

Publications

August 6, 2026 • Updates

Is Your AI Strategy Putting Your Trade Secrets at Risk?

Key Takeaways

- Employees' use of public generative AI platforms can expose proprietary information and may undermine trade secret protection when confidential business information is entered into tools that are not designed as confidential repositories. It can also create liability exposure if an employee enters a third-party's confidential information into non-confidential AI platforms.
- Losing confidentiality can limit a company's ability to claim trade secret protection, creating litigation risk even when an employee or counterparty otherwise complies with a nondisclosure agreement.
- Updating AI policies, employee training and confidentiality provisions can help companies restrict use of public AI tools while preserving approved workflows for enterprise AI solutions.

Generative artificial intelligence has become an indispensable business tool. Employees use platforms like ChatGPT and other publicly available AI models to draft documents, analyze data, troubleshoot technical issues, and streamline everyday work. While these tools can significantly improve productivity, they also present an often-overlooked legal risk: the potential loss of trade secret protection.

For companies that rely on proprietary information to maintain a competitive advantage, understanding this risk — and taking steps to mitigate it — is becoming increasingly important.

Why Public AI Can Jeopardize Trade Secret Protection

Under both federal and state trade secret laws, information qualifies as a trade secret only if it derives economic value from not being generally known and the owner takes reasonable measures to maintain its secrecy.

That second requirement is where public AI platforms create concern.

Unlike enterprise AI environments that contractually protect customer data, publicly available AI models generally are not intended to serve as confidential repositories for

Related People

- Jay E. Heidrick

Related Capabilities

- Intellectual Property
- Restrictive Covenants & Trade Secrets Litigation
- Artificial Intelligence & Machine Learning
- Intellectual Property Litigation

sensitive business information. Uploading source code, proprietary algorithms, customer lists, pricing strategies, product designs, or other confidential information into a public AI platform may undermine the argument that the company took reasonable steps to preserve secrecy. If confidentiality is lost, trade secret protection may be lost as well.

Why Your Existing NDA May Not Be Enough

For decades, companies have relied on nondisclosure agreements to preserve confidentiality when sharing sensitive information with employees, vendors, prospective business partners, and other third parties. Traditionally, those agreements have been sufficient because the recipient was contractually obligated not to disclose the information further.

Generative AI introduces a new category of risk that many existing confidentiality agreements were never designed to address.

Even if a recipient never intentionally discloses your confidential information to competitors or the public, uploading that information into a public AI model may itself compromise its confidential status. In other words, your counterparty could inadvertently jeopardize your trade secrets despite remaining otherwise compliant with the NDA.

As a result, companies should consider updating their confidentiality agreements to expressly prohibit the disclosure or uploading of confidential information to public or non-enterprise AI platforms without prior written authorization.

Likewise, companies should evaluate how they use information provided to them under and NDA. If a company imports confidential information it received under an NDA into a non-confidential AI platform, it may jeopardize the trade secret status of that information, and create litigation exposure. Care must be given not only to information a company provides under and NDA, but also information a company *receives* under an NDA to ensure it protects the confidential status.

A Litigation Scenario to Consider

Imagine a key employee who resigns and joins a competitor. She takes proprietary technical information with her, and your company files a trade secret misappropriation lawsuit.

During discovery, however, it becomes apparent that while employed, she regularly pasted portions of the same confidential information into a public AI chatbot to help draft reports or solve technical problems as part of her daily activities. The former employee may still have acted improperly by taking the confidential information, but the defendant argues that the company failed to take reasonable measures to preserve secrecy because employees routinely entered confidential information into public AI tools without meaningful restrictions or oversight.

Whether that argument ultimately succeeds will depend on the facts and the applicable law, but it is an argument few companies want to litigate.

Practical Steps Companies Should Take Now

As organizations continue integrating AI into everyday operations, governance should evolve alongside the technology. Companies should consider:

- Updating AI usage policies to prohibit employees from entering trade secrets or other highly confidential information into public AI platforms, including confidential

information received under an NDA. By contrast, enterprise AI platforms that provide contractual confidentiality protections and do not use customer data to train public models may present different legal considerations, although companies should still conduct appropriate diligence before use.

- Identifying and categorizing the company's trade secrets to help employees understand what information may not be shared with AI tools.
- Training employees on the distinction between approved enterprise AI solutions and publicly available AI platforms.
- Review and revise NDAs, vendor agreements, SaaS contracts, and other confidentiality provisions to prohibit counterparties from uploading your confidential information to non-approved AI services.

Generative AI offers tremendous opportunities, but it also requires companies to rethink longstanding approaches to protecting confidential information. Organizations that proactively update their policies, agreements, and employee training will be better positioned to preserve valuable trade secret rights while still realizing the benefits of AI. For questions about the issues discussed in this alert, contact your Polsinelli attorney.