



BALANCING EMPLOYEE MONITORING WITH PRIVACY CONCERNS

Is it legal to “keep an eye” on employees? If employees agree to be monitored, can you conduct routine surveillance on the company team?

Employees are entitled to some privacy on the job, but as a business owner, you’re entitled to keep up with employee activities – especially as these activities relate to employee performance.

What are the rules and regulations regarding monitoring company employee activity?

To keep up with the latest on Nevada employee privacy law, we interviewed **Swen Prior, a labor and employment partner with the law firm of Snell & Wilmer in Las Vegas**. Prior has been involved in many important legal decisions and writings on labor and employment issues in Nevada.

For **Business telephone** recording and monitoring, Prior pointed out that, “Nevada is an all-party consent state, which means that all parties must consent to being recorded during a telephone conversation. Blanket contracts where employees consent to having telephone conversations recorded are not recommended and likely do not act as employee consent.”

“**Personal calls** have an important exception,” he said. “When an employer realizes the call is personal, he or she should immediately stop monitoring the call. So the issue is not necessarily whether the call was made from a business phone or from a personal phone ... however, an employee can be disciplined for abuse of the company phones system, etc., which should be spelled out in the employees’ handbook and policies.”

Business-owned computers fall into the same category as business telephones. If the computer is owned by the company, employers are generally entitled to look at employee activity, including personal emails and texts. Prior reiterated the importance of having a “clear computer use policy that states that the employee has no expectation of privacy as to the computer or device that is owned by the company.”

Email accounts: Under some circumstances personal email accounts may also be examined if access to the account was obtained through a business-owned device. However, if the employee uses a personal device to access the Internet, employers should avoid monitoring. Prior explained, “Employers can monitor equipment which they own. However, employers do not have a right to monitor email hosted by a third party, like web-based email programs. Certainly, if your software shows repeated access to personal e-mail on company time, then that is a disciplinary issue. But reading and capturing the employee’s e-mail from a third-party host could raise a potential violation of privacy claim.”



Surveillance cameras in the workplace are considered legal, especially in common areas, or areas within the company's premises where valuable items or information are stored. Employees can expect privacy in locker rooms, rest rooms, and changing rooms, however.

Prior clarified that "there is a bizarre distinction between surveillance with audio vs. silent surveillance. If the location uses audio and visual surveillance, then the employers should take several steps to ensure that there is no expectation of privacy. For example: the location should post a sign in a conspicuous location that states "AUDIO RECORDING IN PROGRESS" or something to that effect. Also, the employer should include a provision in the employee handbook that audio and video recording are conducted. Employees should then sign a consent form as a condition of employment. Best practice is to avoid audio surveillance and limit your 24 hour surveillance to video-only."

Creating Balance in Employee Monitoring

In today's tech-connected workplace, the difference between business and personal communications varies from company to company. In order to maintain staff morale, it's critical to publish all company monitoring policies so all parties - employees, customers, company management, and call recipients - understand the company's policies.

Sometimes, employees may access company files using their own equipment over the weekend. An employee may place an online business order using a company telephone, but on his or her own time. The line between business and personal communications isn't as clear as it once was. In fact, some businesses encourage employees to BYOD - bring your own devices - to conduct routine business. According to Prior, "the technology trends (such as the BYOD policies) will continue to merge employees' personal lives with their work lives." So it is important that "employers implement protocols and consent agreements regarding the use of, and disclosing the companies inspection and ownership rights of, the various technological systems."

Monitoring employee activity is essential to maintaining productivity levels, to help avoid employee theft, and to identify possible cases of data theft by employees moving on to another company. Prior notes, however, that "employers should be mindful of the potential legal issues implicated when monitoring employees. There are very important questions of law that must be addressed with regard to employee monitoring and surveillance. Both federal and state laws dictate the use of electronic recording equipment. The unlawful monitoring by employers can give rise to a civil suit for invasion of privacy and potentially expose the employer to criminal prosecution."

According to Prior, the key to minimizing your litigation exposure is to "provide notice of your monitoring and privacy expectations in the workplace in various handbooks and policy statements and then to obtain consent and acknowledgments of these policies from your employees." It is important to be open and honest with employees. For example, if you install key logger software to monitor employee activity, employees should be notified and accepted practices laid out in detail.

Develop a clear, legally defensible company policy on the use of business equipment so employees understand acceptable behavior using company-owned equipment.

Also, by informing employees and obtaining acknowledgments of your company's monitoring policies, you may avoid a costly lawsuit brought by a disgruntled employee who feels his or her privacy has been unjustly tracked by your company.

Create an open policy, inform employees of acceptable practices, and legally track employee performance with the advice of your business' legal counsel.

Protect your company's rights, and protect your employees' rights, with good advice from a legal professional and a clear, unambiguous privacy policy.

The information provided is presented for general informational purposes only and does not constitute tax, legal or business advice.

Source: NevadaSmallBusiness.com

Copyright 2014

Reprinted with permission.

