Davis Polk

Three steps for safeguarding trade secrets in the world of generative AI

November 29, 2023 | Client Update | 4-minute read

Generative artificial intelligence (generative AI) tools pose new risks to a company's trade secrets. This client update describes three steps that companies should consider to protect their secrets in this new world.

Generative AI is here to stay—and with it, the risk that employees may deliberately or inadvertently compromise their companies' trade secrets. Recent studies have found that 10.8% of knowledge workers have tried using ChatGPT in the workplace and that sensitive data comprises up to 11% of what employees paste into the tool.[1] Even more troublingly, source code was the second?most common type of confidential data provided to ChatGPT in a six-week period earlier this year.[2]

While companies may prefer otherwise, employees will continue to try to use generative AI to assist in their work, and owners of trade-secret information must account for the special risks posed by those tools. It is axiomatic that the disclosure of information to a third party can compromise that information's status as a trade secret, and both federal and state laws require that trade-secret owners take reasonable measures to keep their information secret. However, the precautions that companies have historically taken are likely insufficient to protect against a new exfiltration vector that tempts workers at an unprecedented rate.

Accordingly, trade?secret owners should consider taking the following steps to safeguard their trade secrets from the use of generative AI by their employees.

- **Update employment agreements, trainings, and handbooks**: A standard part of a trade?secret owner's playbook is to train their employees at onboarding and throughout the course of employment on the handling of sensitive information. Trade-secret owners must now consider updating their agreements, trainings, handbooks, and related materials (e.g., confidentiality pledges or acknowledgments) with express guidance on the use of generative AI tools that employees are apt to use in the workplace. At a minimum, the materials should specify which generative AI tools are permitted or prohibited, the types of information that can safely be pasted into a particular generative AI tool (e.g., publicly available source code), and the process by which the employee should report inadvertent disclosure of sensitive data. Trade-secret owners should also consider requiring employees to complete periodic acknowledgments asking whether they have used any generative AI tools in their work recently, and to answer such questions during any exit interview.
- **Negotiate agreements with generative AI providers:** To the extent a company wishes to provide its employees with a particular generative AI tool for work purposes, it should carefully negotiate the terms of its agreement with the generative AI provider. Because any default terms are unlikely to provide sufficient protections for a company's information, trade-secret owners should choose generative AI providers who are willing to agree to additional protections. Specifically, the terms of use and non?disclosure agreements must make clear that any of the company's confidential information disclosed to the provider via the tool's prompts continues to belong solely to the company. The agreement should also restrict the provider from disclosing any confidential information it may receive from the company and prevent the provider from incorporating such information into its model, especially if that model may be used by other companies. Moreover, to the extent that the default terms attempt to limit or eliminate the provider's liability for confidentiality breaches or trade-secret misappropriation, trade-secret owners should seek to modify or omit such terms to ensure that the provider's incentives are aligned with the company's.

- **Conduct real-time tracking and retrospective audits:** Companies should step up their forensic-tracking and investigation capabilities, with an eye toward detecting potential exfiltration of company information by employees in real time and/or after the fact. Trade-secret owners should consider contracting with third?party providers and/or developing in-house tracking capabilities for the use of widely available services such as ChatGPT. For example, a company's IT or forensic personnel can use automated tools to monitor employees' activity on company-issued devices for visits to the websites of ChatGPT and other generative AI providers. Company personnel can also investigate particular employees by triangulating between their generative AI use and other contemporaneous activity, such as accessing or downloading sensitive files. With those capabilities in hand, companies can notify and/or reprimand offending employees as they engage in risky behavior, as well as target the employees who are most in need of remedial training.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Matthew J. Bacal
+1 212 450 4790
matthew.bacal@davispolk.com

David Lisson
+1 650 752 2013
david.lisson@davispolk.com

James Y. Park
+1 650 752 2044
james.park@davispolk.com

[1] Cyberhaven, *11% of data employees paste into ChatGPT is confidential*, https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt/ (last accessed Nov. 28, 2023).

[2] *Id.*; *see also* Cybernews, *Workers regularly post sensitive data into ChatGPT*, https://cybernews.com/security/workers-regularly-post-sensitive-data-into-chatgpt/ (last accessed Nov. 28, 2023).