The Pros And Cons Of Protecting AI As Trade Secrets

By **Jennifer Maisel and Andrew Stewart** (March 4, 2024)

Jennifer Maisel

Andrew Stewart

Trade secrets have become a de facto intellectual property right for securing valuable artificial intelligence information.

Despite regulatory trends toward greater transparency of AI models, federal policy acknowledges, and perhaps endorses, trade secret protection for AI information.

For example, the October executive order on AI recognizes that enterprises may undertake physical and cybersecurity measures to protect model weights — and requires reporting on those measures.[1]

The National Institute of Standards and Technology's December request for information seeks input on "information sharing best practices for generative AI, including for how to share with external parties for the purpose of AI red-teaming while protecting intellectual property, privacy, and security of an AI system."

More broadly, the Defend Trade Secrets Act, which took effect in 2016, further strengthened trade secret protection by empowering an owner of a trade secret to sue in federal court when its trade secrets have been misappropriated.

This article addresses why trade secrets have been a favored form of IP protection for valuable AI information, the unique hurdles in keeping AI information secret, and litigation trends to watch.

How Trade Secrets Fill a Gap Left by Patents and Copyrights for Protecting AI Information

Increased focus on trade secrets is driven in large part by recent decisions by the U.S. Copyright Office finding no copyright protection over solely machine-generated works,[2] the U.S. Patent and Trademark Office's "Inventorship Guidance for AI-Assisted Inventions" confirming the need for human inventorship,[3] and the shifting contours of patent eligibility following the U.S. Supreme Court's decision in Alice Corp. v. CLS Bank International in 2014.

Unlike copyrights and patents that protect only certain types of information, trade secret protection can attach to virtually any kind of information so long as that information derives independent value from not being generally known and is the subject of reasonable efforts to maintain its secrecy.

Indeed, trade secret protection can attach to information that has historically not been entitled to copyright or patent protection, such as purely mathematical concepts or data used for training AI systems.

Accordingly, developers and implementers may maintain a panoply of trade secrets that relate uniquely to AI technology, including model weights and parameters, training

datasets, and training processes and rules.

Similarly, implementers and users of AI technology may maintain certain AI inference and output as trade secrets that may not otherwise qualify for patent or copyright protection due to a respective lack of a human inventor or author.

As will be detailed below, however, there are unique hurdles to overcome in order to maintain AI information as a trade secret.

AI Technology Poses Unique Hurdles to Maintaining AI Information as a Trade Secret

Trade secret protection generally does not attach to information that can be reverse-engineered through proper channels, such as through inspection of a lawfully obtained product.

Enterprises must also take sufficient, i.e., "reasonable," measures to protect their trade secrets. Moreover, trade secret protection does not prevent others from independently coming up with and using the same information.

In some respects, AI technology raises many of the same issues as traditional software programs and services when it comes to implementing reasonable technological measures to protect proprietary information. For example, enterprises will want to ensure they have agreements in place with any third-party vendors with sufficient data security protections and restrictions on access and use of proprietary information.

Much like other software, an AI computer system hosted locally — e.g., on-site and within an enterprise's digital ecosystem — may offer greater security protection as compared to a system hosted on a third-party server that must be accessed over a network.

But AI technology poses unique data protection and security risks that are not necessarily present in traditional software solutions. These unique risks include, for example:

- Lack of traditional data protection mechanisms for AI models, such as encryption and access controls;
- Specific training samples may be identified from model output due to model memorization, inference attacks, inversion attacks and other vulnerabilities;
- Model and system behavior evolve over time as new information is learned or as the model drifts;
- Proprietary knowledge learned from one machine learning task may be reused for other tasks, such as through transfer learning;
- Ground truth data may be faulty, incomplete, biased or poisoned, leading to undesirable or unpredictable model inference;
- Model inference may not be confidential if other parties are able to independently obtain the same or similar inference from the model; and
- The threat landscape is rapidly evolving due to the opacity and complexity of AI models.

The unique security risks of AI technology will lead to novel interpretations as to what it means to misappropriate AI information through improper means, or what measures are reasonable under the circumstances to protect trade secret information.

Critically, trade secret protection over model parameters or training samples may be forever lost if new threat models emerge that make it possible to reverse engineer such information. Sensitive inferences may also leak if appropriate access controls are not in place to ensure that only authorized individuals are able to engage with an AI system or with sensitive datasets.

Use Caution With Departing Employees

Over the past decade, trade secret litigation peaked in 2017, following the passage of the Defend Trade Secrets Act.

Insider threats are a common theme in trade secret misappropriation cases, such as where a former employee who once had authorized access to a trade secret later misappropriates that information when she or he leaves the company.

The Waymo LLC v. Uber Technologies Inc. litigation in the U.S. District Court for the Northern District of California illustrates a common fact pattern involving former employees misappropriating trade secrets upon their departure.[4] In February 2017, Waymo, Google LLC's AI self-driving car subsidiary, filed a suit against Uber and Waymo's former employee.

Waymo alleged that the former employee had misappropriated trade secrets related to Waymo's self-driving light detection and ranging technology and used those secrets in founding his own self-driving car companies, Ottomotto and Otto Trucking, which were later acquired by Uber. The case settled a year later when Uber agreed to pay Waymo 0.34% of its equity, which was valued at approximately $245 million.[5]

Similar fact patterns are present in other trade secret misappropriation cases involving former employees of electric and self-driving car companies.[6]

In February 2015, Loop AI Labs Inc. filed suit against its former CEO and Almawave in the Northern District of California, in Loop AI Labs v. Gatti, alleging misappropriation of trade secrets.[7] The court ultimately imposed dismissing sanctions due to the plaintiff's attorney's obstructive behavior,[8] which included throwing coffee at opposing counsel during a deposition.[9]

Similarly, in March 2020, Neural Magic Inc. sued Meta Platforms Inc. and a former employee in Neural Magic v. Meta Platforms in the U.S. District Court for the District of Massachusetts, for misappropriation of trade secrets relating to optimizing sparse matrix multiplication operations for neural networks.[10] The parties settled shortly before trial.

With AI talent in hot demand, and with increasing freedom of movement of employees to competitors, we anticipate that trade secret disputes will continue to proliferate over AI information.

Key Takeaways

Although trade secrets offer many advantages to protecting AI information, enterprises may find it challenging to keep such information under wraps in view of the unique disclosure

risks posed by AI systems and the risk of insider threats.

In view of these unique risks, enterprises should carefully review and regularly update internal policies, agreements and other AI-governance mechanisms to ensure that appropriate measures are in place to protect valuable trade secret AI information.

Enterprises should also take advantage of multiple forms of IP protection where possible, particularly in view of uncertainty in how existing legal frameworks will adapt to a novel technological context.

Jennifer Maisel is a member and Andrew Stewart is an associate at Rothwell Figg Ernst & Manbeck PC.

[1] October 30, 2023, Executive Order § 4.2(i)(B).

[2] See, e.g., Review Board Decision on "A Recent Entrance to Paradise" (Feb. 14, 2022), available at https://www.copyright.gov/rulings-filings/review-board/docs/a-recent-entrance-to-paradise.pdf; Registration Decision on "Zarya of the Dawn" (Feb. 21, 2023), available at https://www.copyright.gov/docs/zarya-of-the-dawn.pdf; and Review Board Decision on "Theatre D'opera Spatial" (Sept. 5, 2023), available at https://www.copyright.gov/rulings-filings/review-board/docs/Theatre-Dopera-Spatial.pdf.

[3] Available at https://www.federalregister.gov/documents/2024/02/13/2024-02623/inventorship-guidance-for-ai-assisted-inventions

[4] Waymo LLC v. Uber Techs. Inc., No. C 17-00939 WHA, 2017 WL 2123560 (N.D. Cal. May 15, 2017)

[5] https://jolt.law.harvard.edu/digest/waymo-v-uber-surprise-settlement-five-days-into-trial

[6] Faraday&Future Inc. v. Evelozcity Inc., No. CV 18-737-DMG (RAOX), 2018 WL 11346536 (C.D. Cal. Aug. 9, 2018); WeRide Corp. v. Kun Huang, No. 5:18-CV-07233-EJD, 2020 WL 1967209 (N.D. Cal. Apr. 24, 2020).

[7] Loop AI Labs Inc. v. Gatti, No. 15-CV-00798-HSG, 2017 WL 934599 (N.D. Cal. Mar. 9, 2017), aff'd,742 F. App'x 286 (9th Cir. 2018)

[8] Id.

[9] Loop AI Labs Inc. v. Gatti, No. 15-CV-00798-HSG(DMR), 2017 WL 386344 (N.D. Cal. Jan. 27, 2017),order amended and superseded sub nom. Loop AI Labs Inc. v. Gatti, No. 15CV00798HSGDMR, 2017 WL 1436099 (N.D. Cal. Apr. 24, 2017)

[10] Neural Magic Inc. v. Meta Platforms Inc., 659 F. Supp. 3d 138, 182 (D. Mass. 2023).