Bringing AI Out of the Shadows: How to Manage the Use of AI in Your Workplace

Labor & Employment Law Update

By Rebecca Bush and John Williams on January 28, 2025

Artificial intelligence (AI) is everywhere these days, including your workplace.

While there is no one-size-fits-all AI policy that will work for every company, here are our general thoughts about how employers can constructively manage the use of AI.

The "Shadow IT" Problem

Many companies struggle with "shadow IT"—the unauthorized information technology some employees use to do their work.

Your shadow IT problem could be the employee who conducts video meetings on Zoom because they like it better than the video application your IT department supports. It could also be the employee who saves sensitive company information in their personal Dropbox or Github accounts to work on it from home.

While shadow IT might be caused by a well-meaning employee's efforts to work more productively, it puts your confidential company information at a greater risk of compromise or theft.

AI Is a New Type of Shadow IT

The rollout of ChatGPT-4 and other human language-based AI products over the past two years has created a whole new world of shadow IT challenges for employers and their system administrators.

Your tech savvy employees are probably experimenting with the new AI tools to draft press releases, summarize documents, transcribe sales calls, write computer code, or build spreadsheets. At the same time, your IT vendors are quickly introducing new AI capabilities into their service offerings (e.g., Google's Gemini and Microsoft's Co-Pilot) without clearly explaining how these programs handle your company information.

What Can Employers Do About It?

While strictly prohibiting the use of AI tools in your workplace is always an option, doing so won't stop the AI hype in the marketplace and may send the wrong message to your high-performing employees.

We instead recommend a cautiously open-minded approach. As an employer, you should be willing to consider investing in technology that can demonstrably help your employees work smarter and faster. On the other hand, you and your employees have a shared responsibility to use AI tools in a way that protects your company's digital and physical assets.

There are two important pieces of this strategy:

> ***1. Regular, High-Quality Employee Training.*** AI should become a regular topic in your company's security awareness program. Your employees need to understand that an application like ChatGPT may use their input to "train" its models.
>
> Employees should never share confidential company information (including personal data about other employees or customers) with a chatbot unless there are controls in place to make sure the information doesn't end up in another company's "training set."
>
> ***2. Careful Vendor Monitoring.*** Because AI is a hot topic, IT vendors are rolling out new AI features in their products at a breakneck pace. Sometimes these new features are accompanied by amendments to their terms of service or privacy policy that allow the vendors to use your company information for model training (aka "scraping").
>
> Your security and systems administrators should carefully review how these vendors will use your company information and make sure that you do not give the vendor permission to use company data. For example, LinkedIn recently implemented data sharing for "generative AI improvement," leaving it to users to figure out how to opt out.

Conclusion

It may sound simple, but thinking before you chat and reading the fine print are two steps that will help you regain control over how AI is used in your workplace.