Big Brother, Big Implications: Creating an Employee Monitoring Policy Without Creating Additional Legal Liability

May 8, 2010 by Adam Santucci

This post was contributed by Samuel N. Lillard, Of Counsel, and Anthony D. Dick, an Associate, members of McNees Wallace & Nurick LLC's Labor and Employment Practice Group in Columbus, Ohio.

According to recent estimates, upwards of 90 percent of employers monitor employee workplace activity in some way or another. The appeal is obvious. When done properly, monitoring can help companies increase productivity and efficiency, protect assets and proprietary information, and identify and hopefully prevent harassing conduct, libel, employee theft, vandalism, hacking, and other inappropriate behavior. But when companies overstep permissible boundaries, their monitoring efforts can have severe legal and financial consequences. There are a substantial number of cases, including several recent decisions, where companies have learned the hard way that their right to monitor employees' work activities has limits.

For example, in Hernandez v. Hillsides, Inc., 47 Cal.4th 272 (2009) (pdf), the employer, in a legitimate effort to determine who may have been viewing pornography on a work computer late at night, placed surveillance cameras in certain employees' offices without the employees' knowledge. Instead of catching the offender, the employer captured images of employees changing their clothes for post-work workouts, female employees viewing their pregnancy scars, and other private activities. In ruling against the employer, the California Supreme Court held that although employees' right to privacy in work offices is not absolute, they have "a reasonable expectation of privacy under widely held social norms that the employer would not install video equipment capable of monitoring and recording their activities – personal and work-related – behind closed doors without their knowledge or consent."

In a recent New Jersey case, Pietrylo v. Hillstone Restaurant Group, 2009 WL 3128420 (D.N.J. 2009) and Pietrylo v. Hillstone Restaurant Group, 2008 WL 6085437 (D.N.J. 2008), two restaurant servers created a password protected MySpace page where they and certain fellow co-workers could go to vent about the trials and tribulations of working in a restaurant. A supervisor learned of the MySpace page and pressured an employee with access to give him the password. Once on the site, the supervisor found messages that included sexual remarks about members of management and customers and references to violence and illegal drugs. The two servers who created the page were terminated and subsequently sued under stored communications laws that limit which individuals may access stored electronic communications. The trial court denied summary judgment to the employer holding that the restaurant's employee monitoring authority did not include private online communications on a social network outside of work. The two employees subsequently won a small jury verdict.

The U.S. Supreme Court is set to decide a public sector employee monitoring case in its current session. In City of Ontario v. Quon, 529 F.3d 892 (9th Cir. 2008), cert. granted Dec. 14, 2009 (pdf), City of Ontario SWAT officers were given police-department-owned pagers that allowed them to send text messages. They were told in a meeting that the text messages would be treated like e-mails under the City's employee monitoring policy and that the City would have the right to review such messages at any time to determine whether the pagers were being used for personal purposes. Despite the representations made in the meeting, officers received mixed messages from supervisors and other staff members as to whether the City would actually ever review the messages. Sgt. Jeff Quon, an officer who was issued a pager, used it on numerous occasions to send sexually explicit text messages to his wife and mistress. At some point, the City of Ontario requested Quon's transcripts from the wireless provider without his permission and read the personal messages. Quon sued claiming the City violated his Fourth Amendment right against unreasonable searches. The lower court ruled in favor of the City. The appellate court reversed. The Supreme Court recently heard oral arguments and a decision is expected in the coming months.

These cases should serve as a warning to employers. While there are no hard and fast rules to ensure that your business does not find itself involved in litigation concerning workplace surveillance and employee privacy issues, adhering to a few basic principals can help minimize the potential liability.

1. **Put it in Writing**. Courts are much more likely to rule in favor of the company in any employee privacy suit when there is a clearly articulated written policy in place. At a minimum, it should state under what circumstances, if any, an employee should have a reasonable expectation of privacy and list all the mediums and ways in which the company may monitor employees (i.e. video surveillance, telephone monitoring, e-mail monitoring, Internet monitoring, GPS tracking of company vehicles and employees, etc.)

2. **Clearly Communicate the Policy to Employees**. A written employee monitoring policy is of little value if employees are not aware it exists. The policy should be incorporated into the Employee Handbook and distributed on a semi-annual or annual basis. Any time the policy is changed or updated, the new policy should immediately be distributed to employees. Each time the policy is distributed, it is a good idea to have each employee sign an acknowledgment that they have read and understand the policy.

3. **Know Your State's Laws**. While federal law contains relatively few restrictions on employee monitoring, state law may vary. For example, in some states employee notification is required if an employer is utilizing electronic surveillance. Similarly, in some states, employees must give consent to be monitored by video surveillance. Determine exactly what the law is in your state and whether it is more restrictive than federal law.

4. **Be Consistent!** Even-handed enforcement of the policy is essential. A perception that a certain individual or group is being targeted in enforcing an employee monitoring policy can quickly lead to a claim for discrimination.

While employee monitoring is commonplace and can be a useful tool in increasing employee efficiency and protecting company assets, employers should be aware of the potential pitfalls in implementing and enforcing an employee monitoring policy. A well thought out and carefully crafted employee monitoring policy could be invaluable to protecting a business's valuable assets while minimizing any potential legal liability. Most savvy business owners will contact a trusted and knowledgeable attorney if they are contemplating implementing such a policy.