BusinessManagement DAILY

JANUARY 14, 2014

Weigh pros, cons of surveillance in wired workplace

by Matthew Webster, Esq., Gray Plant Mooty, Minneapolis

As technology becomes more and more intrusive, today's employees naturally wonder how far their employers can pry. While the U.S. Constitution doesn't expressly mention a right to privacy, most people hold this concept dear, and courts have long recognized cases alleging invasion of privacy.

Employees who disclose personal information on social media sites may hotly contest an employer's use of that information. Those same employees are also often upset at an employer's ability to search their email, survey their computer searches and monitor their keystrokes.

Employers, on the other hand, are often afraid not to search online for information about prospective and current employees. Concerns about potential liability and lost productivity make surveillance an attractive option. New technologies like theft detection software, remote electronic tracking and facility-access recording devices have only intensified this long-running debate.

Carefully weigh the risks and benefits when evaluating whether any form of employee surveillance is right for your organization.

Surveillance and the law

Many state and federal laws affect workplace surveillance. For example, employers are prohibited from obtaining information related to employees' protected class status, such as national origin, religion, sexual orientation or family medical history.

Workplace surveillance may violate the National Labor Relations Act by discouraging union organizing or collective bargaining.

Many states prohibit employers from taking negative employment action against employees for their use of lawful consumable products such as tobacco or alcohol on their own personal time.

Surveillance could reveal all those characteristics or activities.

Federal and state laws also proscribe surveillance that results in retaliation against whistle-blowers. Some states' laws restrict audio and video recording in the workplace.

Surveillance of any sort can injure the relationship between management and employees, creating a culture of mistrust. Conversely, measures such as electronic productivity monitoring might actually align employees' interests with management, resulting in a more productive and collegial workplace.

Notice helps

When engaging in any type of employee surveillance, it may be wise to provide some form of advance notice to employees. Consider obtaining a signed acknowledgment from employees. Areas subject to video monitoring should have a clear and visible notice that monitoring is taking place. That helps dispel any expectation of privacy and makes surveillance seem more reasonable to employees.

Narrowly tailored

You should have good business reasons to justify employee surveillance, and surveillance should be narrowly tailored to that business purpose.

Such business reasons could include decreasing employee dishonesty or theft, promoting workplace productivity or efficiency, responding to inappropriate technology usage and investigating misconduct.

The surveillance should be limited in time, scope and subject matter. You should plan to only gather information sufficient to accomplish the business purpose.

Whether you currently employ workplace surveillance or are just exploring the feasibility of surveillance, ensure that it's designed to serve—and only serve—a legitimate business purpose.

On an issue as sensitive as employee surveillance, it's especially important to discuss it with your attorney.

Matthew P. Webster is an associate in Gray Plant Mooty's Minneapolis office, representing employers in all areas of labor and employment law and litigation. Contact him at (612) 632-3000 or ***matthew.webster@gpmlaw.com****.*

What to include in tech policies, user agreements

Any employer that provides telephones, computers or mobile devices should craft a clear technology policy that governs proper use and lists impermissible uses of workplace technology and social media.

The policy or user agreement should also specify when employees' technology usage may be monitored. It should remind employees that technology used on company-provided or -reimbursed devices is not private and can be monitored by the employer.

The policy should specify prohibitions and limitations on employees' use of workplace technology. It might also prohibit or limit personal use of technology on company time, as well as using that technology for unlawful acts such as harassment.

The document should also instruct that employees are not to disclose or improperly use the employer's confidential information, trade secrets or sensitive financials via technology.

The policy might also instruct employees that any endorsements of the company or its products must be truthful and disclose the employee's relationship with the company.

7600 Leesburg Pike, Suite 300, Falls Church, VA 22043-2004 (800) 543-2002

Consider prohibiting or limiting technology use by nonexempt employees outside normal working hours, in order to minimize compensable “working time.”

Finally, the policy or user agreement should state that all company devices are to be returned when employment ends. Employees may also be required to permit removal of any company-related data from employees’ personal devices used for work.