Supplement to the Los Angeles and San Francisco

Daily Journal

OCTOBER 25, 2023

TOP TRADE SECRETS Lawyers 2023

AI AND TRADE SECRETS: A COMPLICATED FRIENDSHIP

By Eugene Y. Mar and Tom Pardini

Excitement has been growing for decades around the development, training, and use of generative AI, but this past year the excitement escalated into a frenzy. Everyone is considering how AI impacts their business.

This article examines the intersection of AI and trade secrets, including whether the widespread use and adoption of AI threatens trade secret protection and what trade secret protection is available to protect the use of and implementation of AI in a business. We address this intersection in three stages of an AI life cycle: the ingestion of data, training and deployment, and content generation.

I. Ingestion of trade secret data

In April 2023, news emerged that several Samsung employees pasted proprietary, confidential source code into a public version of ChatGPT to check for errors in the code. The news quickly served as a warning to companies that, if the use of generative AI is not closely regulated, it could easily destroy trade secret protection for sensitive information.

Under the California Uniform Trade Secrets Act (CUTSA), a claimant must demonstrate that its alleged trade secrets derive independent economic value from not being generally known to the public and that the claimant has taken reasonable measures to preserve the secrecy of the trade secrets. Cal. Civ. Code § 3426.1(d). The uploading of once-proprietary source code into a public generative AI tool calls into question whether a company has taken reasonable measures to maintain the secrecy of that trade secret. After all, the ingested source code could become part of a future generative AI response that could be sent to anyone.

However, if in this example, the Samsung engineers had pasted the source code into a proprietary generative AI tool hosted in a closed Samsung computer network, then the conclusion would be very different. In a closed, proprietary deployment, there is an instantiation of the AI tool that exists only on the company's servers, and the outputs are not transmitted to any servers outside of the company network. In that situation, the company would still be maintaining the secrecy of the source code and the code would not be generally known to the public.

This concern about protecting sensitive trade secret information has spurred many companies to implement AI use policies, in addition to technological limitations restricting the use and deployment of generative AI tools by its employees. For example, it was reported that, after this mishap, Samsung limited the upload capacity for any user using ChatGPT to 1024 bytes. Samsung was also reported to be considering the prospect of developing its own AI chatbot. Even for companies that are not in a position to develop

Eugene Y. Mar *is a partner at Farella Braun + Martel and chair of its Technology Industry Group.* **Tom Pardini** *is a senior associate in the Technology Idustry Group.*

or deploy their own AI tool, however, employee training sessions on the proper use of AI should be prioritized. This training should teach employees not to check for errors in their source code using a public version of an AI tool, even if the uploaded code incorporates a significant portion of open-source material. Companies should also ensure that any trade secret information is protected from discovery by scraping bots or LLMs (large language models) that are acquiring a large volume of online data to train their algorithms.

II. Training and deployment of the model

There are a variety of deployment models for generative AI. For a company that has developed its own generative AI algorithm, that algorithm can be protected as a trade secret. *See, e.g., Neural Magic, Inc. v. Meta Platforms, Inc.*, 2023 WL 2383172, at *17 (D. Mass. Mar. 6, 2023); *LivePerson, Inc. v. 24/7 Customer, Inc.*, 83 F. Supp. 3d 501, 514 (S.D.N.Y. 2015). If that AI tool is then distributed to the public or licensed to others, the company that developed the tool should specify in the license and/or terms of use that the licensee/user cannot reverse-engineer the tool in order to protect the trade secrets associated with the algorithm.

For a company that has licensed an AI generative tool for its own use and has been training it with its own data in a closed environment, there could be trade secret protection available for what information is being used to train the AI as well as the intermediate output. In that closed environment, the trade secret protection could extend to cover the specific prompts and problem formulations that are being used to train the AI tool. A best practice would be to limit the knowledge about the specific prompts and problem formulations to the employees who are involved with training the AI tool. Finally, the company should ensure that the license for the AI tool specifies that the training data, information about how the tool is being trained, and the intermediate outputs are the licensee's intellectual property.

III. Content generated by AI

The U.S. Patent Office and U.S. Copyright Office, along with the courts, have repeatedly found that content purely generated by AI is not eligible for patent or copyright protection in the United States because it is a statutory requirement that a human conceive of the invention or create the content. For content that is partially generated by AI and partially generated by a human, however, there remains significant uncertainty around whether that content is entitled to patent or copyright protection. In fact, at a September 27 session of the House Subcommittee on Courts, Intellectual Property, the head of the U.S. Copyright Office testified that copyrightability remains a "tough question" when looking at works partially generated by AI.

Conversely, the definitions of a "trade secret" under the Defend Trade Secrets Act or CUTSA do not impose a statutory requirement that the information must be human-generated. Thus, assuming the deployment and use of the AI tool is in a closed environment and the output is protected as a company secret, content that is purely generated by AI should be eligible for trade secret protection.