

Trade Secrets and Generative AI – Employers Should Remain Mindful of the Risks

Artificial Intelligence (AI) is transforming workflows for a growing number of professionals. According to a [Pew Research Center survey](#), approximately 1 in 5 workers in the United States now say they use AI in their work. In a [2026 report on the state of AI](#), Deloitte found that the number of workers with “sanctioned access to AI tools” had increased by 50 percent in just the past year. As employees become increasingly familiar with, and even reliant on, these tools, employers should remain mindful of the risks of using generative AI (Gen AI) in the workplace, including the inadvertent disclosure of their trade secrets.

The Requirement of Secrecy

The Uniform Trade Secrets Act (UTSA) defines a trade secret as a piece of information that derives value from not being generally known, and “is the subject of efforts that are reasonable under the circumstances to protect its secrecy.” Under the UTSA definition, a trade secret may be “a formula, pattern, compilation, program, device, method, technique, or process.” Materials like business plans, pricing strategies, and customer lists can be considered trade secrets as well.

Because the value of a trade secret depends on preventing its disclosure, the very act of inputting this information into a Gen AI tool can erode its protection.

The Risk of Disclosure

When an employee feeds information into a public Gen AI tool, they generally cannot control what happens to the information after that. The data in one user’s prompts may be used to further train or refine the model, and ultimately make its way into outputs for other users. ChatGPT’s Terms of Use acknowledge that user content may be used as training data.

In addition to being used as training data or voluntarily disclosed by the platforms, information shared with a Gen AI tool could also become discoverable in litigation. Dozens of lawsuits have been filed against Gen AI companies in recent years. One prominent example is the New York Times’ copyright infringement lawsuit against OpenAI and Microsoft, which has since been consolidated with a number of other cases into a multidistrict litigation in the U.S.

POSTED:

Mar 12, 2026

RELATED PRACTICES:

[Intellectual Property](#)

<https://www.reinhartlaw.com/practices/intellectual-property>

[Corporate Law](#)

<https://www.reinhartlaw.com/practices/corporate-law>

[Labor and Employment](#)

<https://www.reinhartlaw.com/practices/labor-and-employment>

RELATED SERVICES:

[Artificial Intelligence](#)

<https://www.reinhartlaw.com/services/artificial-intelligence>

RELATED PEOPLE:

[Elizabeth Elving](#)

<https://www.reinhartlaw.com/people/elizabeth-elving>



District Court for the Southern District of New York. In that case, the plaintiffs sought production of OpenAI's user chat logs in discovery. Although OpenAI objected on privacy grounds, the court found the information to be relevant and ordered that 20 million chat logs be produced in anonymized form. Situations like this will likely become more common as lawsuits involving AI companies progress, creating a new vulnerability for users who shared sensitive or proprietary information with those platforms.

When a user does not know what will happen to the information they put in their prompts, this can have serious consequences for trade secrets whose value derives from not being generally known.

Undermining Reasonable Efforts

Even if a trade secret is not shared more broadly, the very act of providing it to a Gen AI tool can threaten its protections. To establish that a particular piece of information is a trade secret, an owner will need to demonstrate that they used reasonable efforts to keep it secret, including by avoiding voluntary disclosure to third parties.

Entering trade secrets into Gen AI tools like ChatGPT may be considered equivalent to such a disclosure. In February 2026, the U.S. District Court for the Southern District of New York ruled in *United States v. Heppner* that the attorney-client privilege did not extend to documents a party prepared using Claude (Anthropic's Gen AI platform) and later shared with their attorney. In reaching this decision, the court noted that Anthropic's Privacy Policy allows for the sharing of users' personal data to certain third parties, and that users of AI "do not have substantial privacy interests" in their communications with public AI platforms.

Applying the same reasoning, a court may find that a company that inputs its trade secrets into a public Gen AI tool, particularly one that does not or cannot guarantee confidentiality, is effectively revealing the information to an outside party, and not making reasonable efforts to protect its secrecy.

Notable Incidents

The pitfalls of trade secrets and AI are not just hypothetical. In a widely reported 2023 incident, employees of Samsung uploaded source code into ChatGPT to optimize it and check for errors, leading to an inadvertent leak of trade secrets. Following this incident, Samsung implemented a policy banning the use of



ChatGPT by employees.

In the 2024 case *West Technology Group LLC et al. v. Sundstrom*, two companies brought an action against a former employee, alleging that he used the platform Otter to transcribe confidential meetings, and improperly retained access to the information after being terminated. The plaintiffs alleged that the former employee's use of the Gen AI tool amounted to Misappropriation of Trade Secrets under the Defend Trade Secrets Act.

As these incidents reflect, it has become common for employees to use AI to streamline workflows and make regular tasks more efficient. But when those tasks involve confidential or proprietary information, these everyday uses can carry significant risks.

Managing Risk

There are steps that companies can take to mitigate the risks of using Gen AI in the workplace, even as the technology, legal landscape, and public's understanding of it continue to evolve. Some companies have prohibited or restricted the use of certain tools by employees or on company devices altogether. Some may enter into agreements with vendors who provide closed systems, which do not retain user data for training. Others have developed their own internal AI applications.

Companies may also consider implementing or updating their policies to govern the use of AI tools specifically. Employees should be informed about what type of information cannot be shared, and what type of inputs are permitted. These guidelines can be integrated into onboarding and ongoing training to ensure widespread knowledge, as more employees begin to adopt these tools.

These efforts can help companies realize the benefits of AI in the workplace while minimizing associated risks. For more information or assistance with advising on or implementing these steps, please contact Elizabeth Elving or another member of Reinhart's Artificial Intelligence Team.

These materials provide general information which does not constitute legal or tax advice and should not be relied upon as such. Particular facts or future developments in the law may affect the topic(s) addressed within these materials. Always consult with a lawyer about your particular circumstances before acting on any information presented in these materials because it may not be applicable to you or your situation. Providing these materials to you does not create an attorney/client relationship. You should not provide confidential information to us until Reinhart agrees to represent you.