Articles + Publications | May 8, 2026

Is Your AI Tool Quietly Destroying Your Trade Secrets?

WRITTEN BY

Jeffrey Kramer | Alexandra Lancey

Artificial intelligence is everywhere now: in your contracts, your research workflows, your customer service queue. And if your company is using it without thinking carefully about trade secret exposure, you may be quietly dismantling critical protections your company has spent years building.

We've seen it happen, and so have the courts. In a widely reported 2023 incident[1], Samsung engineers uploaded proprietary source code into ChatGPT to optimize it and check for errors, inadvertently leaking trade secrets. Samsung responded by banning employee use of the tool entirely. More recently, in *West Technology Group v. Sundstrom* in the District of Connecticut, a company sued a former salesperson who had used an AI transcription tool to record confidential meetings, and then retained access to that information after his termination.[2] And in a January 2026 decision from the Northern District of California, a *pro se* plaintiff's Defend Trade Secrets Act (DTSA) claim was dismissed because she had developed her alleged trade secrets through ChatGPT, meaning she had voluntarily disclosed them to OpenAI and could not satisfy the requirement to maintain secrecy over the alleged trade secret.[3]

The last example is particularly instructive: The very act of using an AI tool to create something valuable can undermine your ability to protect it from public disclosure.

The Problem With Feeding AI Your Best Ideas

Obtaining trade secret protection for your business information under the DTSA requires two essential elements: (i) your information needs to be economically valuable because it is a secret, and (ii) you need to take reasonable measures to keep it a secret. Using AI tools the wrong way may prevent you from proving that second element.

When employees paste proprietary pricing models, customer data, internal strategies, or product formulas into a third-party AI platform, that information doesn't necessarily stay put. Depending on the vendor's data practices and terms and conditions, it may be used for model training, accessible across user environments, or stored in ways that create real exposure. If your confidential information ends up in someone else's AI output, your "reasonable measures" argument just got a lot harder to make. Without that, your trade secret claim goes with it.

And It Cuts Both Ways

Companies building or refining their own AI models face a different trade secret problem. If someone else's confidential information ended up in your training data — even inadvertently, through a vendor or third-party dataset — your model may have effectively absorbed it. That's a trade secret misappropriation claim waiting to happen, regardless of intent.

Courts are still working out exactly how trade secret doctrine applies to AI-generated outputs and training pipelines. The case law is young and evolving fast. That legal uncertainty cuts both ways, and it's exactly why getting ahead of these issues matters more than waiting to see how things shake out.

An Evolving Understanding of "Reasonable Measures"

Courts don't grade on a curve when assessing whether a company has taken reasonable measures to protect its trade secrets from disclosure. They look at what you and your employees did. And increasingly, that means looking at whether you addressed AI tools as a specific disclosure risk, not just whether you had a general confidentiality policy.

Practically speaking, and depending on the circumstances, that may mean AI-specific vendor due diligence, updated employee policies about what can and can't go into third-party AI systems, contractual protections around training data use, and access controls that keep your most sensitive information out of AI environments where you can't control what happens to it.

The Bottom Line (for Now)

Trade secret law was designed for a world where information stayed where you put it. But AI has changed that. Companies that don't update their protection strategies accordingly are taking on risk.

The good news: These risks are manageable with the right advice, early. The less good news: These risks are much tougher to mitigate after a dispute arises.

---

[1] https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/.

[2] *West Tech. Grp. v. Sundstrom,* Case No. 3:24-cv-00178 (D. Conn.).

[3] *Trinidad v. OpenAI*, Case No. 4:25-cv-06328 (N.D. Cal.).

RELATED INDUSTRIES + PRACTICES

- Artificial Intelligence
- Intellectual Property
- Labor + Employment
- Noncompete + Trade Secrets