

A solid yellow triangle pointing downwards, located to the left of the 'BLOGS' header.

## BLOGS

Archives;Employee Surveillance;Investigations & Training;Privacy & Information Security;Social Media & Technology;Workplace Policies

# Best Practices for Workplace Surveillance

Last week, this blog featured posts about the growth and reported benefits of workplace surveillance, as well as some of the legal risks that can arise from surveillance. Workplace surveillance can run the gamut from conducting targeted email searches to investigate potential misconduct by a particular employee to using complex software programs designed to detect theft, cyberloafing, or inappropriate internet usage by anyone in the workforce. As discussed in our previous posts, surveillance may create opportunities to decrease employee dishonesty and improve performance, but these potential benefits should be balanced against legal risks posed by the workplace surveillance.

As promised last week, this post focuses on some best practices and practical tips related to workplace surveillance. Regardless of the type of employee surveillance at issue, an employer should consider doing the following:

***Be Mindful of Your Company Culture:*** Apart from legal risks, surveillance can carry practical downsides that may, for some employers, outweigh the potential upsides of employee surveillance. Depending on the company's culture and the type of surveillance being used, surveillance can injure trust, relationships, and create negative morale. These days, most companies reserve the right to monitor employer provided technology and work emails, but installing advanced tracking devices or video cameras in the workplace is less common and might, for some employers, lead to an unacceptable level of negative fall-out. Before embarking on surveillance, each employer should determine the unique impact of surveillance on its workplace and whether the benefits of surveillance outweigh any downsides.

***Provide Notice of Potential Surveillance:*** If your company does decide to engage in surveillance, the company should notify employees in advance of any potential surveillance. This notice should be provided in writing, and the company should obtain a signed acknowledgement of receipt from each employee. In addition, if video surveillance is used, it is a good idea to post a notice of the video monitoring in monitored areas. Taking steps to be transparent can reduce employees negative reaction to surveillance by ensuring employees are aware of when and how they might be monitored and what is and is not private activity. Notice can also reduce legal risks, because the surveillance will seem more reasonable, and the employer will have arguments that employees consented to the surveillance.

***Be Mindful of Where You Place Surveillance Tools:*** If your company does decide to engage in surveillance, be mindful of where you place tracking or surveillance tools and check with legal counsel on any applicable federal, state or local laws. For example, some areas, such as restrooms or changing rooms, are so private that they should be off limits for surveillance. In addition, some activities, such as union meetings, are off limits and should not be subject to any surveillance.

***Technology Policy or User Agreement:*** Employers should establish and distribute a clear, lawful employee technology policy or enter into user technology agreements with employees. The policy or user agreement should set forth the permissible and impermissible uses of workplace technology and social media and should explain when employees technology usage may be monitored. The policy or user agreement might also include the following:

- A reminder that technology usage on company provided or reimbursed devices is not private and may be monitored by the company;
- A prohibition or limitation on the personal use of technology on company time;
- A prohibition on using employer-provided or reimbursed technology to engage in unlawful acts, such as harassment, defamation, or the like;
- The requirement that employees not use technology to disclose or improperly use the employers confidential information, trade secrets, or sensitive financial information;
- A prohibition or limitation on the use of technology by non-exempt employees outside of normal working hours to minimize working time for which such employees must be paid;
- A warning to employees that any endorsements of the company or its products or services must be truthful and disclose the employees affiliation with the company; and
- A requirement that employees agree to surrender company devices when employment ends and permit the company to remove any company-related data from an employees personal devices used for work.

*Conduct Narrowly Tailored Surveillance:* An employer should have good business justifications for any surveillance and should narrowly tailor its surveillance to its business purpose. More specifically, a company should:

- Only conduct surveillance for legitimate business purposes, such as to decrease employee dishonesty, to promote productivity, to prevent or respond to inappropriate technology usage, and/or to investigate misconduct;
- Surveillance should be limited to a reasonable time, scope, and subject;
- An employer should only gather the information necessary to accomplish the business purpose and should not gather extraneous, personal information about an employee;
- When an employer identifies employee information as personal or otherwise irrelevant, it should cease reviewing the information; and
- Surveillance should be conducted with the guidance of legal counsel and by trained individuals.