Untangling The Legal Complexities Of Trade Secrets And AI

By **Joshua Lerner and Nora Passamaneck** (March 26, 2024)

Joshua Lerner

Nora Passamaneck

With broad adoption of generative artificial intelligence tools, some commentators have suggested that trade secret law is the best means for protecting innovations. Looking to trade secret law to protect AI is facially appealing.

U.S. courts have rejected the notion that AI may be the sole inventor or creator of a patented invention or copyrighted work,[1] and aspects of generative AI may have difficulties overcoming the patent eligibility, written description, enablement and novelty hurdles to patentability.[2]

In comparison, the Defend Trade Secret Act does not require a human creator: It defines "owner" to mean "the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed."[3]

The DTSA also defines a "trade secret" broadly to include all forms and types of information — so long as it meets certain requirements discussed below.[4] Furthermore, trade secrets do not require upfront disclosure or filing fees.

But is trade secret law a one-size-fits-all solution for protecting a company's generative AI innovations? While trade secret protection potentially applies to all forms of information, that breadth of coverage may make identifying the information and any later misappropriation difficult.

Further, the protected information must also be subject to a company's "reasonable measures to keep such information secret," and "derive independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."[5]

These requirements also create barriers to protection and, at a minimum, raise questions about whether trade secret law is always the best tool for protecting these innovations.

Below, we explore the requirements for and identify issues unique to AI.

All Forms of Information

There is no doubt that trade secret law currently provides some benefits for protecting AI innovations, including the lack of a requirement for human involvement in the creation of the secret information.

But even this distinction requires further analysis.

While the U.S. District Court for the District of Columbia rejected copyright protection for AI in Thaler v. Perlmutter last August, that case was unique insofar as there was no human hand in the purported copyrighted work.[6] The court expressly left open the possibility that

the same result may not follow in a case in which there was more human involvement in the work.[7]

Thus, even the basic question of ownership may not tilt so far in favor of trade secret law in future cases.

Trade secret law is also appealing for protecting AI innovations because, as discussed above, the definition of a "trade secret" includes all forms of information. Every aspect of generative AI could qualify for trade secret protection if the other requirements are met.

For example, trade secret protection could extend to:

- The AI platform itself if internal to the company;
- The underlying algorithms and models;
- Training data;
- Input parameters; and
- The model outputs.

But this broad net of potential coverage may make identifying the trade secrets within AI difficult.

The challenge is that trade secret owners will ultimately need to identify their trade secrets with specificity, whether for purposes of taking reasonable measures or in litigation. Cases already have demonstrated the difficulty in describing AI-related trade secrets.

For example, in T2 Modus LLC v. Williams-Arowolo last September, the U.S. District Court for the Eastern District of Texas rejected that the plaintiff had sufficiently identified the alleged secrets at issue.

It explained that it is not enough to "merely describe the end results of or functions performed by the claimed trade secrets," or "merely describe the claimed trade secret in conclusory terms such as 'artificial intelligence,' 'machine learning,' or 'proprietary software' without including additional specific information."[8]

These cases show that courts will require plaintiffs to describe their alleged secrets with sufficient specificity to reveal actual trade secrets, not just categories of information that could be trade secrets.

But meeting these particular requirements may be uniquely difficult with generative AI. An employer may not know the specific inputs used without computer log information, training data may be difficult to define, and the algorithm at issue could require the submission of extremely sensitive source code.

Perhaps most importantly, models continue to learn, such that training data and outputs may change over time. We may well reach a point where the owners of AI tools do not know how or why a certain output is generated.

Reasonable Measures to Keep Such Information Secret

Trade secret owners must take reasonable measures to protect their trade secrets.

Reasonable measures typically include nondisclosure and confidentiality agreements,

employee trainings, security restrictions, and exit interviews.[9] What is reasonable will depend on the particular circumstances,[10] including the company's size, sophistication and industry.[11]

Given that both AI and companies' use of it is rapidly evolving, generic practices adopted by a company before its use of AI may be insufficient. Indeed, the reasonable measures inquiry focuses on the specific information at issue and the company's practices with respect to that information.

For example, the Judicial Council of California Civil Jury Instructions on reasonable measures, applied in at least one federal court to a DTSA claim, asks the jury to weigh whether:

- The information was marked with a confidential warning;
- Whether the company instructed its employees to treat the information as confidential;
- Whether the company restricted access to the information to persons who had a business reason to know the information;
- Whether the company restricted access to the information or kept the information in a secured area;
- Whether the company required employees or others with access to the information to sign confidentiality or nondisclosure agreements;
- Whether the company took any specific action to protect the information, or whether it relied on general measures taken to protect its business information or assets;
- The extent to which any general measures taken by the company would prevent the unauthorized disclosure of information; and
- Whether there were any other reasonable measures available to the company that it did not take.[12]

Given this fact-based inquiry focusing on the specific information at issue, a company's reliance on basic form confidentiality and assignment agreements may be insufficient.

These generic agreements may not provide clear — and reasonable — guidance regarding what aspects of AI a company believes are confidential and assigned to the company by virtue of employment.

Further, as a company's use of AI evolves, it may need to reevaluate what aspects of its AI use it considers confidential, and ensure that employees are informed through agreements and trainings.

Finally, a company should consider it and its employees' level of sophistication. For example, a sophisticated company developing its own internal AI platforms may need to take different and additional measures — e.g., restricting access, specific agreements directed to AI innovations — than those of a company that merely allows its employees to use AI as a time-saving measure.

In sum, companies looking to trade secret law to protect AI innovations will need to carefully review the measures they take to keep information secret and ensure it properly takes into account their use of AI.

"Derive Independent Economic Value ... From Not Being Generally Known"

To be a trade secret, the information must "derive independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means" by those who can obtain economic value from its use.[13]

Implicit in this definition is a requirement that the information must be secret — trade secret laws do "not offer protection against discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering, that is by starting with the known product and working backward to divine the process which aided in its development or manufacture."[14]

The "not generally known" and "not readily ascertainable" requirements raise questions as to what aspects of AI are valuable by virtue of being kept secret. To state the obvious, publicly disclosing outputs will necessarily prevent trade secret protection from applying to the outputs themselves.

More broadly, training data may be widely available to use and/or purchase, and there are many open-source AI tools.

If companies are using overlapping training sets and open-source code, it seems possible if not likely that many companies may end up mistakenly believing that they own unique and valuable information that is in fact widely known among other companies that used similar technology.

Eventually, these seeming secrets may cross the threshold to being generally known and/or reasonably ascertainable.

Conclusion

In sum, not all AI innovations will meet the trade secret requirements.

Companies will need to analyze very carefully how they are using AI, what aspects of their use are confidential — and can reasonably be kept confidential — and whether current policies and practices adequately take into account the unique aspects of AI.

Joshua Lerner and Nora Passamaneck are partners at WilmerHale.

[1] See Thaler v. Vidal, 43 F.4th 1207, 1212 (Fed. Cir. 2022), cert. denied, 143 S. Ct. 1783 (2023) ("[T]he Patent Act, when considered in its entirety, confirms that 'inventors' must be human beings."); Thaler v. Perlmutter, No. CV 22-1564 (BAH), 2023 WL 5333236, at *4

(D.D.C. Aug. 18, 2023) ("Human authorship is a bedrock requirement of copyright."); see also Thaler v. Comptroller-General of Patents, Designs and Trade Marks, Michaelmas Term, UKSC 49 (Dec. 20, 2023) (AI platform listed as inventor "is not a person, let alone a natural person and it did not devise any relevant invention").

[2] Shlomit Yanisky-Ravid, Regina Jin, Summoning A New Artificial Intelligence Patent Model: In the Age of Crisis, 2021 Mich. St. L. Rev. 811 (2021) (discussing potential limitations of applying patent law to AI).

[3] 18 U.S.C. § 1839(4).

[4] 18 U.S.C. § 1839(3).

[5] 18 U.S.C. § 1839(3).

[6] Thaler v. Perlmutter, No. CV 22-1564 (BAH), 2023 WL 5333236, *4 (D.D.C. Aug. 18, 2023).

[7] Id. at *6.

[8] T2 Modus, LLC v. Williams-Arowolo, No. 4:22-CV-00263, 2023 WL 6221429, at *5 (E.D. Tex. Sept. 25, 2023); see also, e.g., Yammine v. Toolbox for HR Spolka z Ograniczona Odpowiedzialnoscia Spolka Komandytowa, No. CV-21-00093-PHX-MTL, 2023 WL 6259412, at *6 (D. Ariz. Aug. 8, 2023) (rejecting plaintiff's trade secret identification "as pertaining to its development of various processes that automate the work of recruiters 'with enhancements in artificial intelligence,' which include 'patterns … to make enhanced prognostications that accurately identify when a tech professional may be interested in changing their job,'" as "merely identif[ying] the types of information that generally could qualify as a trade secret" and not the actual trade secrets at issue); Loop AI Labs Inc. v. Gatti, 195 F.Supp.3d 1107, 1114 (N.D. Cal. 2016) (rejecting as too conclusory alleged secret described as "[a]pplication of Plaintiff's technology to the analysis of big data generally owned by medium to large companies and governmental entities . . . with large volumes of structured and unstructured data from multiple sources and in need of quickly performing analyses of the data and obtain actionable inputs or results that can quickly be used for a variety of applications in various fields including customer relationship management, customer experience needs.").

[9] See, e.g., Neural Magic, Inc. v. Meta Platforms, Inc., 659 F. Supp. 3d 138, 172 (D. Mass. 2023); Better Holdco, Inc. v. Beeline Loans, Inc., 666 F. Supp. 3d 328, 385–86 (S.D.N.Y. 2023); Tri Tool, Inc. v. Hales, No. 22-CV-01515-DAD-KJN, 2023 WL 7130610, at *4 (E.D. Cal. Oct. 30, 2023).

[10] Neural Magic, Inc. v. Meta Platforms, Inc., No. CV 20-10444-DJC, 2020 WL 13819257, at *5 (D. Mass. 2023); Adler v. Loyd, 496 F. Supp. 3d 269, 281-83 (D.D.C. 2020).

[11] Softketeers, Inc. v. Regal W. Corp., No. 819CV00519JWHJDEX, 2023 WL 9227097, at *12 (C.D. Cal. Dec. 26, 2023); Arkeyo, LLC v. Cummins Allison Corp., 342 F. Supp. 3d 622, 629–30 (E.D. Pa. 2017).

[12] Judicial Council of California Civil Jury Instructions No. 4404 (2023); Softketeers, Inc. v. Regal W. Corp., No. 819CV00519JWHJDEX, 2023 WL 9227097, at *12 (C.D. Cal. Dec. 26, 2023).

[13] 18 U.S.C. § 1839(3)(B).

[14] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974).