FOUR ETHICAL CONSIDERATIONS FOR USING EMPLOYEE MONITORING SOFTWARE ON REMOTE WORKERS

BY ERNIE SMITH **/ JUN 11, 2021**

(Feodora Chiosea/iStock/Getty Images Plus)

The use of employee monitoring software on remote employees might seem like a smart way to handle a difficult situation, but it could raise significant ethical issues—especially if a user's work computer is also their personal one.

Many employers are dealing with largely remote workforces for perhaps the first time in their histories. And that shift is creating a sudden interest in employee monitoring tools, which essentially allow employers to look at what an end user is doing.

But such tools have become controversial. Last year, the Electronic Frontier Foundation (EFF) put out a lengthy report discussing the issues.

"While aimed at helping employers, bossware puts workers' privacy and security at risk by logging every click and keystroke, covertly gathering information for lawsuits, and using other spying features that go far

beyond what is necessary and proportionate to manage a workforce," the foundation's Bennett Cyphers and Karen Gullo write.

EMPLOYEE MONITORING SOFTWARE CONSIDERATIONS

Given the growing use of monitoring tools, it might be worth discussing the ethics of requiring employees to install them. A few considerations:

How does it change the dynamic between leaders and employees? As an article from *The Conversation* notes, the use of such monitoring tools has the potential of backfiring significantly, as it could break a basic barrier of trust that drives a strong relationship. "The uncomfortable reality is that many employers feel entitled to monitor employee activity. If I'm paying their salaries, they argue, they should be doing my work. Their time is mine," the report, written by researchers from Victoria University of Wellington, states. "The problem with effectively intimidating employees into being productive is that it strongly suggests an organizational culture of mistrust—yet research shows that mistrust undermines productivity."

Have you properly researched your vendor? Can you trust them with worker data? The privacy issues aside, part of the problem with these tools is that they were often purchased in haste—an *AdAge* article described the acquisition of such software as "panic-buying." And while using such software is legal for employers to do, some of the tools, as EFF notes, may grab data more aggressively than you may need, even doing things like keylogging or accessing the webcam or microphone. If such tools are going to get used, it's imperative that steps be taken to understand what the tools can do, the vendor's background, and that you can feel comfortable with your employees using them.

Does it threaten employees' privacy off the clock, too? As EFF notes, many employees use their work laptop as their primary computer, meaning that surveillance software might not only be tracking their work lives, but their personal ones. Additionally, such products can be used to access information, however inadvertently, that most end users would consider private. "Most products take periodic screenshots, and few of them allow workers to choose which ones to share," Cyphers and Gullo write. "This means that sensitive medical, banking, or other personal information are captured alongside screenshots of work emails and social media." As *IT Security Central* notes, that could potentially create liabilities down the road.

Could the software be at odds with your association's mission? Many associations have missions that stand for things like protecting consumers, standing up for issues of privacy, acting ethically, and other similar issues. Such software could create quandaries if the software undermines the goals of the association in some way. It's worth researching where a balance may lie. As Reid Blackman put it in a *Harvard Business Review* article last May: "Given the risk of alienating employees coupled with the possibility of error and misapplication of these tools, it is quite likely that, for many, the juice just isn't worth the squeeze."

This article originally appeared on AssociationsNow.com. Reprinted with permission. Copyright ASAE: The Center for Association