Articles + Publications | February 28, 2024

Less Is More When It Comes to Employee Monitoring

Labor & Employment Workforce Watch

WRITTEN BY

Kathleen Grossman

RELATED OFFICES

Houston

With the increase in remote work, employers' concerns over the security of proprietary company information and employee productivity have increased their reliance on technologies to manage and monitor employees.

Many employers have long tracked employees both in and out of the workplace by utilizing an abundance of sophisticated tools to monitor employees' activities and productivity, including at home or anywhere an employee may be located with a device used for company business. Digital surveillance technologies can review employees' keystrokes, mouse activity, idle time, and time spent working in different applications or on different activities within company systems. These tools can monitor employee emails and browser activities, and can even record conversations between and among employees using on-site video surveillance, GPS tracking and cameras in company vehicles.

There is no doubt that these technologies can be valuable tools for employers. They can provide additional security, reduce liability through early detection of unlawful or inappropriate conduct, streamline the investigation of employee complaints, and allow employers to advance performance goals and manage performance deficiencies. But how should employers use the surveillance tools at their disposal? An analysis of the legal risks and practical considerations associated with employee monitoring may support a "less is more" approach.

In that regard, several federal and state laws would suggest that employers should exercise caution in their use of employee monitoring tools:

- **Wire Tap Laws:** The Electronic Communications Privacy Act of 1986 ("ECPA") broadly prohibits the interception of oral, wire, and electronic communications. To comply with the ECPA, employers must manifest a legitimate business purpose for intercepting employee communications or obtain advance employee consent. In this regard, it is important for employers to note that even though they may have legitimate business reasons for monitoring employee activity on company systems or otherwise relating to company business, and although employees may acknowledge and accept an employer's monitoring practices, those reasons and consents do not necessarily extend to third parties (e.g., an employee's friend or family member) who have not consented to such interception.
- **NLRA:** Overly broad surveillance programs run the risk of infringing on employees' rights under the National Labor Relations Act ("NLRA"). In October of 2022, the General Counsel for the National Labor Relations Board ("NLRB") issued a memorandum advocating for a formal framework under which employees' NLRA rights would be presumed violated if workplace surveillance and management practices, viewed as a whole, would "tend to interfere with or prevent a reasonable employee from engaging in activity protected by the [NLRA]" (i.e., protected union or concerted activity). To rebut this presumption, the memorandum suggested that employers would have to establish that their practices are narrowly tailored to address legitimate business

needs that cannot be satisfied by less intrusive means. In May of 2023, the White House Office of Science and Technology Policy echoed these concerns, announcing a public request for information "to learn more about the automated tools used by employers to surveil, monitor, evaluate, and manage workers." The White House announcement of the request for information cited potential concerns with employee monitoring, including, for example, that monitoring conversations could deter workers from exercising their rights to organize and collectively bargain with their employers and that constant tracking of employee performance could cause workers to move too quickly, posing safety and mental health risks.

- **HIPAA/ADA:** The more data and information collected through software monitoring, the more likely it is that an employer will intentionally or inadvertently gather employee financial, medical, or other sensitive personal information that may be protected by privacy laws. Consequently, it elevates an employer's responsibility to properly limit access to such information internally and externally and to protect such information from potential data breaches. Failure to do so could increase exposure for violations of laws like the Health Insurance Portability and Accountability Act ("HIPAA"), the Americans with Disabilities Act ("ADA"), and/or state data privacy and security laws.
- **State Privacy Laws:** Many states and localities have adopted laws similar to, or more comprehensive than, the ECPA as well as constitutional, statutory and common law protections applicable to the misuse of electronic communications. For example, the state constitutions of California, Florida, Louisiana, and South Carolina explicitly guarantee residents a right to privacy, and many states recognize common law claims for invasions of privacy. In at least some jurisdictions, when an employee accesses the employee's personal email account using an employer's computer, courts have found that the employee may have a reasonable expectation of privacy with respect to the communications sent or received from that account, particularly regarding sensitive, personal information such as exchanges between an employee and his or her attorney. Some states, like Connecticut, Delaware, and New York, require employers to provide employees with advance written notice of the employee monitoring methods they intend to use, obtain an acknowledgment of such notice, and post an applicable notice in a conspicuous location.

In sum, employers with overly broad employee monitoring practices risk running afoul of federal, state, and local laws governing employee monitoring, wiretapping, unfair labor practices, and invasions of privacy. Moreover, practically speaking, too much monitoring may lower employee morale and ultimately be counterproductive to increasing productivity and deterring rule-breaking. Indeed, a recent study by Harvard Business Review found that monitored employees were substantially more likely to break rules and work less efficiently than employees who were not monitored.

Keeping these risks in mind, we offer employers a few practical considerations:

- ensure that monitoring policies and procedures are narrowly tailored to the company's legitimate business purposes;
- develop and regularly assess and update employee monitoring policies to specify the types of monitoring that will occur and to explain the business purposes behind the monitoring to ensure transparency and to otherwise properly manage employees' expectations of privacy; and
- obtain employees' acknowledgment of, and consent to, employee surveillance policies upon hire and regularly thereafter when making changes to employee monitoring practices or policies.

RELATED INDUSTRIES + PRACTICES

- Labor + Employment