Where are the lines in employee surveillance?

July 25, 2011 | Curtis Smolar

(Editor's note: Curtis Smolar is a partner at Ropers Majeski Kohn & Bentley. He submitted this column to VentureBeat.)

A reader asks: I have had theft of trade secrets in my office. Can I install video cameras or other surveillance measures to view the activities of my employees?

Answer: While spying on your employees happens all the time in movies, if you're planning to monitor your employees in the real world, it's best to proceed with caution. Although some surveillance at work is allowable, the more invasive it gets, the more likely it is that it will be unacceptable.

That said, if you company policy explicitly describes a diminished expectation of privacy at work, it will go a long way towards protecting your company. Lastly, don't be secretive about the video surveillance.

When it comes to surveillance, there are generally four kinds used.

Work related data – This is generally any information pertaining to the hours and quality of work done by employees. This type of monitoring is usually acceptable because it's directly related to the employee's employment, e.g. how well the employee is doing their job.

Additionally, employers are presumed to monitor their employee's hours. Here are some of the less invasive examples of this:

- *Key card access* – Many businesses have locked doors that can only be opened by key cards. These key cards are specifically coded to specific individuals and a record is kept when this employee enters or exits the premises. This, in many cases, is as much for the employee's protection as it is for the company's – as it helps discourage non-employees from entering the office. That said, the information collected is identifiable and is arguably personal. But, because of its general nature, it is probably not objectionable.

- *Log on screens* – Log on screens are screens that pop-up on an employee's computer and require them to enter their username and password. Once this is entered the employee is allowed access to the computer system. Although this is a security device, it also tells the employer when the employee is at work and/or the employee's general location. Because of the general non-invasiveness of this procedure it, too, is generally allowed.

- *Time cards* – Time cards keep track of the employee's time which is used to determine compensation. They are also essential to make sure the employee is within compliance for wage and hour purposes. In some cases the time cards have been integrated into the computer system and will be tied to the log on screens discussed above. This is also generally seen as non-invasive.

Computer data – Computer data falls into the middle category of invasiveness for employees. In some cases, computer data can be the most invasive area of the employer-employee relationship. As discussed in a previous column, the most important issue is that the employer needs to have a clear computer policy, which explicitly states that anything created, sent, received or otherwise done by an employee on company computers belongs to the company and that said

equipment is for official business only, and content viewed on it is monitored periodically.

This policy should include all media, including office-owned cell phones and laptop computers. Otherwise there may be a claim by an employee that emails (or other files read by the employer) are an invasion of the employee's privacy.

It's worth noting that the courts are currently in conflict regarding the privacy of web-based data. By including a statement in the company manual that this data is not private could protect you.

Video monitoring – Video monitoring is often considered very invasive to employees. In many states, an expectation of privacy extends to the work environment. In California, the state constitution grants individuals at work a right to privacy. Additionally, California statutes protect employees from being videotaped in areas where they are getting dressed or undressed. The gray area is when video recording of employees is primarily meant to deter crimes at the workplace.

In *Hernandez v. Hillside, Inc.*, the California Court of Appeals held that employees have an expectation of privacy and that being surreptitiously videotaped is a violation of this expectation. However, the court did find that there might be acceptable ways to videotape– e.g., when you provide notification of the company policy that they are subject to being videotaped.

Audio Recording – In many states, recording conversations – including phone conversations – violates not only the individual's right to privacy but also may be illegal. In California there is a penal code section that states that it is a misdemeanor to record another person without their consent. This statute also creates civil liability for individuals for such actions.

Accordingly, this law protects individuals at work and also trumps one-consent audio recording states — meaning that if someone from a Texas is talking to

someone in California and records the conversation, courts have held that California will apply its law and the taping will considered illegal.

Generally your company's written policy will determine the expectation of privacy an employee has at work. The broader the policy and the more detailed it is as to different technologies used for monitoring the better the chance that the courts will find that the employee had a diminished expectation of privacy.

Startup owners: Got a legal question about your business? Submit it in the comments below or email Curtis directly. It could end up in an upcoming "Ask the Attorney" column.