

# ELECTRONIC MONITORING IN THE WORKPLACE— FOR WHOSE EYES ONLY?

*L. Allison McKeel*

---

- An employer hears that an employee plans to leave to work for a competitor and the employer suspects that the employee is copying computer files containing customer lists and other trade secrets
- An employee complains that a co-worker is sending her unwelcome offensive and sexually explicit e-mails and has refused her requests to stop
- An employer discovers that an employee has used company computers to engage in illegal internet gambling and may be using his company supplied e-mail account for communication in connection with such activities

Employers face a variety of situations giving rise to potential harm from their employees' computer use. When computer misuse occurs, business necessity, employment, and other laws require the employer to promptly investigate and take effective remedial action. What are the employer's rights to monitor and investigate computer use against their employees' privacy rights.

A 2005 survey conducted by the American Management Association and the ePolicy Institute reports that 76% of employers surveyed monitor their employees' Web site connections and 55% store and review employees' e-mail messages.[1] Basic knowledge of applicable laws and an effective electronic monitoring policy can provide a substantial advantage to employers in legally monitoring their employees' computer use.

## APPLICABLE LAWS

Both federal and state laws apply to the workplace monitoring of computer use. The Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-3126) (2005) ("ECPA") provides protection for electronic communications, but contains important exceptions. The ECPA prohibits any person from intentionally intercepting, using, or disclosing any oral or electronic communication. 18 U.S.C. § 2511(1). An "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that effects interstate or foreign commerce." 18 U.S.C. § 2510(12). The legislative history of the Act states that the term "electronic communications" includes e-mail transmissions.[2]

The ECPA provides two exemptions which affect employers' right to monitor electronic communications under the Act. The first is the "prior consent" exemption, which permits interception of electronic communications where one of the parties to the communication has given "prior consent" to the interception. 18 U.S.C. § 2511(2)(d). (The exemption does not apply, however, if the communication is intercepted for the purpose of committing a criminal or tortious act.) *Id.* Access to stored electronic communications is also permitted where authorization has been given "by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(2). Under the prior consent exemption, an employer can avoid questions regarding the propriety of a search under the ECPA when the need arises by simply obtaining consent from the employee prior to the search, preferably at the outset of employment (see below).

The second exemption, the "system provider" exemption, applies to employers that provide their own internal e-mail service. 18 U.S.C. § 2702(a) provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." *Id.* By implication, employers that provide internal electronic communication services, not for use by the general public, are allowed access to such stored communications without liability. See *Andersen Consulting LLP v. UOP*, 991 F.Supp. 1041, 1043-44 (N.D. Ill. 1998).

Given the limitations under the ECPA, plaintiffs have turned to state law to establish claims for the interception of electronic communications by employers. Illinois and other states have enacted wiretapping statutes that prohibit the interception of electronic communications without prior consent. The Illinois statute, 720 ILCS 5/14-1 (2006), defines "electronic communication" in a similar manner as the federal Electronic Communications Privacy Act

and similarly provides that there is no liability for interception where one of the parties to the communication has given prior consent. *Id.*

Additionally, the courts have recognized common law claims for invasion of privacy, particularly under the theory of “intrusion upon seclusion,” for an employer’s investigation into an employee’s activities or information. Although there do not appear to be any Missouri or Illinois cases construing the right to privacy in the context of employee e-mails, courts construing Missouri and Illinois law have recognized such claims in other contexts. See *Fletcher v. Price Chopper Foods of Trumman, Inc.*, 220 F.3d 871 (8th Cir. 2000) (disclosure of employee’s health information); *O’Donnell v. CBS, Inc.*, 782 F.2d 1414 (7th Cir. 1986) (removal of personal papers from employee’s desk). In these cases, however, the courts refused to find liability on the part of the employers on grounds that the employee has failed to establish a legitimate expectation of privacy by his or her express or implied consent to the search.

Public employees have further constitutional rights protecting their privacy interests against unreasonable searches, including their electronic communications. Under constitutional principles, an employer may conduct a work-related search of an employee’s property if the purpose and the scope of the search are reasonable. *Biby v. Bd. of Regents, Univ. of Neb.*, 419 F.3d 845 (8th Cir. 2005), citing *O’Connor v. Ortega*, 480 U.S. 709 (1987). The employee must first establish a legitimate expectation of privacy, however. *Biby*, supra, 419 F.3d at 850. To determine whether the employee has a legitimate expectation of privacy, the courts will consider the employer’s workplace privacy policy and any consent to the search by the employee. *Id.* (affirming summary judgment for employer where privacy policy alerted employees that computer files could be searched under specified circumstances.)

## MONITORING POLICIES

An effective electronic monitoring policy is essential for both private and public employers. The key to effective electronic monitoring policies is to establish clear and direct expectations and to assure that employees review the policy and acknowledge their consent. As set forth above, an employees’ prior consent will avoid liability in the majority of cases. While such policies must be tailored to each employer’s particular circumstances, some common provisions should be considered in every policy:

- Clearly state what, if any, personal use is permitted on company computers, including whether such use is permitted during working hours. (All personal use may be prohibited, except where such prohibition would violate some other protected right such as permitted union communications. See, e.g. *Associated Press*, 2002 WL 31357927 (2002)).
- If the policy applies to other devices such as PDA’s or cell phones, specify that explicitly.
- Clearly indicate that employees should have no expectation of privacy with regard to e-mail messages or internet usage, including Websites visited.
- Specify that there should be no communications of sexually explicit, ethnic slurs, racial epithets or anything that could be offensive or construed as harassment or discrimination.
- Include that employees are not permitted to access other computers without specific prior authorization.
- Address whether employees are permitted to download and/or install files or software from the internet onto company computers. If so, the policy should specify whether prior approval is necessary.
- Set out clearly the disciplinary sanctions for violations of the policy

The monitoring policy should be included in the employee handbook, if there is one. Additionally, at hiring, each employee should be given a copy of the policy and required to sign an acknowledgement that they have read and understand the policy and that they consent to it. Such consent should be renewed in writing at least annually.

*Allison McKeel is Senior Counsel with the law firm Bobroff, Hesse, Lindmark & Martone, PC in St. Louis, concentrating in Employment Law and Commercial Litigation. For more information contact: [allisonmckeel@bobroffhesse.com](mailto:allisonmckeel@bobroffhesse.com) or (314) 862-4681.*

[1] A summary of the Survey can be found at: [www.amanet.org/research/pdfs/EMS\\_summary05.pdf](http://www.amanet.org/research/pdfs/EMS_summary05.pdf).

[2] S. Rep. No. 99-541, at 14 (1986).