic memorandum and retain copies of same; and [9] ensure that enforcement of the policy is consistent and non-discriminatory.