ALM | LAW.COM

New York Law Journal

COMMENTARY

Risks That Generative AI Poses To Trade Secret Protections

Tuesday, June 13, 2023

BY JOSHUA WEIGENSBERG
AND KATE GARBER

With the rapid improvement and deployment of generative artificial intelligence (AI) technology, many companies are grappling with balancing AI's benefits against its risks. Much of the discussion surrounding generative AI has focused on copyright and privacy concerns. For some companies, generative AI may pose another danger that deserves attention: losing potential trade secret protections over valuable business information, such as proprietary code.

Concerns over possible AI-related data leaks raise the spectre of damaging public disclosure of valuable business secrets. Perhaps less appreciated is that even without any public "leaks," the mere disclosure of a business secret to a generative AI program may, absent proper protections, undermine or even cancel out efforts to safeguard that information legally as a trade secret.

Trade Secret Law

Trade secret protections are among the most powerful ways to protect information providing a business advantage, such as proprietary code. Originally a common law doctrine, trade secret law is also now codified by the Defend Trade Secrets Act at the federal level and by most U.S. states' adoption of the Uniform Trade Secrets Act or a variation thereof. In cases where the trade secret is misappropriated, its owner can often go to court to obtain an injunction preventing further misuse of the trade secret as well as monetary remedies, which can be severe.

To avail itself of such protections, however, the owner must employ measures to maintain the secrecy of the trade secret. Several practices are common. These include (without limitation) contractual confidentiality obligations for those given access to the trade secret, establishing physical or technological barriers to unwanted access, and limiting the number of people with access.

It can be challenging to determine what measures are needed in any given situation. Trade secret law has developed across different

jurisdictions, and courts often engage in fact-intensive inquiries to determine the adequacy of protective measures. Contractual and technological protections are not always enough, standing alone, to insulate the trade secret owner.

For example, in one recent case, even where the plaintiff employed strict confidentiality language and password protection for its software, its promotion of the software at certain trade shows was deemed to create a triable issue as to whether the plaintiff could maintain a claim for trade secret misappropriation. *ExactLogix, Inc. v. JobProgress*, LLC, 508 F. Supp. 3d 254 (N.D. Ill. 2020). In another, a company lost trade secret protection for proprietary methods and techniques after it was discovered that not all of its manufacturers had expressly entered into confidentiality agreements. *Town & Country Linen Corp. v. Ingenious Designs LLC*, 556 F. Supp. 3d 222 (S.D.N.Y. 2021). Likewise, even employing passwords and encryption within a firm may not be enough if the firm's employees regularly leave their computers unprotected. *Cellular Accessories for Less, Inc. v. Trinitas LLC*, No. CV 12-06736 DDP (SHx), 2014 WL 4627090 (C.D. Cal. Sept. 16, 2014).

Concerns over possible AI-related data leaks raise the spectre of damaging public disclosure of valuable business secrets, while the mere disclosure of a business secret to a generative AI program may, absent proper protections, undermine or even cancel out efforts to safeguard that information legally as a trade secret.

Generative AI's rapid evolution and technological complexity further complicate the assessment of what protections are appropriate for companies that engage with generative AI, such as software companies that seek to use code-generating and code-editing AI. At the very least, employing both contractual and technological protections is a good start.

Contractual Protections And Generative AI

In efforts to enforce trade secret rights, prior disclosure by the company of the trade secret to third parties that were not under a confidentiality obligation may cut against a trade secret finding. *Ruckelshaus v. Monsanto Co*., 467 U.S. 986 (1984); *Sasqua Group, Inc. v. Courtney,* No. CV 10-528(ADS)(AKT), 2010 WL 3613855 (E.D.N.Y. Aug. 2, 2010).

In the absence of a negotiated agreement with the AI program's owner, the program's general license, terms of use, and privacy policies may set forth its contractual obligations, if any, regarding its users' data. While there are a variety of approaches to such obligations, some publicly available licenses and terms of use purport to give the AI company permission to employ its users' data as further training material to improve the AI itself, or even to disclose such data to third parties. In such cases, the lack of confidential treatment of users' data, and the loss of control over who may access the user's proprietary information and how such information may be used, could weigh against attempts to protect that information as a trade secret.

By way of example, if a software company were found to have allowed a code-generating AI pro-

gram access to the company's proprietary code, and the only contract between the two was the program's general terms of use, which would allow the program to train on the code or transmit it to third parties, then such terms may count against the company's ability to assert trade secret rights. Sophisticated attorneys defending clients against trade secret claims may well begin seeking information in discovery about the plaintiffs' prior use of generative AI to identify instances of disclosure without adequate protections.

Technological Barriers and Generative AI

Courts tasked with determining whether trade secret protections apply will often also look to what sorts of security measures were in place to maintain the secrecy of the trade secret. Commonly used technological barriers for trade secrets include passwords, firewalls, and security software.

The use of third-party generative AI tools complicates efforts to maintain adequate technological protections. Even where the trade secret owner has otherwise taken appropriate measures internally to limit access to its trade secret, the third-party AI tool's technological protections may also be important. This is true even though the program's users do not directly control its data protection measures. When evaluating the adequacy of technological protections, courts may search broadly for any security vulnerabilities that could expose the trade secret to third parties. Companies considering the use of generative AI tools in connection with any trade secret may therefore want to gain comfort first with the tools' technological measures to protect user data.

Beyond Trade Secret Considerations

Finally, it's important to note that in addition to the possible loss of legal protections, the business advantages associated with the trade secret can be lost in unique ways with generative AI.

Generative AI programs that train on one user's information may employ that training data when generating output for a second user, who may well be a competitor of the first user. Recently filed and closely watched lawsuits against AI coding and image-generating AI programs allege specific instances where generative AI has included in its output to users some identifiable portions of works from its training datasets. Even if not included in identifiable form as part of the program's output, the trade secret may nevertheless influence the output more subtly, possibly resulting in loss of the advantages that secret methods or techniques can provide.

These considerations underscore the wisdom of understanding how such programs work, employing the necessary protections, and guiding employees and contractors appropriately when using generative AI programs in connection with any valuable, proprietary business information.

JOSHUA WEIGENSBERG *is a partner in Pryor Cashman's Litigation and Media + Entertainment Groups, where he litigates copyright and trademark matters and other complex commercial disputes.* KATE GARBER *is an associate in Pryor Cashman's Litigation Group.*