How to Protect Your Agency and Your Employees

Misuse of Technology Courts Disaster

by Kathryn M. Vanden Berk

If you are like most child welfare organizations, you have over the past few years created a large inventory of communications devices that you require your employees to use for work. These tools are so vital to efficient operations that we cannot get along without them. Unfortunately, improper personal use of these tools can lead to trouble (see box). An employer's exposure for any of these uses is significant. They may jeopardize your reputation in the community, threaten your financial viability, and illegally disclose sensitive or confidential information. To try to prevent this from happening, you need to develop tough but fair approaches that will maintain your control over use of these devices while ensuring that they remain available to further your organization's mission.

Fortunately, your rights as an employer are recognized in a number of federal and state laws that generally support the belief that an employer must maintain control over communication systems. The cases arising out of them will typically favor the employer—at least where the employer's policies have been clearly stated and appropriately implemented. (See sidebar for case examples.)

COMMUNICATIONS DEVICES

Improper use and problems…

- The Internet lures employees into time-wasting games, electronic retailing, news, contests, and unfortunately, gambling and pornography.
- Internet downloads carry viruses that can cripple your entire system.
- Cell phones are addictive to traveling staff, leading to excessive phone bills, unmonitored personal calls, and accidents due to negligent driving.
- Electronic mail at the workplace can disclose sensitive information to improper receivers, become a location for illicit relationships, and transmit harassing messages from one employee to another.

Federal and state laws

Three federal laws address e-mail monitoring. The Wiretap Act[1] prohibits the intentional interception or accessing of any wire, oral, or electronic communication. This law was amended in 1986 by the Electronic Communications Privacy Act[2] to specifically include e-mail. The amended version allows employers to monitor and access e-mail, so long as employees have been notified of the monitoring or if the communication occurs in the "ordinary course of business."

In addition, under the Stored Wire and Electronic Communications and Transactional Records Access Act[3], employers that provide electronic communication services may access any messages stored in their computer systems without notifying employees of the access.

At the state level, regulation of workplace electronic monitoring is limited, but there are signs of increased legislative activity.[4] Most state laws exempt employers who open or read e-mail that originates, or is received, on an employer-owned computer. A few require employers to give employees notice of all forms of electronic monitoring.

Suggested actions

I suggest that you evaluate your communication system as a whole, but most certainly place

the greatest emphasis on Internet and e-mail use. This emphasis should reinforce the organization's prohibitions against downloading inappropriate, copyrighted, or virus-infected materials and its restrictions against disclosing confidential and proprietary information. In addition, you should limit your employees' expectation to privacy in the use and receipt of e-mail. Specifically, the policy should:

1. Notify your employees that your communication system is the organization's property and is for business use only. Reserve your right to access, review, and monitor e-mail, Internet and phone use, including any data that is stored or transmitted. Establish and publicize the rule that "there are virtually no online activities that can be conducted at the workplace with absolute privacy."
2. Notify employees that your e-mail and voice mail systems retain messages in memory even after they have been deleted by the user. Although it appears they are erased, the messages are often permanently backed up on magnetic tape, along with other important data from the computer system.
3. Prohibit the use of your systems to transmit discriminatory or harassing messages as part of your "standards of conduct" and harassment policies. If you receive a complaint regarding potentially harassing e-mail, investigate and discipline the offender in the same way you would a verbal incident. Include the proper disciplinary action in the policy for improper communications, up to and including termination.
4. Prohibit the e-mail distribution of copyrighted materials without the author's or publisher's permission.
5. Prohibit the e-mail distribution of confidential information without appropriate safeguards as to who can receive it.
6. Remind your employees that e-mail is business communication. It should not be casually drafted, nor should it contain typing errors, jokes, inappropriate comments, or personal opinions. Remind them that e-mail will most likely be discoverable in a lawsuit. Also, because e-mail is sometimes so quickly responded to, instruct employees to double-check all addresses and be sure they are not sending the message to someone who should not be receiving it.
7. Develop spam filters and delete "junk" e-mail on a regular basis. Develop rules to save, file, retain and/or purge e-mail messages in the system in the same way you save, file, retain and/or purge printed correspondence.
8. Develop virus filters for all e-mail and Internet portals, and instruct employees on how to protect the integrity of your computer system.

Due to the variations in state laws regarding privacy, I *strongly* recommend that you have all employees sign a consent form permitting you to monitor their use of all communications devices (in particular, e-mail).

E-mail systems, cell phones, and the Internet are only three devices among many that are a part of your employer-provided communications system. While they are the largest part, don't forget the other components. These include postal mail, fax machines, telephone and voice mail systems, personal computers and computer networks, online services and Internet connections, computer files, video

E-MAIL PRIVACY COURT CASES

A woman was conducting a training session demonstrating the use of e-mail at a car dealership. She randomly selected a message sent by an employee of the Nissan company to an employee of the dealership. Unfortunately, the message was personal and sexual—obviously not at all business-related. After being terminated for poor performance, the Nissan employee sued for invasion of privacy. In an unpublished decision, a California court of appeals ruled that the Nissan employee had no reasonable expectation of privacy because she had signed a statement restricting her e-mail to company business and, even without the signed statement, she knew prior to sending the sexual message that her employer routinely monitored messages. In other words, under these circumstances, she had no reasonable expectation of privacy. *Bourke v. Nissan Motor Corp*, No. B068705 (Cal. Ct. App., July 26, 1993).

In an unpublished decision, a Texas court ruled that searching e-mail stored in an employee's private computer folder is not the same as searching an employee locker, for which courts have held an employee does have a reasonable expectation of privacy. The difference is that the material in an employee's locker is personal and the employer knows that. E-mail folders stored on an employer's computer—even if protected by an employee password—are not personal property but "merely an inherent part of the office environment." *McLaren v. Microsoft*, 1999 Tex. App. LEXIS 4103.

A Pennsylvania company assured its employees that e-mail would not be intercepted or used against employees as grounds for termination or reprimand. Despite this assurance, the company later reviewed e-mails from an employee to a supervisor and used it as the basis for termination. That was perfectly legal, according to a federal court in Pennsylvania. The court ruled that regardless of the company's statements, it was not reasonable for an employee to expect privacy in e-mail sent to a supervisor over a company e-mail system. According to the court, the company's interest in preventing inappropriate comments or illegal activity over its e-mail system outweighed any privacy interest the employee may have. *Smyth v. Pillsbury*, 914 F. Supp. 97 (E. D. Pa. 1996.).

equipment and tapes, tape recorders and recordings, and even bulletin boards and other public posting sites.

Conclusion

The proliferation of electronic communication devices has exploded, and the laws governing your rights as an employer are still being tested. However, early cases provide encouragement that appropriate policies and procedures will be upheld despite the competing demands of employees to obtain some privacy in their workplace. Your attention to the development of clear policies and to their dissemination to all employees will help ensure a productive work environment.▲

Endnotes

1. Federal Wire and Electronic Communications Interception Act, 18 U.S.C. §§ 2510 et seq.
2. 18 USC § 2511(2)(g)(I)).
3. 18 USC §§ 2701-2711.
4. Several states have statutes protecting against the interception of electronic communications. In 1998, Connecticut enacted legislation requiring employers to give prior written notice of electronic monitoring to all employees who may be affected. Pub. Law 98-142. See also, New Jersey Wiretapping and Electronic Surveillance Control Act, N.J.S.A. 2A:156A-1 et seq.; Pennsylvania Wiretapping and Electronic Surveillance Act, 18 Pa. Cons. Stat. Ann. § 5702 et seq. See also Cal. Penal Code § 629; Colo. Rev. Stat. Ann. § 16-15-102; Md. Code Ann. §§10-4A-01-08; and N.Y. Crim. Proc. Art. 700. These statutes are largely patterned after the federal Electronic Communications Privacy Act.

Kathryn Vanden Berk practiced law for 9 years before serving as the president of two residential treatment centers for children. Now with Chicago-based Mosher & Associates, her law practice focuses on nonprofit start-ups, corporate and tax law, and employment issues. She serves as adjunct faculty at the University of Chicago School of Social Service Administration and is a trainer in financial and risk management for the Council on Accreditation for Children and Family Services, 1st and 2nd Annual Best Practices Conference. She also is the author of "Chapter 5—Employment Issues," in the Illinois attorney's handbook entitled Not-for-Profit Corporations, 2001 Ed., published by the Illinois Institute of Continuing Legal Education. She can be reached at info@beavandenberk.com.

SAMPLE POLICY
Use of Communications Equipment

Communications equipment and services provided by this Agency include mail, electronic mail ("e-mail"), facsimiles, telephone systems, computers, computer networks, online services, Internet connections, computer files, video equipment and tapes, tape recorders and recordings, cellular phones, and bulletin boards. If you use any communications systems, you will be asked to sign this consent form authorizing us to monitor and control your use of it.

All communications services and equipment, including the messages transmitted or stored by them, are the sole property of the Agency. All outgoing messages, whether by mail, facsimile, e-mail, Internet transmission, or any other means, must be accurate, appropriate, and Agency-related. You may not use the Agency's address for receiving personal mail or use Agency stationery or postage for personal letters.

You may not send personal correspondence from the Agency in any fashion that would appear to be an official communication of the Agency, since you may be perceived by the recipient as a representative of the Agency and, therefore, what you write may damage or create liability for the Agency.

Most services and equipment have toll charges or other usage-related expenses. Please be aware of these charges and consider cost and efficiency needs when using any device that we have provided for Agency business. Please consult with _____ if there is a question about communication use.

Online services and the Internet may be accessed only by persons specifically authorized by the Agency. Authorized persons must disclose all passwords to the Agency but should not share their passwords with any other individuals.

Your online use should be limited to Agency-related activities. Generally, you should not use Agency communications services and equipment for personal purposes except in emergencies or when extenuating circumstances warrant it. When personal use is unavoidable, you must log any user charges and reimburse the Agency for them.

You may not use e-mail, facsimiles, or any other insecure communication system to communicate confidential Agency information.

You may not duplicate or download from the Internet or from an e-mail any software or materials that are copyrighted, patented, trademarked, or otherwise identified as intellectual property without express permission from the owner of the material. When appropriate Internet material or e-mail files are downloaded, they should be scanned using the Agency's antivirus software.

Finally, improper use of Agency communications services and equipment will result in loss of privileges and whatever relief the Agency decides, in its sole discretion, is warranted under the circumstances. Improper use includes any misuse as described in this policy as well as any harassing, offensive, demeaning, insulting, defaming, intimidating, or sexually suggestive written, recorded, or electronically transmitted messages.

ACKNOWLEDGMENT: I, _____, have read the above requirements and agree to abide by the above policies. I understand that any violation of these policies pledge will result in loss of privileges and whatever relief the Agency decides, in its sole discretion, is warranted under the circumstances.

Date: _____ Signed: _____