Viral TikTok Video Serves as a Reminder for Employers to Review Your Workplace Monitoring Policies

Insights
10.03.22

As a recent viral Tik-Tok video made clear, younger professionals are beginning to recognize that employers could be monitoring their workplace communications – which may mean that you will want to revisit your policies and practices. The now-deleted video that made the rounds on social media noted that companies can review their employees' "private" conversations through workplace messaging apps like Microsoft Teams — and the post reached 204,000 views before being taken down by the poster. While it's a common practice for employers to monitor electronic communications stored on company-issued technology, the proliferation of remote work and increased use of chat apps means that more workers are socializing with colleagues over company-owned electronic systems. But the ability to monitor employee communications comes with many questions and choices for employers: Do your employees realize you can monitor them? If not, do you need to update your policies? Are you taking steps to reserve your legal right to monitor employees? If so, how much monitoring should you actually be doing, and how will this impact workplace morale? You should consider all these questions — and more — when molding your workplace monitoring policies and practices. Here are a few points for employers to note.

Should You Notify Employees?

Under a patchwork of federal and state laws, an employer's right to monitor employees may be restricted depending on the nature of the surveillance and the laws in the relevant jurisdiction. Many workers expect employers to monitor their email communications on the company's network, and employers often disclosed this to employees through handbooks and other electronic communications policies.

However, when it comes to new and developing methods of communication — including video conferencing and chat apps — employees may not always assume employers are listening. And you may need to let them know. In fact, in some contexts, you need to obtain consent and provide specific notices before engaging in electronic monitoring.

At the federal level, the Electronic Communications Privacy Act (ECPA) prohibits the intentional interception of electronic communications, with the following two exceptions:

1. The **"business purpose" exception** allows an employer to monitor employee communications as a necessary incident to the rendition of services or to protect the rights or property of the

business.

2. The **"consent" exception** allows employers to monitor communications when the employee has given prior consent.

At the state level, employers are starting to see additional requirements. For example, a recently enacted New York law requires employers to give employees written notice, have them sign a written acknowledgment, and post the notice in a conspicuous place that can be seen by all employees who are subject to monitoring. You should check the laws in your jurisdiction to see if there are any specific rules to follow.

Consider the Impact on Morale

While adhering to legal requirements is important, employers should also consider the non-legal ramifications of monitoring employees — including the impact of active workplace surveillance on employee satisfaction.

Employers would also be wise to consider whether certain monitoring activities like geolocation monitoring — even where permitted and with notice and consent from employees — may capture more data than you would want or need. This could include information relating to potentially protected off-duty conduct or membership in a protected class that would otherwise be unavailable to you. This could potentially lead to a discrimination claim if you later discipline or terminate the employee and you have this information at your disposal. So, you will want to work with your legal counsel before setting such policies.

Conclusion

If you have questions regarding your workplace communications monitoring policy, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on our Privacy and Cyber Team. We will continue to monitor developments in this area, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information.

Service Focus

Counseling and Advice

Privacy and Cyber