

Commentary***Employer Monitoring Of Employee Internet Use And E-Mail:
Nightmare Or Necessity?***

By
Peter J. Bezek
Shawn M. Britton
and
Robert A. Curtis

[Editor's Note: Peter J. Bezek is cofounder and managing partner of Foley & Bezek, LLP with offices in Santa Barbara. Shawn M. Britton is of counsel to, and Robert A. Curtis is an associate in the firm. Foley & Bezek, LLP specializes in business and complex litigation including e-commerce and Internet issues, such as intellectual property disputes on the Internet. They can be reached at (805) 962-9495. Copyright 2001 by the authors. Responses to this article are welcome.]

Internet and e-mail use is proliferating throughout the business world. Employer monitoring of employee Internet use and e-mail is also on an upward swing. But before jumping on the monitoring bandwagon, employers should consider the costs and benefits of monitoring so that they can devise monitoring policies that create the maximum benefits and that minimize potential liabilities.

What Problems Are Created Or Exacerbated By Internet Or E-Mail Use?

The world of "cyberspace" is popularly viewed as a new and different realm with unique characteristics requiring us to treat it and our visits to it as if we were visiting a new planet where established rules and customs do not apply. This view has both positive and negative results. On the positive side, it increases awareness of the potential for new problems or the exacerbation of old problems by the use of the new technologies. For example, the ability to communicate instantaneously with large numbers of people is a characteristic of the Internet. As a result, defamatory statements on the Internet are published to a huge, even worldwide audience.

On the other hand, users must recognize the dissimilarities between regular mail and e-mail. For example, an employee assumes that his regular mail is not read by others without his knowledge. As a result, he may assume that the same is true for his e-mail when, in fact, his employer is reading it. While at least one court¹ has determined that an employee has no reasonable expectation of privacy in e-mails sent on a company's e-mail system even though the employer had assured its employees that e-mail would be private, it is certainly likely that other courts will find that employees do have a reasonable expectation of privacy. In California, for example, the right to privacy in the State Constitution applies to actions by private employers.² Thus, the prob-

blems of Internet and e-mail use arise both as a result of the new technology and as a result of expectations about how it will be treated.

Sexual Harassment

Among the most serious problems is the use of the Internet or e-mail as a tool of sexual harassment. Of course, sexual harassment in the workplace is hardly a new problem. But the Internet and e-mail have made it easier for harassment to occur. When people communicate on the Internet or by e-mail, they tend to do so in a more informal manner than they would in a letter and often in a more offensive or aggressive manner than they would in a face-to-face or telephone conversation. One result of this is that communication on the Internet tends to be more aggressive and often more sexually offensive or threatening than other forms of communication.

These general Internet communication styles have carried over into Internet communication in the workplace. The problems created by these styles are exacerbated by the ease of communicating to large numbers of people. When one or two employees begin circulating offensive material, it encourages others to participate. In addition, it increases the number of people who are exposed to the offensive communications. For example, in a recent case,³ a female pilot was subjected to sexually discriminatory and harassing comments on an electronic employee bulletin board. The ease of use of the electronic bulletin board encouraged other male employees to join in the bashing and made the comments available to every employee of Continental Airlines.

The ease of access to pornography on the Internet also exacerbates the problem of sexual harassment at work. An employee is not likely to bring Playboy magazine to work; however, he may be tempted to view the material from his desk computer. Others may be exposed to his computer screen, thus creating a hostile and offensive environment. An employee is not likely to photocopy pornography and circulate it to others' in-boxes. But it is easy for employees to circulate pornography by e-mail. Indeed, surveys of major corporations have shown that a substantial number of the web sites visited by employees are pornographic.⁴ The mere knowledge that their co-workers are routinely visiting such sites may make female employees feel that they were working in a sexually hostile and discriminatory environment, especially if the computer screens are viewable in the general office environment.

Defamation

The increased audience for defamatory statements is another serious problem created by the availability of the Internet or e-mail. Again, the tendency of e-mail or Internet users to use bolder language is part of the problem. The ease with which an off-hand comment can be circulated to a huge audience is dramatically increased. And the ease with which the recipients can forward that comment verbatim around the world only adds to the potential damages. Under the general principles of respondeat superior, an employer can be held liable for the actions of its employees who use the facilities of the employer for improper purposes. If the employee's conduct is foreseeable and the company took no steps to prevent the behavior, a company could be found liable for any malicious and intentional behavior on the part of the employee. *Restatement (Second) of Agency*, §§ 228-237, 244-248.

Intellectual Property Problems

The misuse of material protected by copyright, trademark, or patent could result in employer liability. Liability may be found for the conduct of employees in downloading and distributing such material in the workplace or in posting such material on the Internet using office computers. Text, graphs, and software that appear to be freely available on the Internet are often subject to intellectual property laws that limit copying, distribution, and use. For example, in one case,⁵ a federal district court addressed the issue of whether an operator of a computer bulletin board service where users had downloaded unauthorized copies of photographs copyrighted by Playboy, could be held directly liable for copyright infringement. The court found the defendant directly liable for displaying and distributing the copyrighted photographs, despite the fact that he had not personally posted the unauthorized copies and arguably lacked knowledge that the infringing acts were occurring.

The wrongful dissemination of trade secrets or confidential business information is also made easier by the Internet and e-mail. An employee need not sneak actual files out of the office to distribute them; he only needs to forward them electronically. And he no longer merely has access to the limited files he works on; he now may have access to information throughout the company through the computer system. The risk of wrongful dissemination is not only from intentional acts of employees. Anyone who has ever chosen the wrong addressee from their e-mail address book knows how easy it is to send information to the wrong person accidentally.

Furthermore, to the extent an owner of trade secrets must take reasonable steps to maintain the confidentiality of these secrets, if an employer allows employees to transmit secrets by e-mail, even for proper purposes, there may be a claim that the employer has not taken reasonable steps⁶ due to the relative ease with which people may wrongfully obtain access to e-mail.

Loss Of Productivity

Employee use of the Internet or e-mail can also result in lost productivity. Hours spent "surfing the web" are not generally spent for work purposes. Last year, Xerox Corporation fired 40 workers for spending work time "surfing" pornographic and shopping sites.⁷ The ease of forwarding e-mail has resulted in employees having excessive jokes, stories, and the like circulated to them, thus increasing the amount of time it takes for them to read their e-mail. It is difficult to detect when an employee is using his computer for work or non-work purposes, thus encouraging employees to spend time on non-work activities.

Expanded 'Paper Trail'

A more mundane problem is that e-mail continues to exist in a computer system long after it is deleted by the recipient. Thus, these documents are available for review by employees pursuing claims against their employers, employers investigating employee wrongdoing, and opposing parties in litigation. Since people usually treat their e-mail messages informally and often use language they would not otherwise use, information contained in e-mails can be especially damaging. Discovery of old e-mails in litigation can lead to revelation of very damaging material otherwise unavailable.⁸ A clear destruction policy for e-mails is important to any law firm and its clients.

What Are The Benefits and Drawbacks Of Internet And E-Mail Monitoring For Employers And Employees?

Due to the problems created or exacerbated by the use of the Internet or e-mail, many employers have decided to monitor their employees' use of them. Sometimes this is done with the employees' knowledge, but often it is not. In making the decision whether to monitor, the employer should consider the benefits and costs to both itself and its employees.

There are several benefits to employer monitoring. First, the employer is better able to ensure that its employees are using their work hours for work. If an employee is logged into a travel web site for an hour a day, the employer will know that there is a problem. Second, the risk of the Internet or e-mail being used for harassing or offensive purposes will be lessened; and if such behavior does occur, it can be corrected quickly. Thus, the employer will have a greater opportunity to provide a working environment that is not hostile or offensive or otherwise likely to lead to employee claims of harassment or discrimination. Third, monitoring may prove effective in uncovering employee misconduct, such as the unauthorized dissemination of trade secrets.

As always, where there are benefits, there are costs. While monitoring may provide protection to an employer because it allows the employer to remove inappropriate material, it can also end up creating liability. If an employer undertakes monitoring, he may have a higher duty to ensure that no offensive, harassing, or otherwise inappropriate material remains on the system. As the court noted in *Blakey*, "employers do not have a duty to monitor private communications of their employees; employers do have a duty to take effective measures to stop co-employee harassment when the employer knows or has reason to know that such harassment is part of a pattern of harassment."⁹ When an employer monitors, it is more likely that it will be deemed to have knowledge of harassing material. If no action is taken, this could result in direct liability for the employer. Thus, once an employer commences monitoring, it must do so continuously and purposefully or risk increased liability. The differing results of actions against two Internet service providers highlight this potential problem. In an action against CompuServe,¹⁰ the court found no liability on the part of CompuServe for defamatory material, in part because CompuServe made no claim that it would monitor the material placed on its sites. The court considered CompuServe to be like a news vendor or book store. On the other hand, in another case, Prodigy was found to be liable for defamatory material placed on a website because Prodigy held itself out as a provider that controlled the content of its bulletin boards and because Prodigy used software and bulletin board leaders to enforce its content guidelines. Thus, Prodigy was found to be similar to a newspaper publisher.¹¹

Second, if an employer's policy is to monitor e-mail, there is no basis for employees to have an expectation of privacy. In addition to helping create a higher duty for ensuring that the system is not used for inappropriate purposes, the lack of an expectation of privacy can create problems with employee morale. Studies have shown that employees who are monitored in various ways have increased stress and fatigue, higher absenteeism, and lower morale. Perhaps it is common sense; no one feels good knowing that he is being "watched."

Another potential downside for employers is that in order to create a policy that is less open to challenge, the monitoring policy should include monitoring of all employees,

even at the highest levels. Management must consider whether they want their Internet use and e-mail messages to be reviewed.

Employers must also realize that monitoring requires direct expenses — paying someone to review the material and paying for the software needed to permit monitoring. These costs vary depending on the extent of the monitoring desired. The most basic software is website monitoring software. This type of software logs the Internet addresses of websites viewed by a particular employee and the length of time spent at each website during the course of a day. More complex versions of this software can monitor information entered into the websites by the computer user. Thus, an employer could monitor e-mail messages sent using public services, such as hotmail. Software of this type can range from \$100 to \$5,000 depending on the complexity and depth of the monitoring desired.

Another type of software is e-mail monitoring software. This type of software searches outgoing and incoming e-mails for certain keywords or file types. For example, this software can be programmed to scan outgoing e-mails for curse words or attached pictures and then prevent the e-mail from being sent and simultaneously forward those e-mails to the system administrator for review. Software of this type can range from \$200 to \$1,000.

The most intrusive form of monitoring is keystroke monitoring software. This type of software records and logs every keystroke typed by the user of the computer. Therefore, contents of e-mails and website search requests are recorded and can be easily viewed by the employer. Software of this type can range from \$400 to \$1,000 depending on the complexity and depth of the monitoring desired.

Finally, there is the potential for liability under the Electronic Communications Privacy Act or under common law torts, such as invasion of privacy. Under the ECPA, e-mail can be intercepted or accessed under certain conditions. The term “interception” has been defined narrowly by one federal appellate circuit to mean during the transmission.¹² Under that interpretation, once the message has arrived at the recipient’s address, it is no longer possible to “intercept” it. Thus, under the holding of that case, interception is impossible unless an automatic routing software is used to send duplicates of all messages to the employer.

One exception in the ECPA is that e-mail may be intercepted if there is consent by one party.¹³ Consent may be obtained explicitly by having the employee sign a written consent. It may also be implied by advising employees that their e-mail will be monitored. If an employee thereafter uses the system, he is giving implied consent to the monitoring. Consent is not implied easily, however; a mere statement to employees that monitoring is possible or may occur is not enough to show implied consent. Actual notice that monitoring does occur is required. For example, in a case¹⁴ involving monitoring of an employee’s telephone calls, the employer argued that the employee had impliedly consented because she 1) had been advised that her employer might monitor and 2) knew that monitoring was possible because of the existence of an extension phone at her employer’s home. This was not sufficient to support a finding of implied consent.

A second exception allows interception if it occurs in the normal course of employment activities that are a necessary incident to the rendition of services to the provider of the

e-mail service or to the protection of the rights or property of the provider.¹⁵ The exception for business use of the provider is a risky provision on which to rely. Even if the employer is providing the Internet or e-mail service, it is difficult to know how broadly the courts will interpret activities necessary for the services to the provider or protection of the rights or property of the provider. Arguably, this exception includes the right of an employer to ensure its property is used for only business purposes. But this is far from settled.

There is no prohibition for accessing stored e-mail unless the electronic communication service is provided to the public.¹⁶ Thus, if an employer is providing the e-mail to its company and not to the public, it may access all of the e-mail stored in the system for any purpose. For example, in *Anderson Consulting LLP v. UDP, et al.* (ND Ill. 1998) 991 F. Supp. 1041, 1043, the court found that a company providing its own Internet e-mail system is not providing service to the public.

If an employer monitors its employee's e-mail but does not fall under an exception to the ECPA, it faces liability under that statute. In addition, there is the possibility of liability under the tort of invasion of privacy. Finally, employers should keep abreast of new developments that may change the law in this area. For example, a bill has been introduced in the Senate that would amend the ECPA to require employers to notify their employees if their e-mail is being monitored, if their computer keystrokes are being monitored, or if their telephone calls are being listened to.¹⁷

These various costs and benefits to an employer must be considered along with the costs and benefits to employees. The benefit to employees, as discussed above, is that there is a greater likelihood that the Internet and e-mail will not be used to harass or offend. However, the obvious drawbacks are the lack of privacy and the corresponding mental stress and lower morale.

If An Employer Decides To Monitor, How Can The Potential For Liability Be Reduced?

After conducting a cost/benefit analysis, many employers may determine that it is their interest to monitor employee Internet use and e-mail. In this case, there are steps that can be taken to reduce the risk of liability for monitoring. If the employer intends to monitor generally, the most important step is to advise employees that this monitoring is taking place. Surprisingly, studies have shown that the majority of employers who monitor do not apprise their employees of it. Not advising employees of monitoring destroys many of the benefits of monitoring. If employees are unaware of monitoring, they are not as motivated to ensure that they do not use the system improperly. In addition, the employer does not obtain the benefit of being seen as concerned about providing a work environment free of harassment. Furthermore, failing to advise employees makes it impossible to show that employees consented to the monitoring. The employer who monitors surreptitiously leaves himself open to charges of invasion of privacy or violation of the ECPA.

If an employer decides to monitor a particular employee suspected of wrongdoing in the hopes of finding evidence against the employee, advising the employee beforehand defeats the purpose. In this situation, however, if the employer nonetheless chooses to run the risks of monitoring, the employer should be careful to conduct the monitoring

in a way designed to achieve the limited purpose of the investigation in order to minimize the invasion of the employee's privacy, thus reducing potential exposure to charges of invasion of privacy.

An employer who chooses to implement a monitoring policy should clearly state the policy in the employee handbook and should circulate the policy to employees periodically. The policy should state that the employer will monitor, not just that it may monitor. As discussed, there is no implied consent otherwise. To minimize liability, the policy should not limit the monitoring or state that it is only for specific purposes. When a policy is limited, for example, to ensuring that the system is used for business purposes only, there will be room for disagreement in the future as to whether monitoring exceeded the policy. On the other hand, a policy of unlimited monitoring is more damaging to employee morale. The employer must decide if the benefits outweigh the costs.

The policy should state that by using the company e-mail, the employee relinquishes any expectation of a right to privacy. Further, the policy should remind employees that the system is company property. The policy may also require that any Internet or e-mail use be limited to business purposes. The employer must determine if it really wants to enforce such a policy keeping in mind that it should be enforced at all levels.

If possible, the employer should have all employees execute documents giving consent to the employer monitoring. Again, however, the scope of the consent is important. Furthermore, even if the employer has express or implied consent to unlimited monitoring, disputes will be minimized if the monitoring is limited to business purposes.

Employees should be educated that the presence of a password does not mean the employer cannot access the material. Similarly, employees should be advised that deletion from their computer does not delete messages from the system.

In order to reduce the problems created by long-term storage of potentially damaging e-mail, employers should create a policy requiring regular deletion of all messages from the company system.

Employees should be educated about the possible intellectual property liabilities associated with downloading material from the Internet. There should be a written policy establishing guidelines for the material employees will be permitted to download or publish on the Internet.

The world of cyberspace is upon us. The benefits brought about by this revolution are immense. But new challenges are also created. Thoughtful employers will be able to harness the powers of these new technologies while minimizing the possible abuses and harms they create. Without a thoughtful strategy, employers are at risk for employee abuses, employee dissatisfaction, statutory violations, and tort liability. The cost of implementing a thoughtful strategy is well worth it.

ENDNOTES

1. Smyth v. The Pillsbury Co. (ED Pa 1996) 914 F.Supp 97.

2. Luck v. Southern Pacific Transportation Company (1990) 218 Cal.App. 3d 1.
3. Blakey v. Continental Airlines (2000) 164 NJ 38.
4. See, for example, "Over 24 Percent of Employee Time is Non-Work Related," *Business Week*, Aug. 11, 1998; Seminerio, Maria, "Penthouse Web Site Popular with PC Companies," *PC WEEK ONLINE*, Apr. 2, 1996; Trip, Gabriel, "New Issue at Work: On-line Sex Sites," *New York Times*, June 27, 1996 at C1; and *Associated Press*, "The X-rated Files — Cyberporn Forays Targeted," *St. Louis Post Dispatch*, Feb. 7, 1996 at 1C.
5. Playboy Enter. v. Frena (M.D. Fla. 1993) 839 F. Supp. 1552.
6. For example, California Civil Code Section 3426.1 defines trade secrets in part as information that "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."
7. Notice of Electronic Monitoring Act, H.R. 4908 IH, 106th Congress, 2d Session.
8. See, for example, Siemens Solar Indust. v. Atlantic Richfield Co. (SDNY 1994) 1994 U.S. Dist LEXIS 3026.
9. Blakey, *supra*, at 42.
10. Cubby, Inc. v. Compuserve, Inc. (SD NY 1991) 776 F. Supp 135).
11. Stratton Oakmont, Inc. v. Prodigy Services Co. (1995) 1995 NY Misc. LEXIS 229. A federal statute now prohibits liability for a provider of an interactive computer service for content provided by another. 47 USC §230. But the analysis of the earlier cases remains valid.
12. Steve Jackson Games, Inc. v. United States Secret Service (5th Cir. 1994) 36 F. 3d 457.
13. 18 U.S.C. §2511 (2)(d).
14. Deal v. Spears (8th Cir 1992) 980 F. 2d 1153.
15. 18 U.S.C. §2511(2)(a)(i).
16. 18 U.S.C. §2702.
17. Notice of Electronic Monitoring Act, H.R. 4908 IH, 106th Congress, 2d Session. ■