Articles + Publications | September 17, 2025

The Secret Formula: How Generative AI Could Change Reverse Engineering Forever

WRITTEN BY

Evan Gibbs | Grace M. Goodheart

As generative artificial intelligence (AI) programs become more commonplace and more powerful, they in turn become more useful — and present more risks. But what can a company do if a generative AI program recreates its most closely guarded trade secret?

Fortunately, judges are showing signs of readily adapting to this new landscape, and recent judicial decisions are shedding some light on how trade secrets can be protected in the age of AI. The few courts that have addressed this specific issue to date have largely been able to fit the issues into the framework provided by existing law.

When it comes to trade secrets, the applicable law is the federal Defend Trade Secrets Act (DTSA), along with similar state laws. (For simplicity's sake, we'll refer to analogous federal and state trade secret laws as "the DTSA.) Under the DTSA, a trade secret is generally a piece or compilation of information which has independent economic value because it is kept secret from others, particularly competitors. The DTSA protects trade secrets from unlawful misappropriation, which means using improper means to acquire a trade secret or using a trade secret with knowledge (or a reason to know) that it was improperly acquired.

Generally, reverse engineering — the process of lawfully purchasing a product, taking it apart, and figuring out how to reconstruct it — is not a violation of the DTSA. *See*18 U.S.C. § 1839 ([T]he term 'improper means' [under the DTSA]…does not include reverse engineering…). However, if that process is taken over by a generative AI program, directed by a person who uses targeted prompts to attempt to recreate a trade secret, the conduct may cross the line from reconstruction into misappropriation.

One recent case in the U.S. Court of Appeals for the Eleventh Circuit demonstrates that use of a computer program to process inhuman amounts of data can constitute an improper taking of trade secrets, even if the method used to gather the data is generally lawful. In *Compulife Software, Inc. v. Newman et al.*, the plaintiff's trade secret was a database of insurance quotes. The plaintiff's website was public and allowed individuals to pull insurance quotes from its database, but the plaintiff guarded the structure of the database and restricted access to the full database. The Eleventh Circuit found that the defendants used a "scraping" program (a type of lawful program used to gather information for targeted advertising, journalism, and other purposes) to carry out a targeted attack on the database. The scraping program successfully scraped millions of proprietary insurance quotes from the plaintiff's trade secret database. Although the defendants did not take the *entire* trade secret, they gained access to *enough* of the database to harm the plaintiff's business. The Eleventh Circuit determined that the defendants wrongfully acquired the plaintiff's trade secrets by using the "scraping" program to gather

inhuman amounts of data.

Another case currently pending in the U.S. District Court for the District of Massachusetts, *OpenEvidence, Inc. v. Pathway Medical, Inc. and Louis Mullie,* illustrates how a bad actor might use a generative AI program to reconstruct a competitor's proprietary technology and trade secrets. In that case, the target of the alleged attack was the generative AI program itself. The defendants allegedly used false credentials to log in to the plaintiff's AI platform, then used targeted prompts to bypass the restrictions placed on the generative AI and convince it to disclose the instructions and algorithms which formed the basis of its functions. In that way, the defendants allegedly sought to reconstruct the generative AI program itself and create their own, competitive program. Although the court has not yet substantively addressed the allegations, the case is an excellent example of how generative AI could be used to discover sensitive or trade secret information.

Extrapolating from these cases, it is easy to see how generative AI models may pose a risk to trade secrets. Generative AI models are typically trained on vast amounts of publicly available data, which may be gathered using processes similar to "scraping." Each time a user inputs a prompt or uploads a file for the program to analyze, additional data is added to the generative AI program for its later use. And although generative AI models typically create *new* outputs, rather than regurgitating the data *inputs*, a bad actor crafting the right prompts may be able to recreate some of that training data, including trade secrets.

These risks exist even if the generative AI model has never actually "seen" the underlying trade secret. Commentators believe that generative AI models may be able to find patterns in vast libraries of input data and identify correlations that humans may not readily see, allowing the generative AI program to reconstruct a competitor's product or trade secret simply by having greater access to information, and more processing power, than any human. In that case — and assuming that the human user of the AI was not acting improperly — it is possible that a court would find that the trade secret was lawfully reverse engineered by the generative AI. Another complicating factor in these types of analyses is that it is often difficult (or impossible) to ascertain what information was used to train a generative AI model, and that process itself can be a trade secret.

Although there are few cases yet addressing these issues, the DTSA is flexible enough to adapt to new technologies and new methods of misappropriation. We expect that as these cases come before the courts, the contours of the law will shift to account for these new challenges.

Companies with protectable trade secrets should continue to take reasonable precautions to safeguard those trade secrets from disclosure or use. In the age of generative AI, those safeguards should include instructing and training employees not to input trade secret or sensitive information or documents into a public AI tool, and may also require updates to nondisclosure or confidentiality agreements in order to prevent former employees from recreating trade secrets through targeted prompts to a generative AI program.

RELATED INDUSTRIES + PRACTICES

- Artificial Intelligence
- Labor + Employment