Electronic Privacy Rights: The Workplace

With the rise of technology there arose a fear of surveillance. However, George Orwell's 1984 passed us by without noticeable big brother control, and the national concern over espionage diminished with the demise of the U.S.S.R.

These past threats were concerns over the use of technology by governments that had sufficient resources to use the technology for sinister purposes. The new threat is not technology in the hands of government, it is technology alone. What once required massive manpower now requires merely a personal computer? Technology has made the power to monitor others widely available, whether to governments, private enterprise or individuals. This article discusses some of the laws applicable to the monitoring of employees in the private workplace.

An employee, by the very nature of the employment relationship, must be subject to some level of monitoring by the employer. However, this monitoring has limits. Courts have held that it is a tortuous invasion of privacy for an employer to monitor employee telephone conversions. Similarly, mail carried through the U.S. postal service is granted a high level of protection.

However, much employee communication now takes place over private and public networks via e-mail, or voice mail. These forms of communication are very different from telephone calls and letters. For example, after transmission and receipt, these communications are stored for an indefinite period of time on equipment under the exclusive control of the employer. Additionally, these communications can be examined without the knowledge of the communicators. As is often the case, the law has difficulty keeping pace with the issues raised by fast changingtechnology.

Electronic Communications Privacy Act -

In the federal sphere, only the Electronic Communications Privacy Act of 1986 (ECPA) directly prohibits the interception of e-mail transmissions. The ECPA prohibits the interception by (1) unauthorized individuals or (2) Individuals working for a government entity, acting without a proper warrant. The ECPA is mostly concerned with the unauthorized access by employees or corporate competitors trying to find out valuable information. However, while there is no specific prohibition in the ECPA for an employer to monitor the e-mail of employees, the ECPA does not specifically exempt employers.

The ECPA has several exceptions to the application of the prohibition of interception of electronic communications. The three most relevant to the workplace are (1) where one party consents, (2) where the provider of the

communication service can monitor communications, and (3) where the monitoring is done in the ordinary course of business.

The first exception, consent, can be implied or actual. Several courts have placed a fairly high standard for establishing implied consent. For example one court held that "knowledge of the capability of monitoring alone cannot be considered implied consent." Accordingly, for an employer to ensure the presence of actual consent, it should prepare, with advice of counsel, a carefully worded e-mail Policy Statement that explains the scope of employer monitoring. This Policy Statement should be signed by the employees. One example of how this Policy Statement needs to be carefully written is that if it states that personal communications will be monitored only to determine whether there is business content in the communications, then this would probably not amount to consent to review the full text of personal communications.

Additionally, notice that communications might be monitored may have a significantly different legal affect than a notice stating that communications will be monitored.

The second exemption is that the ECPA exempts from liability the person or entity providing the communication service. Where this service is provided by the employer, the ECPA has been interpreted as permitting the employers broad discretion to read and disclose the contents of e-mail communications, without the employee's consent. However, employers should not rely on this exception, because it might not apply in all cases, such as to incoming (as opposed to internal e-mail) if the e-mail service is provided by a common carrier (e.g., America Online or MCI mail, which are not provided by the employer).

Under the third exception, courts will analyze whether the content of the interception was business or personal and allow the interception of only business-content communications.

State laws -

State tort laws are often viewed as the primary sources of protection for privacy of electronic communications. The most common tort that would apply is the tort of invasion of privacy. This tort occurs where "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."

This tort does not require that personal information be actually acquired, disclosed or used. However, the intrusion must be intentional and highly

offensive to a reasonable person. Additionally, there must be a reasonable expectation of privacy by the employee.

Employees often believe that their communications are private because they have a password which they can select and change independently or because they are communicating through outside common carriers. Cases have often turned upon whether this belief was reasonable given the fact that the employer had the ability all along to access the files, though the employees were not aware of this. In determining the outcome, courts will weigh the reasonableness of the employee's expectation of privacy against the business interest of the employer in monitoring the communication. However, it is important to emphasize that in the final analysis courts have traditionally held that legitimate business interests permit employers to intercept communications.

Additionally, state constitutions might provide some protection. A number of state constitutions provide a specific right of privacy. But, only California has specifically determined that its constitution provides a cause of action against nongovernmental entities. However, even in California, the courts will give significant weight to the business interests of the employer.

Conclusion -

As discussed, much of the law of privacy in the workplace turns on the reasonable expectation of privacy. When evaluating different situations, it is important to keep in mind that the law in this area is a moving target, as recently expressed by Professor David Post of Georgetown University Law Center (in The American Lawyer, October 1995) "until we have all spent more time in this new electronic environment, who can say what our expectations really are --let alone whether they are reasonable?"

In the workplace, federal and state laws provide some protection to employee communications. However, this protection is quite limited. Until the law develops further, employers should prepare carefully drafted Policy Statements that explain how the employer intends to monitor employee communications. And employees, even in the absence of such Policy Statements, would be well advised to consider their communications available and accessible to the employer. Also, where privacy is an issue, employees and employers can create a more productive work environment if they work together to jointly develop a Policy Statement that balances the legitimate interests of both the employer and the employees.

From THE COMPUTER LAW REPORT December 28, 1995 [#15] Copyright 1995.
The Computer Law Report is distributed (usually) weekly for free and is prepared by William S. Galkin, Esq. The Report is designed specifically

for the non-lawyer. To subscribe, send e-mail to galkin@aol.com.
