Insights, News & Events

AVOIDING INVASION OF PRIVACY CLAIMS WHEN USING EMPLOYEE MONITORING SOFTWARE

Insights
Mar 30, 2021

Computer technology in the workplace is, in many ways, a double-edged sword. It allows for increased efficiency, instant communication, worldwide collaboration, vast data storage, and information security. These real, practical, and valuable benefits – among countless others – make computers ubiquitous in the modern workplace. Yet this same technology can also create issues for employers, including the risk that working hours will be spent watching YouTube videos and trolling Facebook – or worse, engaging in reckless or malicious behavior that jeopardizes the security of the business. To mitigate these risks, many employers turn to employee monitoring software. While this software can be an asset, it can also create serious privacy concerns if not implemented properly and used appropriately.

Service Focus

Privacy and Cyber

Types of Employee Monitoring Software

Employee monitoring software is a catch-all category of software that includes many different products from many different software developers. Broadly speaking, this software allows employers to monitor, document, and manage employees' actions through the digital devices used during the workday (e.g., computers, tablets, or cell phones). Some software offers relatively passive features that pose few privacy concerns, like a

website content filter. But not all software is the same, and some can be quite invasive. Some features allow employers to document and control every aspect of the device on which it is installed, such as a keystroke recorder, which can provide a literal "transcript" of everything the employee has done on their computer. Employers have other options as well, many of which, while potentially beneficial in certain instances, may raise privacy concerns if not used appropriately.

Potential Invasion of Privacy Claims

Although there is little case law specifically analyzing the use of employee monitoring software, employee privacy has been litigated in a variety of other contexts. From these cases it is safe to infer that the privacy concerns surrounding employee computer monitoring will vary depending on the nature of the employer, the type of software in place, and the underlying circumstances justifying its use in the first place. For example, a public entity using invasive products could create Fourth Amendment concerns that are not applicable to private employers.

For private employers, the legal concerns surrounding the use of employee monitoring software include, among other things, the potential that employees will assert claims for invasion of privacy and the interception of private communications. General common law principles applicable in most states provide at least two theories under which employee monitoring software could give rise to an invasion of privacy cause of action by an employee: (1) unreasonable intrusion upon the seclusion of another ("intrusion upon seclusion") and (2) unreasonable publicity given to another's private life.

Intrusion Upon Seclusion

A cause of action for the intrusion on seclusion requires a showing of an intentional intrusion on the solitude or seclusion of an employee that would be *highly* offensive to a reasonable person. If employees work remotely from their home, it is possible that

certain types of software could lead to an invasion of privacy claim premised on this legal theory. For example, if a certain kind of software allowed a company to remotely access components of the employee's computer like the webcam or internal microphone and that resulted in the surreptitious recording of the employee in their own home, an intrusion upon seclusion claim could be justifiable.

Publicity Of Private Life

A more likely scenario is one in which the use of employee monitoring software reveals facts about an employee's private life that the employee otherwise wished to maintain as confidential. This could give rise to an invasion of privacy claim if an employee shows a wrongful intrusion into their private activities that results in suffering, shame, or humiliation to a person of ordinary sensibilities. For example, a keystroke monitor could reveal private facts about an employee's medical conditions, financial status, or love life. Imagine an employee using a work computer to search for divorce attorneys during their lunch break. If that information became widely known "office gossip," the employee might attempt to bring an invasion of privacy cause of action premised on wrongful publicity given to the employee's private life.

Preventive Measures

The risks associated with invasion of privacy claims can be mitigated by implementing appropriate policies, providing the proper disclosures to employees, and using common sense.

- For instance, you should consider implementing written policies whereby employees are informed that work computers may not be used for personal business.
- Likewise, you should notify employees that all company computers are subject to monitoring. This is not only a good practice, but is required in some states where an employer plans to engage in

employee monitoring, such as Connecticut and Delaware, subject to limited exceptions.

- You should also use common sense when implementing employee monitoring software. If an employee works primarily from their home, the types of software and data captured or collected should be limited to those that will not allow an unreasonable intrusion or gather or store data for which there is no legitimate business need.

With these policies and practices in place, employees will have a more difficult time asserting a reasonable expectation to privacy in the use of company computers.

Conclusion

In sum, employee monitoring software can provide tangible benefits and increase productivity. When implemented appropriately, the risks relating to invasion of privacy claims associated with the use of such software can be mitigated to a large extent. As such, if your company is planning on using such software, you should review and update your policies as necessary, carefully consider the nature and scope of data collected to maximize the usefulness of the software and minimize any potential downside, and coordinate with your Fisher Phillips counsel before implementation.

We will continue to monitor any further developments in this area, so make sure you are subscribed to Fisher Phillips' alert system to gather the most up-to-date information. If you have questions, please contact your Fisher Phillips attorney or any attorney in our Privacy and Cyber Practice Group.