

Every Move You Make: When Monitoring Employees Gives Rise to Legal Risks

Skadden

09 / 21 / 22

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Anne E. Villanueva

Partner / Palo Alto
650.470.4596
anne.villanueva@skadden.com

Crystal D. Barnes

Associate / New York
212.735.2236
crystal.barnes@skadden.com

This article was published in the September 2022 issue of *Insights*.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

Key Points

- Employers monitor employees with various technologies, including instant messaging apps (that identify “active” or “away” status), phone, computer screen and video surveillance, GPS monitoring and even “smart” seat cushions that track health metrics.
- Though monitoring tools can be seen as a way to improve worker efficiency, accountability, productivity and safety, they can lead to legal claims and lower morale.
- Potential legal issues include invasion of privacy, unfair labor practice charges, discrimination, unpaid wages and overtime and workplace injuries.
- Employers monitoring employees should ensure compliance with evolving federal and state laws and review their employee handbooks and applicable written policies.

That employers monitor their employees to some degree is a given. What may come as a surprise is the extent and means of such tracking, often involving advanced technologies, especially during the COVID-19 pandemic. According to research by the management consulting firm Gartner, within the first month of the COVID-19 pandemic, 16% of companies put new tracking software on the laptops of their remote employees, and by July 2020, 26% of companies were utilizing surveillance software. As reported by *The Wall Street Journal*, a survey conducted in July 2022 by the research group International Data Corp. found that approximately 67.6% of North American employers with at least 500 employees utilize some form of employee monitoring software.

Common types of employee monitoring involve phone and video surveillance, GPS monitoring, and time-tracking via billable hours and work cards. In recent years, employers have turned to various other means of keeping tabs on employees, including instant messaging apps on platforms such as Microsoft Teams and Google, which identify each employee’s status as “active” or “away.” These apps allow administrators to track usage and metadata, including the time an employee signs on to a device, the number of messages they send and the number of phone calls or meetings they make, take or join. Some companies apply additional technologies to track the amount of time workers spend on the phone and composing emails. Employers have even used “smart” cushions installed at employees’ work stations, which can track health metrics for heart rate and posture to detect fatigue and identify the amount of time employees spend working and away from their desks.

Advanced modern employee monitoring tools have been nicknamed “tattleware” and “bossware” and even likened to “stalkerware.” They allow employers to engage in live monitoring of almost everything employees do at their work stations — including apps opened, websites visited, time spent on various online activities, music played, facial expressions, tone of voice and writing tone — and can even capture images of employees and their computer screens.

Though more research is needed, some companies view employee monitoring tools as a potential means of improving worker efficiency, accountability, productivity and safety. However, such systems can give rise to legal claims, lower employee morale and inaccurate recording of working time.

Every Move You Make: When Monitoring Employees Gives Rise to Legal Risks

Legislation Related to Employee Monitoring

Federal law. The Electronic Communications Privacy Act permits employers to monitor oral and electronic communications if they have a legitimate business purpose or obtain employee consent. The National Labor Relations Board has held that employers with a unionized workforce must obtain the applicable union's consent before conducting any video surveillance of unionized workers.

State laws. Only three states — Connecticut, Delaware and New York — have enacted legislation requiring employers to provide employees with notice of workplace monitoring. New York and Connecticut require a conspicuous posting of such notice.

California introduced in April 2022, but ultimately withdrew, legislation that would have regulated employee monitoring. The Workplace Technology Accountability Act (AB 1651) would have (i) required employers to notify employees in advance of any monitoring and explain how, when and why monitoring technology was being used on the job, (ii) prohibited employers from monitoring employees while off duty or using their personal devices, (iii) allowed employees to view and correct data about themselves, (iv) banned the use of facial recognition technology and (v) prohibited employers from using algorithms to decide if and when an employee is to be disciplined or fired.

State privacy laws. State laws that provide the following could also impact employee monitoring legislation in the future, even though they do not directly regulate employee monitoring:

- State constitutions containing an express right to privacy, including in California, Florida, Louisiana and South Carolina;
- Data privacy laws, such as the California Consumer Privacy Act and California Privacy Rights Act; and
- State wiretapping laws.

European data protection laws. The EU General Data Protection Regulation and U.K. General Data Protection Regulation already impose stricter requirements than in the U.S. on employers intending to monitor their employees, to ensure the surveillance is necessary, justified and proportionate. The laws require employers to (i) have a legal basis for monitoring, such as it being necessary for the employer's legitimate interests (where that interest is not overridden by the employees' rights and freedoms) or to comply with a legal obligation to which the employers are subject in the U.K. or the EU; (ii) notify employees of the tracking taking place and its purpose; and (iii) undertake data protection impact assessments (DPIAs) to identify the safeguards required and minimize the data protection risks involved. Legitimate interests is a flexible legal basis that has the potential to capture a range of monitoring purposes, though it will be most appropriate where employees would reasonably expect the monitoring and where it will have

minimal privacy impact. Untargeted monitoring, such as looking through an employee's browser history on the off-chance evidence of misuse will be identified, is unlikely to be justifiable.

Legal Risks

Although state legislation regarding employee monitoring is limited, employers should consider potential legal issues that may arise.

Invasion of privacy. A legal claim for intrusion upon seclusion could exist if monitoring software accesses an employee's webcam or internal microphone or records an employee in their home while working remotely and does so in a manner that would be highly offensive to a reasonable person. Similarly, a legal claim for public disclosure of private facts could exist if monitoring software reveals facts about an employee's personal life that are not publicly known and that the worker preferred to keep confidential (such as medical conditions, sexual orientation and/or financial status), resulting in their suffering, shame or humiliation.

Unfair labor practice charges. Because surveillance of employees engaged in protected concerted activity is legally prohibited under the National Labor Relations Act of 1935, an employer may be subject to an unfair labor practice charge if workplace monitoring unveils labor organizing efforts.

Employment discrimination. With the use of employee monitoring tools, including facial recognition software and smart cushions, employers may learn of an employee's legally protected characteristic, such as age, sex, race or disability, which in turn can give rise to a requirement not to discriminate against the individual on the basis of that characteristic. Employers may also learn about discrimination or harassment complaints through monitoring tools, resulting in a legal obligation to investigate the complaint and ensure that the employee is not retaliated against for making it.

Unpaid wages and overtime. Some monitoring software may not fully account for time employees spend working away from their computer, such as while reading, annotating hard copy documents or taking a phone call. In the case of a nonexempt employee, if these tasks result in their working more than 40 hours in a work week, the employee may be entitled to overtime pay. In 2021, a former employee sued for unpaid wages after the former employer required her to install employee monitoring software that audited her keystrokes and presence on her computer's webcam. The employer had not compensated the employee for any 10-minute time frame during which the audit team and software checked in on her and did not see her working. The employee alleged that she often performed tasks away from her computer for which she was not compensated. The parties settled the claim for an undisclosed amount.

Every Move You Make: When Monitoring Employees Gives Rise to Legal Risks

Workplace injuries. Employee surveillance software aimed at monitoring productivity can incidentally cause employees to be overworked and can lead to workplace injuries. In March 2022, Washington state’s Department of Labor and Industries fined a major e-commerce company \$60,000 for “knowingly putting workers at risk of injury” and identified a “direct connection” between employees’ joint and muscle disorders and the employer’s use of monitoring software, which forced workers to overexert themselves to meet quotas.

Takeaways

Employers need to consider whether and to what extent employee monitoring is necessary and track compliance with applicable federal and state laws, which are continuously evolving. Those engaged in monitoring must review their employee handbooks and applicable written policies to ensure they comply with relevant laws. For example, in New York and Connecticut, employers should have each employee sign an acknowledgment form stating they received notice of electronic monitoring, and post a monitoring notice in a conspicuous area in the workplace.

Counsel **Eve-Christie Vermynck** and associate **Alistair Ho** contributed to this article.