Privacy vs. Security

Legalities of Monitoring Workplace Communications

By George Raymond

With an ever increasing proliferation of the use of electronic communications – e-mail, web sites, chat rooms and instant messaging – in addition to faxes, cell phones and Alexander Graham Bell's traditional land-line phone, employers and employees are faced with new legal and ethical issues of privacy. Employers are faced with balancing the privacy expectations and rights of employees with concerns of maintaining the security of confidential and proprietary information and the potential liability for the dissemination of improper materials.

The Electronic Communications Privacy Act (ECPA) prohibiting the intentional interception and disclosure of electronic communications applies to both computer and telephonic communications, including facsimiles and cell phones. Basically, the ECPA prohibits anyone other than the sender and intended recipient of a message from intercepting it in transit, accessing it after at has been stored or disclosing its contents. However, and this is a big however, an employer may be permitted to intercept or access an employee's electronic communication if (i) the employee has consented to such action or (ii) such interception is covered by the "business-use exception" contained in the ECPA.

What the law says

18 U.S.C. § 2511 (2) (d) reads as follows: "(d) It shall not be unlawful under this chapter for a person not acting under the color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortuous act in violation of the Constitution or law of the United States or of a state."

18 U.S.C. § 2510 (5) (a) reads as follows: "(5) 'electronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than –

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by the provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;…"

Obtaining consent

Consent to employer monitoring doesn't have to be express, but under certain circumstances may be inferred from the employees' awareness of a monitoring policy or practice. However, to be on the safe side, an employer should have a written policy that is disseminated to each employee and receive a written consent or acknowledgment of the policy from each employee.

George Raymond

Even if employee consent has not been obtained, an employer may be permitted to intercept messages sent using an electronic communication service provided by the employer. If the monitoring is conducted within the course of the employer's business and the intercepted communication deals with matters in which the employer has a legitimate interest, then the employer need not provide employees with prior notice or obtain their consent. However, if the intercepted communications are obviously of a personal nature, the employer must stop monitoring as soon as that becomes apparent.

Many employees, whether they have a right to privacy in the employment setting or not, find an employer's monitoring offensive. Although in most cases this is not a legal problem for the employer, it is a practical/morale issue. However, an employer cannot allow employees to communicate on the employer's system unmonitored. There are too many cases in which the employer can be held accountable for what is communicated on its system to not have a monitoring policy. The policy, however, should authorize monitoring in a wise, consistent and least intrusive manner as possible.

The next issue of *BizVoice* will include a look at some sample monitoring policies.

Helpline Offers Assistance

The information in this article is provided by the author and publisher as a service to the business community. Although every effort is made to ensure the accuracy and completeness of the information, the author and publisher cannot be responsible for any errors or omissions.

However, if you are a member of the Indiana Chamber of Commerce, you may contact the Chamber's HRhelpline (317-264-6866) to discuss privacy, monitoring or other human resource issues.

INFORMATION LINK

Authors: George Raymond is vice president of human resources, labor relations and civil justice for the Indiana Chamber of Commerce. He can be contacted at (317) 264-6884 or e-mail: graymond@indianachamber.com