Here are all the ways your boss can legally monitor you

Tatum, Hunter . The Washington Post (Online) , Washington, D.C.: WP Company LLC d/b/a The Washington Post. Aug 20, 2021.

FULL TEXT

There are a lot of things your employer doesn't know right now —like the future of remote work or when the coronavirus pandemic might end.

But your activity during the workday is less of a mystery.

The pandemic pushed many into work-from-home setups, and companies turned to employee data to keep tabs on their workforces. Your company can get access to almost everything you do electronically, and monitoring software makes that data easy to collect and analyze.

As some employees see work-from-home time extended because of the delta variant spreading across the world, reliance on employee tracking is staying steady at lockdown-level highs, say executives at monitoring software firms.

Elizabeth Harz, chief executive of Connecticut-based employee monitoring software provider InterGuard, said one of her clients came to her convinced that remote work would mean "economic ruin" for his company. That was until the client saw what InterGuard could do for his newly dispersed workforce, Harz said. The software tracks employees' productivity, down to how long it takes to respond to emails.

"They woke up in 2021 and said, 'Half of our employees don't even work where we are anymore,' " Harz said.

Your company may or may not be collecting data on your every move, but it certainly has the capability. The best way to know for sure is to ask, says Tom Kelly, CEO of consumer privacy firm IDX.

On work-issued computers, employers can gather data from your keyboard, like how often you're typing, and even your webcam, if it's in your employment agreement. On corporate Internet connections, your employer probably can see which sites you visit, and it can access the emails you send from company accounts. Those without office jobs get monitored, too. Amazon, for instance, has reportedly deployed tracking technology for both drivers and warehouse workers. (Amazon founder Jeff Bezos owns The Washington Post.)

Business is booming for companies that make software analyzing the data employees generate during the workday. These programs present reports to superiors on how often employees are typing, when they log off and on, and what social media sites they look at. When the pandemic began last spring, 30 percent of large employers —defined as companies with several thousand workers —adopted employee-tracking software for the first time, says Brian Kropp, chief of HR research for the research and advisory firm Gartner. Now, 60 percent use it in general, he said.

Some states —such as Delaware and Connecticut —require employers to provide written notice to workers if their electronic activity is being monitored. If your company gave notice, it probably came in one of the many forms you signed when you accepted the job, Kropp said. But if you get in trouble for something your employer catches you doing while monitoring you remotely, you probably don't have recourse. Almost all types of employee surveillance are entirely legal, according to Emory Roane, privacy counsel at the nonprofit organization Privacy Rights Clearinghouse.

"In general, you have very, very, very light protections, if any, for employee privacy," says Roane.

You may not be able to avoid tracking, but it's good to know what's private and what isn't. Here are five areas your employer might be watching:

1. Your email

If your company has an enterprise account with a provider such as Gmail or Outlook, authorized administrators can access every email you send and receive, Google and Microsoft said.

But Microsoft says it "does not agree with using technology to spy on people at work."

Companies that pay for monitoring tools such as Teramind can view the content, subject lines and attachments from both professional and personal inboxes, if the employee uses them on the same computer. Employers can put up guardrails around data collection from personal inboxes by telling the tool not to read inboxes accessed in Web browsers, for example, says Eli Sutton, Teramind's vice president of global operations.

Teramind can even scan for signs of disgruntled employees by flagging profanity in emails, as well as visits to job-search sites or negative posts on social media, Sutton said. Its website says it does this to prevent unhappy workers from stealing company data or trade secrets. But there's nothing in Teramind's policy preventing companies from disciplining employees who complain about a boss in an email to a co-worker —or from misusing the tool in any way.

The company has to use it responsibly, Sutton said, adding that Teramind can be abused just like anything else, and his company cannot implement safeguards without significantly hindering the software's capability.

2. Your focus and activity

Monitoring tools including Teramind, InterGuard, ActivTrak, Hubstaff and TimeCamp gather data from your keyboard and mouse to see when employees are "active" and when they've stopped clicking around.

Spend too long scrolling on social media and your activity could be flagged. Teramind's clients may set rules like "no more than five minutes of Facebook at a time" or "no more than 60 minutes of Facebook a day," Sutton said. If the Teramind "agent" is turned on, the tool can collect social media activity, including what you type, even if you're using your personal accounts from a work computer or remote network. Some companies create exceptions for certain apps and sites to avoid collecting data from employees' personal social media accounts.

Hubstaff can take intermittent screenshots of your desktop to see what you're up to. With Teramind, administrators can even access real-time recordings of employees' desktops. And London-based start-up Sneek takes workers' photos throughout the day and lets people activate video chats with the click of a button, according to its website.

3. Your browser

If you're on a company computer, any unencrypted traffic is most likely visible to your employer, privacy experts say. If you're on a personal device, traffic routed through a company network is visible, so your company could have access, Roane said. Be cautious about what you search while connected to the company's Internet, whether in the office or remotely. Your employer may not be able to see what you did on a website, but it can probably see that you accessed it.

4. Workplace collaboration tools

Say it with me: Do not bare your soul over Slack, Google Meet, Microsoft Teams or other office collaboration tools. In the case of Slack, whoever owns a Slack workspace —in this case, your employer —can apply to export messages from private conversations and direct messages, per the company's export policies. Slack says it will allow exports of private conversations only if the employer has a "right under applicable laws." But U.S. law allows companies to monitor employee communication that's part of the "normal course" of employment, which means, especially if you've signed an agreement outlining the employer's right to your communications, Slack is unlikely to deny the request.

Slack also reports your activity on the tool. Say you spent the day gazing at clouds but didn't request time off to do so. Slack might sell you out right here: [workspace].slack.com/stats. I searched my own name under the "members" tab and checked how many days I'd been active on Slack out of the past 30. (It was 23 days, compared with 27 for one of my colleagues. Now everyone knows I'm unlikely to check channels on weekends.)

Remote monitoring software can also record your video conferences. Teramind can capture audio and video from Zoom, Webex and Microsoft Teams, for example.

5. Your surroundings

Members of your household aren't necessarily immune to employee monitoring, even though they don't work at your company. Teramind can collect data from the microphone and speakers on your computer, which could record ambient noise from your home office, Sutton said.

Some companies have gone further: Multinational call center company Teleperformance drew criticism after pressuring employees in Colombia to sign a contract allowing the company to install cameras in their homes where they work, NBC News found. And specialized smartphone apps have been sending employees' locations to their managers in real time for years.

What if I don't like this at all?

If you don't want your company to digitally stand over your shoulder, there's not much you can do.

Some employers even use this data to make personnel decisions —like letting people go —and, while that might not be a good idea, they're in their rights to do so, Gartner's Kropp said. Recently, Russian company Xsolla said it used AI analytics to justify the layoff of 150 "unengaged" employees, according to reports.

One silver lining is that companies rarely look at this data at an individual level, Kropp said. The average manager, InterGuard's Harz said, isn't a creep.

"At the end of the day, most managers don't care if you're buying your kid's back-to-school lunchbox on Amazon," she said. "They're doing the same thing."

Monitoring tools also serve essential functions for companies. Occasionally, employees make cybersecurity mistakes or steal sensitive data, and automated systems help stop that. Employee data makes for more "personalized" experiences on workplace software the same way personal data helps websites serve more tailored offers, ads and features, Kropp said. And employees who feel like they're spending too much time on busywork can use InterGuard's time-tracking tools to gather hard evidence, Harz said.

If data collection also helps companies track productivity and encourages employees to stay focused, what's the harm?

Who's tracking what?

Different ways companies are using monitoring software to track employee productivity

Source: The companies

Surveillance makes employees lose trust and motivation, says Allen Holub, a software consultant who helps teams work together more effectively. If you think your employees are going to steal from you, that's a hiring problem, he said. And if you worry they're not going to do their jobs, then you've failed to create a system that incentivizes them —maybe because they're not paid a fair wage or their contributions at work don't feel meaningful.

According to IDX's Kelly, this all hinges on how employers treat monitoring software: Are they being transparent, sharing which metrics they're collecting and why, and treating employees well?

The more important question, though, is whether employees have any power in this back-and-forth, said Roane, the Privacy Rights Clearinghouse counsel. The line between "monitoring" and "surveillance" depends on whether individual employees can opt out of data collection.

"You can say no to the job," Roane said. "But you probably can't say no to that collection."

DETAILS

Subject:	Software; Web sites; Employers; Privacy; Employees; Social networks
Business indexing term:	Subject: Employers Employees Social networks

Location:	Connecticut United States--US
Publication title:	The Washington Post (Online); Washington, D.C.
Publication year:	2021
Publication date:	Aug 20, 2021
Section:	Technology
Publisher:	WP Company LLC d/b/a The Washington Post
Place of publication:	Washington, D.C.
Country of publication:	United States, Washington, D.C.
Publication subject:	General Interest Periodicals--United States
ISSN:	26419599
Source type:	Blogs, Podcasts, &Websites
Language of publication:	English
Document type:	News
ProQuest document ID:	2563070178
Document URL:	https://www.proquest.com/blogs-podcasts-websites/here-are-all-ways-your-boss-can-legally-monitor/docview/2563070178/se-2?accountid=44910
Copyright:	Copyright WP Company LLC d/b/a The Washington Post Aug 20, 2021
Last updated:	2021-08-21
Database:	U.S. Major Dailies