What Are Your Privacy Rights When You Work From Home?

by Lorelei Laird
Freelance writer

If you're working remotely and using equipment owned by your employer, it's worth thinking twice before switching between work tasks and personal tasks. Regardless of your company's privacy policy, employers have very broad rights to watch what their workers do.

Even when you work from home, employee privacy is limited, but there are things you can do to address your remote work privacy concerns and stay employed. Learn what they are.

What Privacy Rights Do Employees Have?

Employees have very few electronic privacy rights when working from home because there are generally very few employee rights to privacy at work. According to federal law and court cases, employers have the right to monitor your use of employer-provided equipment and computer networks, including what you type, your files, what web pages you visit, and your work email.

What privacy rights exist for email are for personal email—but not if you're using it on the employer's equipment or network. And for social media, even if you make a post on your own time and computer to a password-protected social media site, your employer may still legally penalize you if someone else forwards it.

That's part of why Professor Ifeoma Ajunwa of Cornell University's Industrial and Labor Relations school, who is also an attorney, co-wrote a law review article called "Limitless Worker Surveillance."

"Right now, employers have carte blanche in terms of what they can do regarding surveillance and worker monitoring," says Ajunwa, who is also associate faculty at Cornell Law School and Harvard's Berkman Klein Center.

Are There Any Exceptions to Worker Monitoring?

There are some exceptions. Generally, employers may not videotape employees in bathrooms or break rooms, although it's not clear how that would apply in an era of virtual meetings. Employers may not legally read messages related to genetic information or union organizing, and union contracts may prohibit monitoring altogether.

The National Conference of State Legislatures says Connecticut and Delaware state laws require employers to disclose that they're monitoring employee email, and at least 26 states forbid employers from demanding employees' social media passwords. Selective monitoring of employees based on race, gender, or certain other demographics could violate civil rights laws.

And it's not clear to what extent employers can monitor what workers do on computers or smartphones they own but are using for work. Enid Zhou of the Electronic Privacy Information Center, a D.C.-based nonprofit, says courts haven't yet ruled on that.

Do Workers Know What Employers Can Access?

Zhou says the simplest way to protect your digital privacy rights could be to find out what your employer is monitoring and avoid conducting any sensitive business that way.

"Having notice is the most important thing," says Zhou. "[As well as] knowing exactly who has access to your information and choosing platforms where your employer doesn't have that [access]."

Your employer may explain this in a company privacy policy or an employment contract, or you may have to ask. Unfortunately, Zhou says most employers are not obligated to answer truthfully—and withholding your consent could get you fired. There's also at least one case where a court found that an employer had a right to monitor workers' email, even though it expressly said it wouldn't, according to the worker rights nonprofit Workplace Fairness.

Should Workers Use Their Personal Equipment?

Edgar Ndjatou, executive director of Workplace Fairness, says the best way to protect your privacy is to conduct all personal business using equipment that you personally own, though Ajunwa notes that some employers may forbid this.

"Anytime you use an employer's hardware or email system or software ... in most instances, it can be subject to search or exposure," says Ndjatou, a former employee rights lawyer. "So, particularly when you're at home, [it's] even more important that you be mindful of the device you use."

Lewis Maltby, president of the National Workrights Institute, adds that you should not be logged on to any sort of employer network when you do that. Even if you're not actively using the connection, your employer can see what you're doing when your computer is part of the employer's network.

"There aren't many things in law that are simple. This one's pretty simple," says Maltby, author of *Can They Do That? Retaking Our Fundamental Rights in the Workplace*. "If you're using your personal computer for something, you're absolutely safe from intrusion by your boss unless you log onto your boss's network."

As telecommuting becomes the norm, Zhou says, employees may push back more against surveillance. But for now, she suggests staying well-informed

about your own workplace—and reminding employers that intrusive surveillance is bad for workplace morale.

"Implementing these types of tools increases the stress of your employees. And that decreases employee morale," she says. "So, it's not necessarily the best business model."

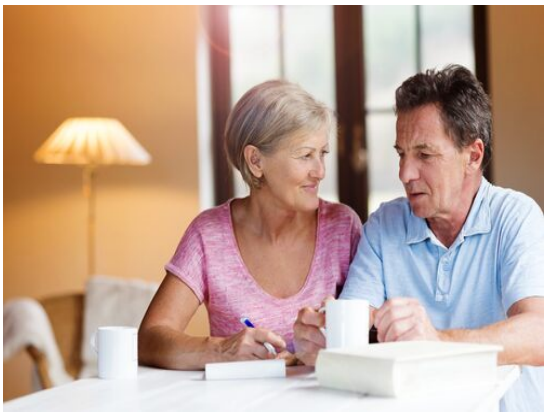
Have more questions about your Privacy Rights?

LEARN MORE

Related Articles

Estate Planning Checklist

Need help getting started with your estate plan? Use this checklist to remember the important parts of making an estate plan.
read more



Top 10 Duties of an Executor of a Will

The role of executor is usually assigned to a close member of the family. Given the nature of the assignment itself, the role can be quite a challenge—both mentally and emotionally. What follows is a list of executor's duties that hopefully will create the right expectations for the job.
read more