



Executive Recruiting  
Outplacement  
Human Resource Consulting  
Professional Assessments  
Training and Development

## Employee Privacy and Electronic Monitoring

There is no question that there are many good business reasons to monitor employee communications, including measuring productivity, maintaining confidentiality, and limiting employer liability for employee misconduct. For example, you may want to measure employee output (such as keystroke counts) or assess the quality of customer contacts (particularly by telephone and e-mail). You also may monitor to ensure your communications systems are used according to policy and are not compromised by viruses or inappropriate personal use.

Still, monitoring can be controversial because employees often view it as invasive, distracting, and stressful. And, if done improperly, you may violate federal and state laws that limit your ability to monitor employee telephone and computer communications. Below is a discussion of the legal issues and a practical guide on how to reduce both legal and employee problems when implementing monitoring policies.

### Laws Governing Electronic Monitoring

Interestingly, even though employees may feel that telephone and computer monitoring violates their privacy, the law does not entirely support these concerns. Under federal law, employers have the right to monitor work-related use of telephone, e-mail, and other computer-generated communications, if certain conditions have been met. Title III of the Omnibus Crime Control and Safe Streets Act (commonly referred to as the Wiretap Act), found at 18 U.S.C. §§2510 et seq., generally prohibits the intentional interception of any wire, oral, or electronic communication. (Note that the Wiretap Act initially covered telephone conversations, but was amended by the Electronic Communications Privacy Act (ECPA) to include all electronic and computer communications, including e-mail.)

However, the Wiretap Act contains two exceptions to its interception prohibition: (1) when at least one party to the communication performs the interception, or has previously consented to the interception; or (2) when the interception is by an employer with a legitimate business-related reason for the interception (the "business extension" exception).

**1. Consent.** To qualify, consent may be express, as in a written agreement, or implied from the circumstances, as when an employee is informed that all calls and e-mail will be monitored for quality assurance or training purposes. However, it is not sufficient notice when an employer informs employees that it might start monitoring calls.

**2. The business extension exception.** Under the "business extension" exception, an employer, within certain limitations, may monitor an employee's telephone calls and e-mail without the employee's consent. The exception allows an employer, in the ordinary course of business, to intercept communications if it uses equipment or a component that it furnishes or that is furnished to it by a provider of wire or electronic communications service in the ordinary course of the provider's business (usually, the telephone company). So, under the Wiretap Act, you may monitor and even record an employee's telephone calls without consent as long as you can show a normal business-related reason for doing so and use equipment allowed by the Act.

Generally, the business extension exception also does not apply if the employer listens to a personal conversation beyond the point necessary to determine that it is personal.

Most states also have statutes prohibiting electronic eavesdropping, many of which are modeled closely on the federal Wiretap statute. A few states, such as California, Illinois, and Michigan, are more restrictive and require the consent of all parties before monitoring. The Illinois law allows monitoring when at least one-party consents in limited circumstances, such as for monitoring telemarketing solicitations.

Others also have enacted laws that specifically regulate monitoring computers and e-mail. For example, Delaware requires employers to provide written notice of any monitoring of telephone, Internet, or e-mail use. Connecticut also requires written notice of any electronic monitoring, but exempts employers that use the monitoring to collect evidence of unlawful activity or hostile workplace harassment.

### **Access to Stored Electronic Communications**

Employer monitoring of stored e-mails and voicemails is much less regulated and generally allowed under federal law. Under the ECPA sections codified at 18 U.S.C. §§2701, et seq., employers that provide electronic communication service may access messages once they are stored in their computer or telephone systems, without notifying employees of the access.

### **Best Practices Include Reasonable Policy, Selective Monitoring**

As discussed above, the law allows employers to monitor when certain conditions are met, and most businesses find there are legitimate business reasons to retain the right to do so. However, any type of surveillance can cause serious morale problems if not handled appropriately. No one likes to be spied on, particularly when engaged in personal, non-work related activities, even if these activities occur at work.

To reduce these problems, your best bet is to be "up front" – communicate your policy carefully and clearly, and then monitor only to the extent necessary. The following five strategies will help your organization prevent abuse while promoting positive employee relations.

#### **1 - Develop a policy specifically addressing monitoring of employee communications and educate your employees about it. The policy should:**

- Clearly state that the computer system and communications services are the property of the employer;
- Reserve the right to monitor employees' electronic communications;
- Explain the business-related reasons for the monitoring;
- Describe permissible work-related and personal telephone, e-mail, and Internet use;
- Prohibit inappropriate use, including: excessive personal use; sending, accessing, or storing discriminatory, harassing, defamatory, or pornographic material; duplicating or distributing copyrighted material without permission; and transmitting confidential, proprietary, or trade secret information; and
- Include penalties for policy violations, up to and including termination.

**2 - Keep the monitoring work-related.** Acceptable reasons include monitoring to respond to a complaint regarding policy violations or to improve employee performance, customer relations, and the quality of products and services.

**3 - Make it reasonable regarding personal use.** A policy that prohibits all personal use is usually both impractical and virtually impossible to enforce in many employment environments. Similarly, draconian punishments for a relatively minor policy violation will understandably be viewed as unfair by many of your employees.

**4 - Check state law.** If you are in a state that requires the consent of all parties to monitor telephone calls, consider adding a prerecorded message to all incoming and outgoing calls to inform non-employees of potential monitoring.

**5 - When in doubt, give notice and get consent.** Remember, monitoring is always legal when you get consent, so if you are going to monitor employees, have them sign off on it when they are hired or when you start monitoring.

Reprinted with permission from HR Matters E-Tips, copyright Personnel Policy Service, Inc., Louisville, KY, all rights reserved, the HR Policy and Employment Law Compliance Experts for over 30 years, 1-800-437-3735. Personnel Policy Service markets group legal service benefits and publishes HR information products, including a free weekly electronic newsletter, HR Matters E-Tips ([www.ppspublishers.com/hrmetips.htm](http://www.ppspublishers.com/hrmetips.htm)). This article is not intended as legal advice. Readers are encouraged to seek appropriate legal or other professional advice.