Artificial Intelligence Update

May 2024

Protecting Trade Secrets in the Age of Generative AI

Whether they realize it or not, most companies probably own valuable trade secrets. When one thinks of "trade secrets," things like the recipe for Coca-Cola or Kentucky Fried Chicken or perhaps Google's algorithm might come to mind. But trade secrets are broader than these examples and can include things that most companies have, such as customer lists, manufacturing processes, and marketing strategies.

Protecting Trade Secrets

What makes a trade secret a trade secret? First and foremost, it must be a secret, and it must be commercially valuable because it is secret, attributes that the term "trade secret" itself suggests. In addition, the owner must make reasonable efforts to maintain a trade secret's secrecy, for example by using confidentiality agreements, passwords, or physical security, such as perimeter fencing or a security guard at a company's headquarters.

If a company's trade secret meets these requirements, the law extends certain protections, including the ability to sue people who unlawfully use or disclose it. But if the company publicly discloses the trade secret or fails to take reasonable measures to maintain its secrecy, the trade secret status is destroyed and these protections are lost.

Here is where generative artificial intelligence (AI) poses a potential risk. If a company does not properly control the use of generative AI by employees and contractors, its valuable trade secrets may be revealed, eliminating their trade secret status and the associated protections.

Generative AI's Threat to Trade Secrets

Generative AI includes chatbots such as OpenAI's ChatGPT. Released in November 2022, ChatGPT is free to use and already has around 180 million users. After signing up, a user can type a prompt asking ChatGPT to generate text. For instance, if a user enters "Write a poem," it will produce a poem.

ChatGPT does not guarantee confidentiality for information users share in prompts, and OpenAI may review the information that is entered, facts that OpenAI clearly discloses to its users. It is also possible that OpenAI could share information entered by a user with other users in response to their prompts.

Last year, it was reported that a large company had banned the use of ChatGPT after employees entered secret source code into it, asking the program to fix errors in the code. The employees also typed sensitive meeting notes into ChatGPT and asked it to summarize the notes.

The danger here is obvious: If employees enter trade secret information into ChatGPT, the trade secrets could become public, destroying their status. But even if the trade secrets are not released to the public, one could argue that trade secret protection is still lost because the owner failed to take reasonable efforts – such as exercising appropriate control over employees and contractors – to avoid disclosure.

Mitigating the Risk

Luckily, there are safeguards a company can use to protect its trade secrets against the potential threat posed by generative AI.

One obvious option is to simply ban employees and contractors from using generative AI, preventing them from entering trade secret information into such programs. This approach, however, poorly accounts for human behavior; if something is forbidden, it often becomes even more of a temptation.

Another possible solution is a more nuanced strategy that allows employees and contractors to use some form of generative AI, but with limitations to reduce risk. For instance, the company could adopt a policy that allows employees and contractors to use generative AI but prohibits entering sensitive or confidential information as part of any prompt. While this approach is simple and straightforward, it gives employees and contractors a great amount of discretion in deciding what information to input and still poses a substantial risk.

As a better alternative, the company could purchase, or perhaps even design and build, a generative AI application for internal use that maintains the confidentiality of all information entered into it. The company would need to adopt and implement policies that provide guidance on the appropriate use of the internal application and public programs, such as ChatGPT. The company would also need to train employees and contractors to ensure that they understand the difference between the internal application and public programs and the permitted uses of each.

FOR MORE INFORMATION

For more information, please contact:

Jesse L. Jenike-Godshalk
513.352.6702
Jesse.Jenike-Godshalk@ThompsonHine.com

Deborah S. Brenneman
513.352.6638
937.443.6600
Debbie.Brenneman@ThompsonHine.com