Artificial Intelligence and Trade Secret Protection

A Mutually Beneficial Relationship If Proper Safeguards Are Met

By Corey A. Bauer

GenAI has the ability to catapult business productivity and efficiency to heights never before imaginable.

Artificial intelligence ("AI") may one day be dubbed the greatest inventor in history. And while DaVinci and Archimedes aren't watching anxiously from above quite yet, AI is already inventing new methods, computer code, procedures, etc., and companies are beginning to contemplate the concerns inherent in the use of generative AI ("GenAI") applications.

GenAI requires prompts from a user for it to engage in its functionality. It also requires that the GenAI application be "trained" on inputs from either a user, the internet, some other data source, or a combination of some or all of those, to respond to the user. This raises a couple of important questions: (1) what information are employees at a company providing to the GenAI application model to receive information from the GenAI application, and (2) what does the AI application do with the information that the employee provides, or that the AI application provides to the employee?

Arising from these questions are some important legal considerations. Such as, can a company protect IP that was generated by a GenAI application? And how does a company protect the confidential (or trade secret) information it already has from being exposed through a GenAI application?

Protecting Ideas Created by AI under Trade Secret Law

The law is clear that AI itself cannot patent an invention, no matter how novel the idea may be. According to the Patent Act "[t]he term 'inventor' means the *individual* or, if a joint invention, the *individuals* collectively who invented or discovered the subject matter of the invention." 35 U.S.C. § 100(f) (emphases added), and the U.S. Court of Appeals for the Federal Circuit ruled over twenty years ago that "only natural persons can be 'inventors'" under the statute. *Beech Aircraft Corp. v. EDO Corp.*, 990 F.2d 1237, 1248 (Fed. Cir. 1993). More recently, the Federal Circuit affirmed this axiomatic principle of patent law as applied directly to AI. *Thaler v. Vidal*, 43 F.4th 1207 (Fed. Cir. 2022). However, as of February 12, 2024, the U.S. Patent and Trademark Office ("USPTO") issued guidance on AI and patents, stating that a human could patent an idea generated by AI if a human made a "significant contribution" to that invention. See Patent and Trademark Office, Inventorship Guidance for AI-assisted Inventions, Docket No. PTO-P-2023-0043, February 12, 2024. This guidance has yet to be hashed out in the USPTO or the courts, but it is a large development. Nonetheless, a patent comes with disad-

The law is clear that AI itself cannot patent an invention, no matter how novel the idea may be.

Corey A. Bauer is a Partner at Houston Harbaugh, P.C. in Pittsburgh, Pennsylvania. He is a trusted litigator, trial lawyer, and counselor to businesses in intellectual property and commercial matters. Corey focuses his practice on issues relating to the protection of intellectual property in an era of rapid technological growth. He is a member of the DRI Intellectual Property Litigation Committee, Young Lawyers Steering Committee, and the ADTA.

vantages, such as national publication and a limited time of protection.

The Copyright Office has denied multiple applications for copyrighted works created by AI. *See* Copyright Review Board letter to Ryan Abbott, Esq. (February 14, 2022); *see* also U.S. COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 202.02(b) (2d ed. 1984) ("the Office will not register works produced by a machine or mere mechanical process" that operates "without any creative input or intervention from a human author" because, under the statute, "a work must be created by a human being"); *see also* U.S. Copyright Office, "Artificial Intelligence and Copyright," 59942 Federal Register, Vol. 88, No. 167 (August 30, 2023). Recently, at least one District Court has upheld this stance by the Copyright Office. *See Thaler v. Perlmutter*, No. CV 22-1564 (BAH), 2023 WL 5333236 (D.D.C. Aug. 18, 2023) (holding that the Copyright Office did not act arbitrarily or capriciously in denying an application for registration of AI-generated work).

Therefore, if one wants to protect an idea that is generated by AI, the most common solution is trade secret protection. Ideas generated by AI are indeed potentially protectable as trade secrets. This is true even if the information is not "novel." By the very nature of AI, the idea fed by the application to one user may later be fed to another user in the future if similar prompts are used. Fortunately, a trade secret does not need to be original information to receive protection, but it does have other required legal preconditions and caveats.

First, the idea has to fit within the parameters of how a trade secret is defined by federal and state law. The federal Defend Trade Secrets Act ("DTSA") defines a trade secret as:

> [A]ll forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electroni-

cally, graphically, photographically, or in writing if –

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives 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;

18 U.S.C. § 1839(3).

The Uniform Trade Secrets Act ("UTSA"), which has been adopted in some variation by nearly every U.S. state, defines a trade secret as:

[I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) 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

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Uniform Trade Secret Act § 1(4).

As you can see, the types of information that can potentially be covered by trade secret protection are wide-ranging. However, the requirements of independent economic value and reasonable measures and/or efforts to keep said information secret can quickly preclude information from being protectable under trade secret law. Indeed, this is why most information in the world is not deemed a trade secret, and why it is considered a high threshold to meet in court.

Federal Circuit Courts across the country have consistently held that the DTSA and state statutes aligned with the UTSA are substantially similar from a legal analysis standpoint. *See*, e.g., *Mallet & Co. v. Lacayo*, 16 F.4th 364, 381 n.19 (3d Cir. 2021). Even states that have not adopted the UTSA have been found to have similar analyses. *Town & Country Linen Corp. v. Ingenious Designs* LLC, No. 18-cv-5075 (LJL), 2021 WL 3727801, at *16 n.12 (S.D.N.Y. Aug. 23, 2021) (applying DTSA factors to New York common law trade secret). Thus, the following discussion will focus on the law derived from DTSA analyses.

Under the DTSA, a trade secret is *very* generally described as "information" that must (1) have actual or potential "independent economic value" as a result of its secrecy, and (2) have been the subject of "reasonable measures" to maintain its secrecy.

An oft-overlooked principle in DTSA law is that value untethered to value derived from secrecy does not show an alleged trade secret's independent economic value. Simply meaning, commercial value alone is not sufficient. *Synopsys, Inc v. Risk Based Sec.*, Inc., 70 F.4th 759, 772 (4th Cir. 2023); *see also* 18 U.S.C. § 1839(3)(B). As such, to have trade secret protection, information a company generates through an AI application must provide that company with economic value that would be destroyed by the disclosure or use of that information by others. Basic examples of this could be a compiled list of sales leads that a competitor could use to entice customers, or source code that could be reverse engineered.

The DTSA is silent on what constitutes "reasonable measures," but the body of case law makes clear that the key word is "reasonable." A company is not required to act as a police state overseeing its employees to ensure confidentiality. See, *Vendavo, Inc. v. Long*, 397 F. Supp. 3d 1115, 1136-37 (N.D. Ill. 2019). However, given that trade secrets may appear in a wide variety of "forms and types," § 1839(3), the nature of the purported trade secret information can dictate what is considered "reasonable." For example, certain AI applications may doom a purported trade secret generated by that application from the start. Depending on the terms of the end-user license agreement ("EULA") agreed to for the use of the AI platform, the idea generated may already be known to third parties by the very nature of how it was conceived. Many GenAI applications record and use both the prompts and the output for training the AI or other business purposes. Further, the EULA may give the company behind said application the rights to review, use, or even sell the information generated. It would almost certainly be deemed unreasonable to expect secrecy of information generated by an AI application that expressly provides none.

> **An oft-overlooked principle in DTSA law is that value untethered to value derived from secrecy does not show an alleged trade secret's independent economic value.**

Now, referring back to the aforementioned concern that GenAI may provide the same potential trade secret information to more than one person or company: let's assume that Company A has taken reasonable measures to maintain the secrecy of source code generated by an AI application that has independent economic value derived from that secrecy. Let's also assume that the company that owns that GenAI application requires that all users sign an EULA that retains no rights to the prompts or outputs. Nonetheless, a competitor, Company B, shows up and it becomes clear that Company B has the same source code as Company A, used it to create a competing program, and Company A is losing revenue as a result.

Under this hypothetical, if Company B received this information from the same GenAI application as Company A, there may be nothing Company A can do about it. "An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." § 1836(b)(1). The issue for Company A begins with the DTSA's definition of "misappropriation," which is set forth as follows:

(5) the term "misappropriation" means—

(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by *improper means*; or

(B) disclosure or use of a trade secret of another without express or implied consent by a person who—

(i) *used improper means* to acquire knowledge of the trade secret;

(ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—

(I) derived from or through a person who had used *improper means* to acquire the trade secret;

(II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(iii) before a material change of the position of the person, knew or had reason to know that—

(I) the trade secret was a trade secret; and

(II) knowledge of the trade secret had been acquired by *accident or mistake*;

18 U.S.C. § 1839(5) (emphasis added).

Notably, the DTSA expressly states that improper means "does not include reverse engineering, independent derivation, or any other lawful means of acquisition." § 1839(6)(B). In the hypothetical proposed above, where one GenAI user received the same brilliant information from that application as another, the means of acquisition of that information is equally lawful for both Company A and Company B, and absent of any accident or mistake. Moreover, neither Company B nor the company behind the GenAI application owed any duty of confidentiality or secrecy to Company A. As such, the DTSA may prove entirely unhelpful to Company A in this instance.

In summary, information acquired from GenAI applications can be protected by trade secret law at the federal and state levels, depending upon numerous factors. Although it is a largely fact-intensive inquiry to determine whether information is, indeed, covered under trade secret law, the overarching considerations are found in the statutory requirements of independent economic value and reasonable efforts/measures to maintain the secrecy of that information. Further, any entity attempting to protect AI-created information should be mindful of the EULA governing its user relationship with the AI application.

The Strategic Management of AI to Protect Pre-existing Trade Secrets

Some of the same concerns addressed above also relate to the hazards of companies utilizing GenAI with pre-existing trade secret information. GenAI applications (think ChatGPT), have begun to emerge as tools for companies across the world for content creation, programming, data analytics, and strategy formation. According to a September 2023 press release from The Conference Board, a business performance think tank, 56% of surveyed workers in American businesses are using GenAI to perform work tasks, while only 23% of those workers reported their employer having a policy for the use of AI on the job. The practice of using GenAI on the job will only increase in the coming decades. However, one cannot use GenAI without providing prompts. This act of providing information to a third-party AI company comes with potentially grave implications for trade secret protections that companies should be aware of.

The DTSA definition of a trade secret was examined above, and one crucial component of that definition was that the owner of the information must take "reasonable measures to keep such information secret," 18 U.S.C. § 1839 (3)(A). The UTSA and individual state statutes related to the UTSA have a similar precondition to trade secret status. *See, e.g.*, Uniform Trade Secrets Act, § 1(4)(ii) (requiring the trade secret to be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy"). Therefore, similarly to how a company wanting to protect AI-generated information with trade secret protections must be mindful of the EULA terms, so too should a company with existing trade secrets that allows its employees to use AI applications.

As previously mentioned, GenAI applications oftentimes collect and store the inputs that their users type into the application as prompts and the company that created the AI application can review, use, store, and even sell those inputs (depending upon the terms of the EULA). This means that the input may be used in responding to another person's prompt. Or, as is always the case, the GenAI company may be subject to a cyber breach, exposing all collected data. Deleting the prompt information that was provided to the AI application is incredibly difficult, if not impossible, depending upon the application being used. As a result, companies using AI applications may inadvertently disclose their trade secrets to third parties without any guarantee of confidentiality or protection whatsoever.

The response to this reality has been well-reported and widespread across different industries for different reasons. For example, many law firms have banned the use of ChatGPT and other GenAI tools to maintain client confidentiality and ethical standards. Meanwhile, Apple, Verizon, Samsung, Northrop Grumman, and Deutsche Bank, to name only a few examples, also have restricted employee use of ChatGPT for fear of the disclosure of confidential information.

An outright ban on GenAI in the workplace is certainly one solution to the potential disclosure of confidential information, but it's also likely impractical and unwise in the long term. As GenAI capabilities improve and become more intertwined with business as a whole, this type of policy will likely fail or hold a company back from additional efficiency and productivity. In fact, it may do that now to some degree.

There are other solutions to the problem, including targeted access controls. Many companies attempting to attach trade secret protection to information already have protocols limiting access to that information to a select group of employees. Coupling this protocol with a policy on the type of information that may be used as an input in GenAI applications, or even limiting the keywords and phrases that can be used by employees in GenAI applications through additional software, are less hard-lined approaches.

Some companies choose to enter into enterprise licenses with GenAI provider companies that places restrictions on the types of information that the GenAI company can collect, store, and use. An EULA may provide that the GenAI company can use the prompts its customer to train the application and be used in responding to future prompts. An enterprise license could be drafted to prohibit the underlying GenAI model to be trained with inputs from the customer, or to isolate the model being trained by the customer inputs and only provide the customer access to it.

Another concern is a company's third-party vendors and partners' use of GenAI. When providing confidential information to third parties, a company should be cognizant of the fact that their employees may use GenAI in the regular course of business – whether it's known to the third party's management or not. Company leaders may want to consider proposing language in Non-Disclosure Agreements that directly addresses the disclosure of confidential and/or trade secret information through GenAI applications, and other additional policies to protect such information during necessary third-party disclosures.

A final consideration is employee education and awareness. None of the aforementioned policies are helpful if employees are not trained on both the policies and the overall threat that GenAI poses to confidential business information. Companies should be aware of the threats posed by AI to company information and inform their employees accordingly. Additionally, employees should be trained on how to best use AI in their work duties.

In summary, the starting point in evaluating whether the use of GenAI is potentially exposing confidential business information is to review the EULA provided by the company hosting the GenAI application. Companies can negotiate enterprise licenses and implement policies to protect information while still using GenAI in business, so a blanket ban is not always the best method for the strategic use of AI. If a company puts thought behind its actions before using GenAI applications and takes reasonable measures to protect its information, GenAI has the ability to catapult business productivity and efficiency to heights never before imaginable.