What You Should Know Before Monitoring Your Employees and Guests

Publication
3.15.15

Lonnie Giamela and John Mavros' article,"What You Should Know Before Monitoring Your Employees and Guests" was featured in the *Hotel Executive*.

Employees can make or break businesses in the service industry. While customer service oriented employees create a luxurious experience at a lesser establishment, employees that don't prioritize customer service can ruin a guest's experience even at the most finely-appointed hotel.

However, managers and supervisors cannot always be present to recognize and reward desirable service practices, nor can they always be present identify and correct poor practices. With so many points of customer and employee interaction, surveillance is one of the most effective methods to safeguard employee safety and integrity, review employee performance, identify training points, and document "HR issues." Of course, too much of a good thing can be a problem. Employers must understand the difference between valid surveillance and illegal intrusions on privacy rights before taking advantage of video/audio recordings. This article aims to help employers stay on the right side of that fence.

1. What is a "reasonable expectation of privacy"?

The law regarding privacy in the workplace was most recently defined by the California Supreme Court case in *Hernandez v. Hillsides, Inc.* The rule is subjective, yet straightforward—employers must not engage in any activities that would violate an employee's "reasonable expectation of privacy." This helps determine the degree to which a person can reasonably expect to be left unmonitored, but the problem is that it is a nebulous standard that relies on "widely accepted community norms."

There are some obvious places an employee or guest will reasonably expect privacy, for example, in a bathroom stall. However, courts will look at several considerations to determine the reasonableness of an individual's expectation of privacy, such as the customs, practices, and physical settings of the workplace. Other considerations include where the surveillance equipment will be placed, when it will be active, and who will have access to recorded data.

The time and place of activities is another important factor. This includes an inquiry into the physical layout of the area being monitored, whether the area is restricted access, limited from view, or

reserved for performing bodily functions and other personal acts. On the other hand, if an area is open and accessible to coworkers or the general public, or work is performed in the area, employees are unlikely to have a reasonable expectation of privacy.

Courts will also consider who has access to any recordings or videos to determine the severity of an alleged invasion of privacy. In fact, even if an employer collects monitoring information legitimately, an employer may be subject to liability if the information can be accessed by the wrong people. A non-managerial employee should not have access to a recording of his or her co-worker. If the purpose is to monitor customer service performance, only managerial employees should have access. For this reason, employers' must carefully control who has access to any monitoring data.

2. What are you looking for?

Employers may have a variety of reasons for monitoring its employees, but employers must always have a legitimate purpose behind their monitoring practices. Examples of legitimate business needs includes hotel security, loss prevention, employee accountability, training and development, and other legal requirements. It is important for an employer to tailor its monitoring program to a legitimate purpose and have documentation that identifies that link. Without it, employers are subjecting themselves to potential invasion of privacy claims.

3. Always provide notice

Before monitoring an employee, an employer should always provide written notice. Courts have held that written notice can be the difference between whether an employee has waived his right to privacy or not. Indeed, one of the most effective ways to keep a person from expecting privacy is to tell the person he/she is being watched. With written, documented notice, an employer can better defend against an invasion of privacy claim.

On rare occasions, notice might obviate the purpose of surveillance. Employers may implement surveillance programs to investigate an existing pattern of misconduct. In which case, courts have found that an employer's interest in identifying and eliminating misconduct in the workplace can justify limited invasions in to employee privacy.

4. What about social media surveillance?

In some situations, there are laws that explicitly recognize and protect employee privacy in social media. On January 1, 2013, California *Labor Code* § 980 came into effect. Section 980 prohibits employers from requesting employee social-network usernames and passwords, or requesting employees to access social network data in the presence of the employer. Despite this protection, the law generally does not prohibit employers from reviewing content that an employee accessed through work devices or networks. Employees may reasonably expect privacy with their internet and computer use under some conditions, but not so in the work context.

5. Guidelines for implementing a surveillance program

Given the above, employers can limit potential privacy claims by keeping two things in mind.

A. Determine whether a reasonable expectation of privacy exists

The first issue in an invasion of privacy dispute is whether there was a reasonable expectation of privacy. Is the form and manner of surveillance sufficiently related and limited to its purpose? Is the surveillance in a place where a person normally expects to be unobserved? Is it reasonable to expect activity unrelated to work to occur in the area? In the case of phone recording, is the line being recorded provided for personal convenience, or is it reserved for business purposes? Each of these factors can be important.

B. Give employees written notice.

Employers must have a policy that sets forth a purpose and interest served by any surveillance. As part of that, proper notice of that policy should always be provided. Notice can be provided with prominently displayed reminders or better yet, all employees should sign a written policy acknowledgment or consent waiver. While consent is not necessary to monitor employees in most work environments, it can be persuasive evidence that an employee had no reasonable expectation of privacy.

6. Conclusion

There are many legitimate reasons for an employer to monitor spaces at the workplace, in fact, the law might require the employer to do so in some situations. However, surveillance is a sensitive subject and employers have good reason to be cautious. As always, employers should consult competent legal counsel before implementing any workplace surveillance program.

Related People

Lonnie D. Giamela
Partner
213.330.4454
Email