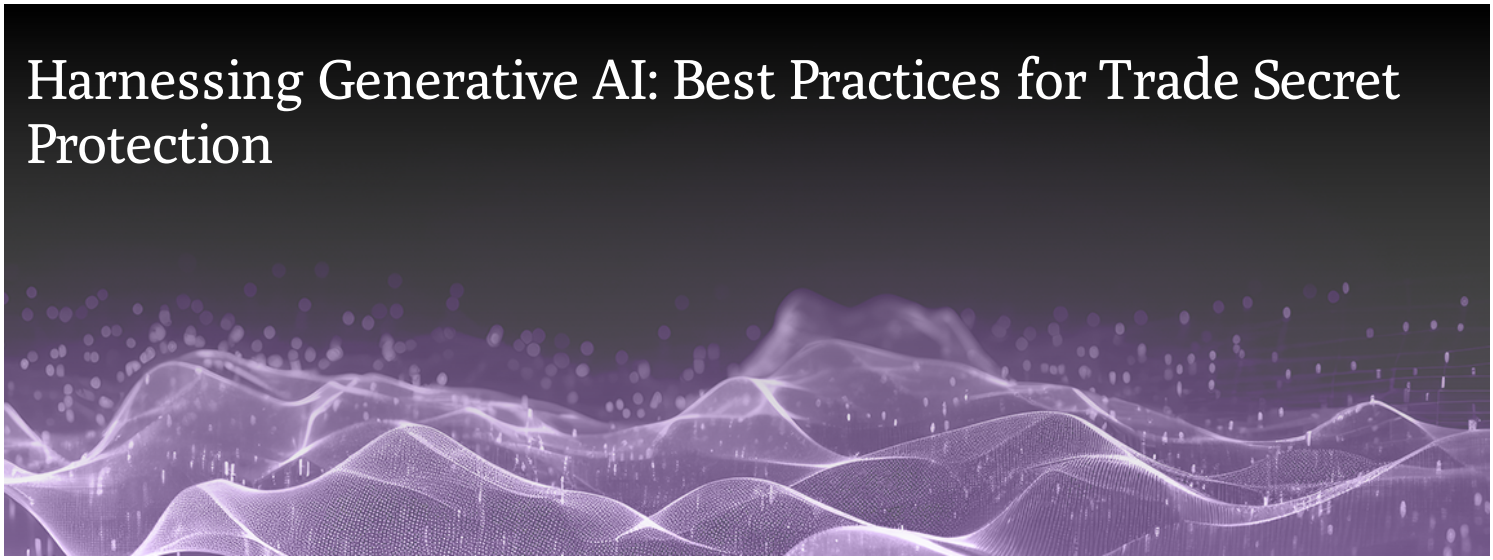
WINSTON & STRAWN LLP

CLIENT ALERT

Harnessing Generative AI: Best Practices for Trade Secret Protection



JUNE 26, 2024

WHAT IS A TRADE SECRET?

A trade secret is commonly understood to be a secret formula, such as the recipe to Diet Coke or Chick-fil-A sauce. However, trade secrets encompass a wide variety of intellectual property assets that most companies own, including customer lists, manufacturing processes, and marketing strategies. The Uniform Trade Secrets Act (the UTSA) defines "trade secret" as "information, including a formula, pattern, compilation, program, device, method, technique, or process that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[1] Trade secrets thus encompass many invaluable assets for businesses of all sizes, and adequate protection is paramount.

Unlike other forms of intellectual property, however, they are not formally registered and instead depend largely on confidentiality.[2] Protection of trade secrets relies heavily on the circumstances surrounding the development and disclosure of the trade secret in question. The Defend Trade Secrets Act (the "DTSA") protects "all forms and types of financial, business, scientific, technical, economic, or engineering information" where (1) the owner has taken reasonable measures to keep such information secret and (2) the information derives independent economic value, actual or potential, from not being generally known or readily ascertainable by others.[3] Thus, for a trade secret to be protected, it must be (1) secret; (2) have commercial value; and (3) be subject to reasonable steps by the rightful holder of the information to maintain secrecy. What constitutes "reasonable measures" is not defined by the DTSA; however, they have previously been identified to include: (i) whether the information was marked with a confidential warning; (ii) whether the company instructed its employees to treat the information as confidential; (iii) whether the company restricted access to the information; (iv) whether the company required employers to sign confidentiality or non-disclosure agreements; (v) whether the company took specific action to protect the information; and (vi) whether there were reasonable measures plausible that the company chose not to take.[4] Failure to take reasonable measures may result in the loss of status as a trade secret.

While historically trade secrets, like other forms of intellectual property, have been products of human invention, the rise in use of Generative AI in the workplace has brought forth legal questions on how to best extend trade secret protections where AI is involved in their creation.

WHAT IS GENERATIVE AI?

Generative AI tools can create new content, such as text, computer code, images, audio, sound, and video, in response to a user's prompt, often in the form of a short written description of the desired output. Generative AI tools are based on machine learning, trained using enormous amounts of data.[5] Generative AI tools are built on a system of inputs and outputs. First, the tool goes through a machine learning period whereby it is trained to generate predictive models and creative outputs through a large data set, often varied and diverse but tailored to the goal of the tool (i.e., customer service, generating scientific or marketing models, etc.). For in-house tools, this can be done with the company's own data; for larger tools such as ChatGPT, this is done with the creator's data set.[6] Once the tool has been trained, the individual user "inputs" a short prompt for the tool to synthesize and produce an "output." Inputs are often retained on the servers controlled by the company that supports the tool, for monitoring of the tool's performance and, in some cases, continued learning. The "outputs" are created by combining the machine learning during the training period with the inputs to produce an output.[7]

Even though Generative AI has only recently become widely available to the public, these tools are already routinely being used in the workplace. Recent studies have found that 56% of workers have tried using Generative AI in the workplace, with nearly 1 in 10 employing the technology on a daily basis.[8] Another study found that sensitive data, which may include the company's own competitively sensitive data or client-sensitive data, comprises up to 11% of what employees paste into the tool.[9] Even more troublingly, source code was the second-most common type of confidential data provided to ChatGPT in the six-week period studied.[10] However, AI tools can be programmed in various ways to avoid disclosing certain types of information.[11] This is both promising, in that protections are possible, and troubling, in that there are many ways that trade secrets may be implicated using Generative AI.

TRADE SECRET IMPLICATIONS WHEN USING GENERATIVE AI

Generative AI tools present several unique trade secret protection issues. Company trade secrets may come in at the machine learning stage as a data set used for training, or in the input stage if an employee user feeds the tool proprietary information to produce an output. As a Generative AI tool may store information after its immediate use,[12] using such tools may risk exposure of trade secrets used at inputs by users, if not properly licensed and trained. Moreover, both inputs and outputs, as well as the tool itself, may be cause for trade secret protection. When it comes to protecting a trade secret, what constitutes "reasonable efforts" is subject to debate when the use of Generative AI is involved; a simple confidentiality agreement may need to be reevaluated to include new guidance on how to interact with AI and ensure that employees are informed of the new risks of exposure relevant to Generative AI.

Importantly, tools such as ChatGPT do not guarantee confidentiality for the information users share in inputs, and OpenAI, the creator of ChatGPT, may review the information that is entered.[13] Inputs that are comprised of trade secrets may also be used to further train the tool, and thus be disclosed to users not affiliated with the company that owns the trade secrets. For example, if Employee A at Company 1 inputs one of Company 1's trade secrets into ChatGPT, the model may learn from that input. Then, if Employee B at Company 2 asks ChatGPT a question, it may generate an answer using a portion of its learning of Company 1's trade secret, risking exposure. Tools do not automatically assume that information is confidential or a trade secret.

Information captured by Generative AI tools, in many cases, cannot be deleted by the user and may be used by the application responsive to subsequent requests by a user, or reviewed by the AI's developer.[14] If an employee inputs a company's trade secret into an AI prompt, that trade secret could be at risk of losing protection. Additionally, providers of tools may monitor and store inputs to check for inappropriate use; in some cases, inputs may be reviewed by humans and thus trade secrets may be exposed.

CAN AI GENERATE TRADE SECRETS?

An ongoing legal question is whether AI can generate trade secrets itself. Trade secret law is primed for protection of trade secrets under the use of Generative AI tools.[15] **Trade secrets are distinguishable from copyrights and patents in that the inventor does not have to be human;**[16] **because trade secrets can be protectable without human involvement in their creation, innovation done with the assistance of Generative AI tools may be protected as a trade secret.** Further, the definition of "trade secret" includes many forms of information and is

uniquely broad; it could encompass a company's internal AI platform, the underlying training algorithms and models, input parameters, and outputs. If AI generates an output using inputs that are already trade secrets under the appropriate package of protections (for example, refining a marketing strategy or secret formula), then the output is most likely also a trade secret. However, if the AI-generated output is created using the training data, then it is likely not protected. Outputs may be covered if all elements of a trade secret are met,[17] and they are kept secret; the extent of coverage of outputs has not been tested and is an unanswered legal question.

BEST PRACTICES TO PROTECT TRADE SECRETS

A company interested in using such tools should create a holistic solution that encompasses both input and output-based solutions and focuses on confidentiality at all levels of development and use. While designing their AI policy, companies should keep in mind the "reasonable measures" standard applicable to protection of trade secrets.

There are many legitimate uses of Generative AI tools in the workplace, and thus an outright ban would be not only impractical but also competitively disadvantageous. Tools can be helpful to create personalized training programs and content, to analyze client-facing work product and point out potential holes, to predict market trends, manage internal systems like document management, automate and streamline business process to reduce processing costs and time to market, and to generate unique visual and written content.[18]

DRAFT AI POLICIES THAT LIMIT THE KIND OF TOOLS EMPLOYEES USE

Rather than an outright ban on Generative AI tools, businesses should draft AI policies that limit the kinds of tools that their employees use. Publicly available systems like ChatGPT are not currently equipped to distinguish between confidential and non-confidential inputs; however, a ban would require constant policing and monitoring to ensure that confidential information is not inputted. Instead, policies could allow employees to use Generative AI tools but prohibit entering sensitive information as part of a prompt, alongside increased trainings on what constitutes sensitive information and the risks of feeding it to an AI tool. In addition to writing policies and training employees, companies can also take steps to ensure that employees are not feeding key trade secrets to AI tools. For example, Samsung has limited the upload capacity for any user using ChatGPT to 1024 bytes, so that large files such as code cannot be inputted.[19] Companies may also consider blocking access to or download of certain tools on company-owned devices. However, this approach gives users a great deal of discretion in their use of the tool and still poses a substantial risk that a user may not understand the company policy, or simply access the tool on a private device to input sensitive information.

PURCHASE OR DEVELOP INTERNAL GENERATIVE AI APPLICATION

Companies should consider purchasing or developing their own internal Generative AI application that maintains the confidentiality of all information inputted and outputted by the tool. Such applications may store information on a private cloud unique to the company, eliminating the concern for shared data or data monitoring by the host. In a closed proprietary tool hosted in a closed company network, outputs remain on the company servers, and the trade secret would remain protected absent cyber threat. However, companies should be aware that such closed network models may limit the data the tool has been trained to use and the learning done over time as the company processes unique inputs, and that employees must still be trained to only use those proprietary tools in favor of others, or the trade secret may lose protection.

USE REASONABLE CONTRACTUAL STRATEGIES

In addition to monitoring of the tool, companies may turn to reasonable contractual strategies. Commonly used Confidentiality and Non-Disclosure Agreements (NDAs) are a great fit for Generative AI tools, if tweaked to appropriately capture the nuances of what can and cannot be inputted into Generative AI tools, and which circumstances various tools are allowed or prohibited. NDAs may include provisions that the company's confidential information disclosed to the provider via the tool's prompts continues to belong solely to the company, or that restrict the company's data tied to the tool to solely be stored on the private, company-only cloud rather than a cloud owned by the creator of the tool. Companies may also consider adding to NDAs and Confidentiality Agreements with their customers or clients a clause that gives consent for use of data within Generative AI tools, or an explanation of company policy with respect to their use by employees and contractors.

Another contractual tool to consider is an End User License Agreement (EULA) to place restrictions on what the AI provider can do with inputs to the system. A EULA for an individual user subscription may specify, for example, that inputs can be used to train the underlying model for third parties; however, a company-friendly enterprise license provision may provide that inputs cannot be used to train the underlying model, or that such trained models are used solely by the company. This is distinguishable from a company-developed tool in that the tool is owned by a third party; however, the specific version used by the company has its data held separately.

OFFER INCREASED TRAINING TO EMPLOYEES AND CONTRACTORS

Finally, all companies should provide increased training to their employees and contractors on what a trade secret is, how to protect one, and the risks and benefits of using AI tools. Courts have consistently found that companies have taken reasonable measures to protect their trade secrets simply by keeping updated employment agreements and policies.[20]

---

[1] The Uniform Trade Secrets Act, § 1.

[2] World Intellectual Property Organization, Frequently Asked Questions: Trade Secrets, https://www.wipo.int/tradesecrets/en/tradesecrets_faqs.html (last visited May 20, 2024) ("Contrary to patents, trade secrets are protected without registration, that is, trade secrets require no procedural formalities for their protection. A trade secret can be protected for an unlimited period of time, unless it is discovered or legally acquired by others and disclosed to the public.")

[3] *See* 18 U.S.C. §1839(3).

[4] 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).

[5] IBM, *What is Generative AI?* IBM Research Blog (Apr. 20, 2023), https://research.ibm.com/blog/what-is-generative-AI.

[6] Stephen Amell, *How to Train a Generative AI Model*, Medium (June 16, 2023), https://medium.com/@iamamellstephen/how-to-train-a-generative-ai-model-1ab605615acd; *supra* note 6.

[7] *Id.*

[8] The Conference Board, *Press Release: Majority of US Workers Are Already Using Generative AI Tools – But Company Policies Trail Behind* (Sept. 13, 2023), https://www.conference-board.org/press/us-workers-and-generative-ai.

[9] Cyberhaven, 11% of Data Employees Paste into ChatGPT is Confidential, https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt/ (last accessed Nov. 28, 2023).

[10] *Id.*

[11] Jeremy Elman, *AI and Trade Secrets: A Winning Combination*, IP Watchdog (Nov. 28, 2023), https://ipwatchdog.com/2023/11/28/ai-trade-secrets-winning-combination/id=170001/. ("Even today, some of the commercially available Gen AIs are implementing a proprietary mode where companies can designate some of the information output as confidential already, so "reasonable means" for keeping inputs and outputs confidential appears possible and qualifying as a trade secret. This would simply be an implementation detail in the way that the information is disclosed. Companies can then license these trade secrets to prevent the output from becoming public.").

[12] Samir Sampat, *Where Do Generative AI Models Source Their Data & Information?*, Smith AI (Sept. 20, 2023), https://smith.ai/blog/where-do-generative-ai-models-source-their-data-information.

[13] *Privacy Policy*, Open AI Blog (updated Nov. 14, 2023), https://openai.com/policies/privacy-policy/.

[14] *See, e.g., supra* note 9.

[15] *Supra* note 11.

[16] In test cases to date, all attempts to protect the intellectual property of a Gen AI under patent or copyright law have failed. The Patent Act requires a human inventor. *See Thaler v. Vidal*, 43 F.4th 1207, 1210 (Fed. Cir. 2022) ("Here, there is no ambiguity: the Patent Act requires that inventors must be natural persons; that is, human beings."); *Thaler v. Perlmutter*, 2023 WL 5333236, *4 (D.D.C. Aug. 18, 2023) ("Copyright has never stretched so far, however, as to protect works generated by new forms of technology operating absent any guiding human hand, as plaintiff urges here. Human authorship is a bedrock requirement of copyright.").

[17] For example, if the application can create the same output for multiple users, then it is not a trade secret because the output is not unique, nor is it secret.

[18] Taylor Karl, *Creative Collaboration: Generative AI's Integration in the Modern Workplace*, New Horizons (Apr. 29, 2024) https://www.newhorizons.com/resources/blog/generative-ai-in-the-workplace.

[19] Mark Gurman, *Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak,* Bloomberg News (Updated May 2, 2023), https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak.

[20] *See, e.g.*, *Philips North America LLC v. Hayes*, 2020 WL 5407796, *9 (D. Md. 2020) (plaintiff plausibly alleged reasonable measures to protect its trade secrets based on reference to "Employee Ethics and Intellectual Property Agreement"); *ExpertConnect, LLC v. Fowler*, 2019 WL 3004161, *4 (S.D.N.Y. 2019) (plaintiff plausibly alleged reasonable measures to protect its trade secrets based in part on reference to employee handbook); *Enterprise Leasing Co. v. Ehmke*, 197 Ariz. 144, 151, 3 P.2d 1064, 1071 (Ariz. Ct. App. 1999) (finding that a company took reasonable measures to protect its trade secrets by limiting disclosures, including a confidentiality provision in its employment agreements with high-level managers, and including a confidentiality provision in the employee policy handbook).

10+ Min Read

Authors

Diana Leiden

Helen Winters

Related Topics

Artificial Intelligence (AI) | Trade Secrets | Generative AI

Related Capabilities

Intellectual Property | Trade Secrets, Non Competes & Restrictive Covenants | Artificial Intelligence (AI) | Technology, Media & Telecommunications

Related Professionals

Diana Leiden

Helen Winters