Levett, Rockwood & Sanders P.C.

NEWSLETTER
A Courtesy To Our Clients and Friends

September, 1998

WATCHING BIG BROTHER: Electronic Monitoring in the Workplace

Companies frequently use electronic devices to monitor the workplace. Cameras may be used to detect theft; customer-service telephone calls may be recorded to assure quality control; and electronic communications may be monitored to insure security of confidential information and compliance with company policies regarding e-mail and the Internet.

But electronic surveillance and monitoring are regulated activities. So if your company is considering any of these measures, you should be aware of the restrictions, including a brand-new Connecticut law that takes effect on October 1, 1998.

NEW CONNECTICUT LAW

The new law, Public Act 98-142, requires employers using any type of electronic monitoring to notify all affected employees in advance in writing. The notice must inform the employees of the types of monitoring which may occur, and the employer must post the notice "in a conspicuous place which is readily available for viewing by its employees."

"Electronic monitoring" under the new law is defined very broadly. It means "the collection of information on an employer's premises concerning employees' activities or communications *by any means other than direct observation,* including the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems."

Exceptions are made for collection of information for security purposes in areas open to the public, and when an employer has reasonable grounds to believe that employees are engaged in conduct which is illegal or creates a hostile workplace environment. In such cases, no prior notice is required. But employers should be careful in relying on these exceptions. The penalty for each violation can be up to $3,000.

Examples of notices required under the new law might include the following:

- The warehouse and factory floor areas are monitored by television cameras to help protect against theft or other loss of company property.

- All use of the company's computer system is subject to monitoring to insure security and protect against violations of company policies.

The new law says that an employer only needs to "post" such a notice. The safest approach, however, is to also include a notice in any employee handbooks and any other places where it is likely to come to the attention of affected employees, and to obtain written consent from employees to any monitoring policy.

OTHER LAWS

The new law supplements many other laws that regulate electronic monitoring in the workplace. The full scope of these laws is quite extensive. The following summary and attached chart discuss only certain key areas of interest to employers.

***Listening* to Phone Calls**. Federal and state laws both prohibit intercepting or overhearing phone conversations with two important exceptions. The first is where one party to a call consents to the monitoring. To come within this exception, it is recommended to obtain prior written consent from the employee to the monitoring policy.

The other exception is for monitoring phone calls on company phones "in the company's ordinary course of business." To come within this exception, the employer must: (a) give reasonable notice that monitoring or recording might occur; and (b) limit such activity to "legitimate business purposes."

What constitutes a "legitimate business purpose" obviously can be disputed. The courts generally uphold purposes

33 Riverside Avenue Westport, CT 06880 (203) 222-0885

such as training and quality control for dealing with the public, and good-faith efforts to detect suspected wrongdoing. To minimize disputes, however, it is always safer to obtain actual consent from employees in advance, preferably in writing

***Recording* Phone Calls**. In Connecticut, *recording* of phone calls is regulated more strictly than merely listening to phone calls. Federal law treats both activities the same, but Connecticut state law limits recording more strictly, prohibiting recording except where:

(a) all parties to the call (not just one party)consent to the recording; or
(b) all parties to the call are informed at the start of the conversation that it will be taped; or
(c) a warning tone is repeated every 15 seconds during the part of the call being taped.

[over ☞]

The strict requirements under the Connecticut law are important reminders to always check local laws. You can't simply rely on federal law alone, or on what you hear on the news about cases in other states.

E-Mail Privacy. The laws governing e-mail are still developing, and the permitted scope of e-mail monitoring is a much-debated topic. At a minimum, it is clear that the federal anti-wiretapping laws, and Connecticut's new workplace monitoring law (but not Connecticut's special telephone recording law), apply to e-mail. As a result, workers have some legitimate expectations of privacy regarding e-mail These expectations may be heightened by an employer's actions, such as providing confidential passwords, or making statements about providing privacy for on-line communications.

At the same time, exceptions under the state and federal surveillance laws may also allow monitoring e-mail on company computers. This is certainly true where the employee has given consent. Less clear is the "ordinary course of business" exception, which is phrased only in terms of "telephone and telegraph equipment" in the federal statute, but which some commentators believe may be interpreted to apply to e-mail. In addition, an employer, as the provider of an e-mail system, may be able to rely on an exception for providers of communications systems to monitor communications on the system in the normal course of business to protect the rights or property of the provider.

Two other factors should be noted. First, expectations of privacy may diminish where employees are clearly informed that the company owns the equipment, that a systems administrator has access to all communications, and that the system is intended only for company business. Second, federal law does not restrict *retrieval of stored messages* by providers of systems (including employers), and most cases of employee e-mail monitoring involve reviewing stored messages rather than reading them as they are sent.

Because the law governing e-mail privacy is still developing, it is advisable for a company to adopt clear and specific policies regarding use and monitoring of e-mail and electronic communications in addition to any other monitoring policies the company might have.

Face-to-Face Conversations. Federal and state laws both prohibit using electronic devices to overhear or record face-to-face conversations unless at least one party to the conversation consents. Thus, a party to a conversation generally may record that conversation. However, one Connecticut court has ruled that an employ*ee's* taping of private conversations with another employee may violate a constitutional right of privacy. To be safe, therefore, it is always better to obtain employee consent to monitor or record a conversation, even where a representative of the employer is a party to the conversation and has consented.

Restricted Areas. A 1971 Connecticut law absolutely prohibits use of any electronic surveillance device or system (audio, visual or other) "in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as rest rooms, locker rooms or lounges." This law thus limits the places where monitoring is allowed, even when proper notice is given under the new law.

COMPANY POLICIES

The following are some guidelines to keep in mind regarding company monitoring policies:

- Post any policy in a prominent place where the affected employees will see it.
- Limit any monitoring to legitimate business purposes, and state those purposes in the policy.
- Do not monitor in areas designed for the health or personal comfort of employees, such as rest rooms, locker rooms or lounges.
- Obtain written consent whenever possible.
- For telephone policies, be specific on the scope of the monitoring. For example, advise which types of calls are covered and notify personnel whether company phones may or may not be used for personal calls.
- Upon determining that a monitored call is personal in nature, do not then monitor the content of the call.
- For on-line policies, consider a disclosure on a log-in screen and, if possible, add a mandatory acceptance procedure to initially access the system.
- Clearly advise personnel whether company computers may or may not be used for personal e-mail, and remind employees that computers are company-owned and that the company reserves the right to monitor and review all use of its system.
- As with all personnel policies, provide a copy to new hires for each to retain prior to acceptance of your offer of employment.

The above suggestions provide only a general outline for monitoring policies. If you would like assistance in developing any policies, please feel free to contact **Ed Chansky** or **Dorit Heimer** of our office at 203-222-0885. Other issues concerning e-mail and electronic files, including security and document retention policies, will be discussed in a future newsletter.

Summary of Connecticut and Federal Statutory Requirements Governing Certain Types of Electronic Monitoring in the Workplace*

	Phones	E-mail	Face-to-Face Conversations	Video Monitoring (no sound)
Connecticut	Notice, plus For Monitoring: consent of 1 party. For Recording: all-party consent; or notice at start of call to all parties; or beep every 15 seconds.	Notice	Notice, plus consent of 1 party Prohibited in areas used for employee health & comfort	Notice Prohibited in areas used for employee health & comfort
Federal Law	For Monitoring or for Recording: 1-party consent; or act in ordinary course of business to protect property or rights of the provider of the phone service; or notice plus legitimate business purpose in the ordinary course of employer's business	1-party consent; or act in ordinary course of business to protect property or rights of the provider of the e-mail service; or retrieval of archived messages by provider of e-mail service	1-party consent	Not regulated

* The above chart is merely a summary. Additional restrictions may apply due to labor union agreements, constitutional privacy issues or other reasons. Other forms of monitoring may also be regulated, and laws may change over time. If you are considering an actual monitoring program, seek legal advice regarding the details of the program.

33 Riverside Avenue Westport, CT 06880 (203) 222-0885