High-tech, high-risk: potential pitfalls from remote employee monitoring

By Melissa Z. Kelly, Esq., and Gregory P. Abrams, Esq., Tucker Ellis LLP

DECEMBER 6, 2022

There can be no dispute that the COVID-19 pandemic fundamentally altered the American workplace by sending employees home to work remotely. Even as the pandemic wanes, a large population of employees remains remote. Many of them will likely stay that way.

With this remote work comes challenges to employers as to how to monitor a workforce out of sight. Certain employers have responded by turning to technology to measure remote employee productivity, improve efficiency, and ensure accountability. Examples include instant messaging apps that reflect "active" or "away" statuses, software that counts keystrokes or scans an employee's face, and GPS monitoring. While employee monitoring can serve important purposes — including making remote work possible for those employees who prefer it — there are potential pitfalls that employers should consider.

The NLRB general counsel's expansive view of potential violations

A recent reminder of the risk that can accompany employee monitoring comes from Jennifer A. Abruzzo, General Counsel for the National Labor Relations Board in her Oct. 31, 2022, memo Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights, in which she described how an employer might run afoul of the National Labor Relations Act (NLRA).

Two sections of the NLRA form the background for Abruzzo's memo. One is Section 7, which, among other things, guarantees employees the right "to engage in concerted activities for the purpose of collective bargaining or other mutual aid and protection." (29 U.S.C. § 157). The other is Section 8, which prohibits employers from interfering with, restraining, or coercing employees in the exercise of their Section 7 rights. (29 U.S.C. § 158.). These protections have long been interpreted to apply equally to union and nonunion employees who engage in concerted activity.

Abruzzo's overarching position is that employee monitoring tools might interfere with the exercise of Section 7 rights by "impairing or negating employees' ability to engage in protected activity and keep that activity confidential from their employer, if they so choose." (Memo at 1). The Memo compares modern employee monitoring techniques to conduct long prohibited under Section 8, such as photographing employees picketing or hand billing, or surveilling employees known to be undertaking protected concerted activity. (*Id*. at 3-4).

To be sure, there is a significant difference between generally monitoring workers' productivity — which is not prohibited by the NLRA — and engaging in targeted monitoring of employees engaging in Section 7 activities. But Abruzzo paints employee monitoring with a broad brush, suggesting that any employee monitoring implicates Section 8.

With this remote work comes challenges to employers as to how to monitor a workforce out of sight. Certain employers have responded by turning to technology to measure remote employee productivity, improve efficiency, and ensure accountability.

It remains to be seen whether the NLRB will adopt the notion that employee monitoring techniques likely violate Section 8. The gist of this position is that an employer using employee monitoring practices must be able to establish that those practices are "narrowly tailored to address a legitimate business need — *i.e.,* that its need cannot be met through means less damaging to employee rights." (Memo at 8). And even where the employer succeeds in making that showing, the NLRB would require the employer to disclose information about its monitoring practices to its employees. (*Id*).

Abruzzo's proposal is not law yet, but it could be as soon as the NLRB is confronted with a case that allows it to consider what Abruzzo proposes. That possibility is a good enough reason for employers to consider how they would demonstrate the business justification for the monitoring practices utilized, and why it is not possible to serve that justification with less intrusive means. Further,

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

THOMSON REUTERS®

employers should consider whether and when it makes sense to disclose to employees their monitoring practices.

The General Counsel's memo is a reminder that, for all of the important purposes served by employee monitoring, those practices can create potential liability for employers beyond federal unfair labor practices.

Privacy laws

For example, employee monitoring can expose employers to liability under federal and state laws that govern electronic privacy and employee monitoring.

The most significant restrictions on electronic privacy derive from the federal Electronic Communications Privacy Act of 1986, (18 U.S.C. §§ 2510, *et seq.*), (ECPA), which generally prohibits employers from intentionally intercepting their employees' electronic communications, including emails and instant messages.

There are two exceptions to the ECPA that may apply in the employment context. One is the "business purpose exception," which permits an employer to intercept electronic communications when doing so is necessary for the performance of duties in the normal course of employment, or to protect the rights or property of the employer. (18 U.S.C. § 2511(2)(a)(i)).

Employee monitoring can expose employers to liability under federal and state laws that govern electronic privacy and employee monitoring.

The other is the "consent exception," which applies to allow the interception of electronic communications if the employer has the employee's consent. (18 U.S.C. § 2511(2)(d)). While explicit consent is not required, an employer that intends to rely on this exception must make it clear in advance that the employer will monitor employees' electronic communications.

Currently, at least three states — Connecticut, Delaware, and New York — have enacted laws that require employers to notify employees of electronic monitoring. (Conn. Gen. Stat. § 31-48d; Del. Code tit. 19, § 705; N.Y. Civ. Rights 52-c). The Connecticut and New York laws mandate that an employer post its notice "in a conspicuous place." (Conn. Gen. Stat. § 31-48d; N.Y. Civ. Rights 52-c). The Delaware law requires an employer that monitors telephone calls, emails, or internet usage either to provide employees daily notice of its monitoring practices, or to obtain a one-time written or electronic acknowledgment of those practices from its employees. (Del. Code tit. 19 § 705).

Other states may soon follow. In April 2022, California introduced legislation that would have significantly regulated employee monitoring, including by: (1) requiring notice of electronic monitoring; (2) prohibiting employee monitoring during off duty hours or while employees are using personal devices; and (3) prohibiting an employer from using algorithms to determine if or when an employee should be disciplined or fired. While the California legislation was withdrawn, it reflects the direction that some states might take on this issue.

Even in those states that have not enacted laws aimed at regulating employee monitoring, there may already be laws that impact an employer's ability to engage in that practice. These include state constitutions that contain an express right to privacy, state data privacy laws, state wiretapping laws, and state common law claims such as for invasion of privacy.

Wage and hour violations

Employers also should be cautious in relying upon employee monitoring practices to determine how much employees should be paid. The Fair Labor Standards Act, (29 U.S.C. §§ 201, *et seq.*), (FLSA), requires an employer to pay nonexempt hourly workers at least the federal minimum wage for all hours worked in a workweek. (*See* 29 U.S.C. §§ 206(a) and 207(a)). And most states have laws mandating compensation for all hours worked.

Yet some employee monitoring techniques — such as software that logs keystrokes, takes screenshots of an employee's computer, or photographs or videos an employee using a camera or computer webcam — may not capture all time spent "working," when considering, for one, time spent on work away from the computer or other monitoring device. Importantly, the possibility that monitoring software fails to capture all compensable time may not excuse an employer from its obligations under the FLSA, particularly if the employer knows or should know that the employee is working. (*See* 29 C.F.R. §§ 785.11-785.13).

Other potential risks

Employee monitoring practices can lead to other, perhaps less obvious issues.

At least one study has suggested, counterintuitively, that employees who know they are being monitored are more likely than other employees to take unapproved breaks, disregard instructions, and otherwise engage in the very behavior that employee monitoring is intended to prevent. "Monitoring Employees Makes Them More Likely to Break Rules," Harvard Business Review, June 27, 2022 (http://bit.ly/3gmHnru). The reasons for this phenomenon are not clear, but the concrete results are — sometimes, employee monitoring can contribute to the very evils it is intended to address.

Takeaways

None of this is to say that employee monitoring should go by the wayside. It can play an important role in protecting employers and allowing employees the flexibility of remote work. But employers should take stock of whether the benefits warrant the accompanying legal risks. If they do, employers should consider taking steps now to mitigate those risks.

Gregory P. Abrams is a regular contributing columnist on employment law for Reuters Legal News and Westlaw Today.

©2022 Thomson Reuters

About the authors

Melissa Z. Kelly (L) is an attorney in the Cleveland office of **Tucker Ellis LLP**. She regularly defends employers in a range of employment lawsuits, including wage and hour collective actions, employment discrimination, wrongful discharge, and employee benefits cases, and counsels employers on numerous issues, including employment agreements, personnel policies, and severance agreements. She can be reached at melissa.kelly@tuckerellis.com. **Gregory P. Abrams** (R) is a partner in the Chicago office of the firm. He defends companies in all types of employment litigation and counsels employers on matters involving, among others, compliance with COVID-19 related obligations, covenants not to compete, wage and hour laws, drug and alcohol testing, employee discipline and termination, and criminal background checks. He can be reached at gregory.abrams@tuckerellis.com.

This article was first published on Reuters Legal News and Westlaw Today on December 6, 2022.

© 2022 Thomson Reuters. This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit legalsolutions.thomsonreuters.com.