



THE LEGALITIES OF MONITORING EMPLOYEE COMMUNICATIONS: WHO HAS THE RIGHT AND WHEN?

By John S. Caragozian and Donald E. Warner

© 2008 All rights reserved.

Dozens of software programs allow monitoring of computer activity. Certain programs record every keystroke on a computer. Other programs take a periodic snapshot of what is displayed on the monitor. Still others copy all outgoing and incoming e-mails and designate where to send the copies. Much of this software can be installed and used surreptitiously by employers.

The American Management Association's 2007 Electronic Monitoring and Surveillance Survey indicates that many private employers install software to monitor employees' computer use. Employers give various reasons for monitoring. For example, some employers want to:

- reduce employees' time spent online for non-business, personal purposes.
- minimize the circulation of racist, sexist, pornographic, or other inappropriate material, which might create liability against the employer.
- avoid disclosure of confidential information.

While these and other reasons may be legitimate, employers still must reckon with legal restrictions on monitoring. The purpose of this article is to introduce some of these restrictions.

FEDERAL LAW

Under federal law, it is generally a felony to intercept the contents of computer or telephone communications (including text messages). It also is a felony to disclose or use the illegally intercepted communications. Punishments may include up to five years' imprisonment. The same law also provides a right for victims to sue civilly and recover either actual damages or a statutory amount (whichever is greater), plus attorneys' fees and, if appropriate, punitive damages.

This general law contains several exceptions, which would eliminate criminal or civil liability. Four of these exceptions are discussed below.

1. Consent

The first and cleanest exception is consent. If one of the parties to the communication consents to its interception, disclosure, or use, then federal law is not violated. The consent may be express or implied. An example of express consent is where an employee signs language such as:

I expect no privacy whatsoever in using my Company computer. I consent to Company monitoring, intercepting, disclosing, and otherwise using my computer communications and other computer activities for any and all purposes, including personnel and legal action against me. This consent applies to any and all of my computer communications and activities (including e-mail, instant messaging, Internet contact, or word processing or other document preparation) and applies regardless of whether the communications or activities are for Company, personal, family, social, or other purposes.

An example of implied consent is where employees do not sign a form, but are warned before any interception that the employer will intercept, disclose, and otherwise use computer communications or activities. This warning could be in an employee manual or it could pop up when the employee switches on his or her computer. An example of an implied consent or warning is as follows:

Warning

By using your Company computer, you acknowledge that you expect no privacy whatsoever in using your computer. Further, by using your Company computer, you consent to Company monitoring, intercepting, disclosing, and otherwise using your computer communications and other computer activities for any and all purposes, including personnel and legal action against you. This consent

applies to any and all of your computer communications and activities (including e-mail, instant messaging, Internet contact, or word processing or other document preparation) and applies regardless of whether the communications or activities are for Company, personal, family, social, or other purposes.

If, after getting such a warning, an employee uses his or her computer, consent to the employer's interception, disclosure, and use is implied.

Some employers might be rightly concerned about the effect that such express or implied consent could have on employee morale. On the other hand, consent might reduce inappropriate computer use. Also, these consents are analogous to "at will" employment provisions: the more the language is softened, the less legal protection is provided to employers. Indeed, some federal case law holds that employers failed to prove consent when they merely warned employees of the employer's "capability" to intercept communications or warned that communications "can" or "might" be intercepted.

While consent generally is a defense to employer liability, it is not absolute. Examples of situations where consent may not be a defense include:

- Federal law provides that consent is not a defense if the intercepted communication is used for any "criminal or tortuous act." An illustration of such an act might be where an employer learns an employee's bank account number and password and then steals funds from the account.
- If an employer's formal policy expresses or implies consent, but, in reality, the employer's conduct provides for some confidentiality of communications, then consent may not be a defense.
- Federal labor law bars surveillance of employees' communications related to organizing or other union activities, and this bar generally cannot be waived.

2. Ordinary Course of Business

Even if no consent is obtained, federal law permits interception, disclosure, and use by the provider of the communications equipment (presumably, an employer) "in the ordinary course

of its business.” Numerous courts have interpreted this language, sometimes with conflicting results and always based on the facts of the specific case. In general, these cases suggest: (a) that the fact that an employer owns or has provided the computers is by itself insufficient to invoke the “ordinary course” exception, (b) an employer cannot necessarily use the exception to justify blanket interception, disclosure, and use of all employee communications, and (c) at least some employers must prove that they took reasonable steps to intercept, disclose, or use only particular communications of interest to their business.

3. Storage

Courts have interpreted the federal prohibition on interception as requiring “contemporaneous” or “real time” interception and have held that an employer’s accessing of communications from the employer’s own “storage” does not violate federal law. Unfortunately, courts have had difficulty in applying these terms to modern technology. For example, if an e-mail message is stored for a split second as part of the transmission process, and if the specific surveillance software accesses the communication during that split second, is the law violated?

Similarly, federal law permits a communications provider—such as an employer—to access computer communications from its own storage. Does this permission include allowing an employer to obtain the communications stored by an outside company that contracts to provide communications services to the employer?

While courts continue to parse these linguistic and technological details on a case-by-case basis and without final consistency, it generally appears that communications or other material stored on the employer’s own server or other storage may be accessed by the employer without running afoul of federal law. Likewise, accessing communications and other material stored on the employee’s employer-provided computer, especially after an employee is no longer employed by the employer and has left behind the computer, may be lawful under federal law.

4. Content

Federal law prohibits the interception, disclosure, or use of the content of a communication. While no courts have made a judgment to this effect, it is perhaps worth questioning whether it would be permissible under federal law for an employer to monitor an

employee's time spent on various computer activities. For example, an employer might argue that software that tracks an employee's Internet use by Web site address and time but not its content should be permissible under the law. On the other hand, if the Web site address suggests its content (such as "LookingForANewJob.com"), then perhaps a federal violation would occur.

STATE LAWS

Many states have their own criminal and civil privacy laws, including broad common law and statutes that may prohibit interception of communications. A few states even have statutes that apply specifically to interception of workplace computer communications. While it is beyond the scope of this article to describe all applicable state laws, it is important for employers to be aware of three threshold issues.

First, state laws that protect people—including employees—beyond federal law are generally not preempted by federal law. For example, to prove consent, several states require all parties to a communication to consent to the interception. By contrast, as noted above, federal law requires the consent of only one party. Accordingly, if an employer were to intercept an employee's communication with an outsider and could prove that the employee had consented to the interception, then no federal violation would have occurred. The employer, however, still might be liable under state law, if the state requires the consent of all parties.

Second, what happens when the intercepted communication is between two persons working in different states, one of which prohibits the interception, while the other permits it? Courts have wrestled with these conflicts without forming a clear pattern.

Third, regardless of whether a state requires one party or all parties to consent and regardless of which state's law applies, consent is typically a defense to a state prohibition on interception. As a practical matter, employers might afford themselves some protection by (1) having their employees expressly or impliedly consent as set forth above, and (2) also warning—and thereby obtaining implied consent from—outsiders with whom employees communicate, say, by automatically adding similar language to all outgoing communications.

Employers should be aware, however, that consent might not always be a defense. Some state privacy protections might not be capable of being waived, so consent to them would not be a defense.

CONCLUSION

Federal law and state laws, by themselves, are complex and difficult to apply. The interplay between federal and state laws and among various state laws adds to the difficulty. Employers should seek legal advice, beyond what is provided in this article, before monitoring employee computer use.

John S. Caragozian is a California lawyer who has written and lectured on workplace computer and other privacy issues. His articles have appeared in the Daily Journal, California Business Law Practitioner, and Los Angeles Lawyer. He currently is corporate secretary and senior counsel at Sunkist Growers, and continues to consult on privacy matters for outside clients and lawyers.

Donald E. Warner is a lawyer in Los Angeles specializing in employment law, representing employers. His interest in employee Internet privacy issues had its origin in privacy matters that he handled, both in and out of court, for his clients.