Kilpatrick

Insights: Perspectives

Gen AI: The "Artificial" Threat to Trade Secrets

April 4, 2025

Written by **Joel D. Bush**

Trade secrets have been a recognized form of intellectual property for at least two centuries, and the advent of new technologies has always challenged either the scope of trade secret protection or the capacity to maintain confidentiality. Today, generative artificial intelligence ("Gen AI") presents new challenges – and opportunities – for trade secret rights. This technology has impacted every major industry across the globe and is a topic around both the kitchen table and the corporate conference room. Investment in Gen AI has soared past a trillion dollars, the marketplace for Gen AI powered products will surpass that mark in the coming years, and nearly every major business has implemented Gen AI as a part of their operations, effecting as much as half of impacted employee activity. Some observers resort to doomsaying about Gen AI's threat to human survival.

A chorus of predictions adds to the clamor about the Gen AI's threat to trade secrets and even their potential demise. Some have written their eulogy, saying that Gen AI "will destroy" trade secrets and that only a "blanket ban" on Gen AI will protect them. Others eagerly await the use of Gen AI to unveil Coca Cola's secret formula, claiming that it could "lose all protection" if "an advanced AI program" replicates it. Still others believe that any trade secrets laying hidden in AI training data are "public" even if never found.

There are reasons to doubt these negative forecasts. The world's most valuable trade secrets are not a few clicks away from becoming valueless public knowledge. No court has held that Gen AI has stripped even one alleged trade secret of legal protection.

As this article outlines, while Gen AI may pose new challenges for trade secret holders, it should not pose an existential threat to trade secrets as a protected form of intellectual property.

I. What are trade secrets?

A trade secret is valuable information, not generally known or easily ascertainable, that is protected from disclosure by one company and that would be of great value if known to a competitor. And like any secret, once it is out, it is no longer a secret.

Determining trade secret status is generally a mixed question of law and fact. The Defend Trade Secrets Act ("DTSA"), 18 U.S.C. §§ 1831, *et seq.*, describes "trade secrets" as follows:

> [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, electronically, graphically, photographically, or in writing..."[1]

To constitute a "trade secret," its owner must "have taken reasonable measures to keep such information secret," and the information must "derive[] independent economic value" from both "not being generally known" and "not being readily ascertainable through proper means" by someone "who can obtain economic value from the disclosure or use of the information[.]"[2]

The law protects "trade secrets" from "misappropriation" by parties wishing to learn—or who do learn—the information either through "acquisition" by "improper means" or "disclosure or use" without permission.[3] "[I]mproper means" includes the use of "theft, bribery, misappropriation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means[.]"[4] Knowing or having reason to know that the trade secret was improperly acquired, disclosed, or used evidences misappropriation.[5] Importantly, trade secrets are not protected from "reverse engineering, independent derivation, or any other lawful means of acquisition[.]"[6]

In short, a "trade secret" is secret valuable information protected by "reasonable measures" that is neither "generally known" nor "readily ascertainable" by one who would gain from its "disclosure or use."[7] And learning or trying – to learn – the secret by "improper means" makes it no less a "trade secret."[8]

II. Opportunities for trade secret protections will remain.

These *legal* elements for trade secret protection will likely protect confidential and highly valuable business information from any challenges presented by Gen AI.

A passing review of the law – and its trendline over the past fifty years – should provide confidence in the continued durability of trade secret protections in the face of innovative technologies.

a. Only Reasonable Measures Required.

To protect a trade secrets, owners are required to undertake "reasonable measures" to maintain secrecy.[9] It should go without saying that "unreasonable" measures – safeguards that lack any contextual reasonableness – are not required. And that is what courts have held for over fifty years.

In 1970, in *E.I. duPont deNemours & Co v. Christopher*, the Fifth Circuit held that otherwise legal aerial photography of a DuPont chemical plant, to discover a secret manufacturing process for producing methanol, was nonetheless an "improper method of discovering trade secrets exposed during construction of the [] plant[.]"[10] In so holding, the court explained that the law does "not require a person or corporation to take unreasonable precautions to prevent another from doing that which he ought not to do in the first place," let alone "guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available."[11] In other words, the court found it unreasonable and unrealistic to require DuPont, for example, "to put a roof over the unfinished plant to guard its secret."[12]

The U.S. Supreme Court subsequently relied on *Christopher* for this "improper means" principle.[13] The Eleventh Circuit applied its reasoning in 2024 in holding that the automated data scraping of millions of fully public insurance quotes from a competitor's website constituted "improper means" for purposes of trade secret misappropriation.[14]

The court in *Compulife 2* found "that even if individual quotes that are publicly available lack trade secret status, the whole compilation of them (which would be nearly impossible for a human to obtain through the website without scraping) can still be a trade secret."[15] In response to an argument that website scraping activities "may be perfectly legitimate," the court explained:

> But the defendants in this case did not take innocent screenshots of a publicly available site; instead, they copied the order of Compulife's copyrighted code and *used that code* to commit a scraping attack that acquired millions of variable-dependent insurance quotes. If they had not formatted and ordered their code exactly as Compulife did, they would not have been able to get the millions of quotes that they got. As we explained in the previous appeal, this deceptive behavior resembles the acquisition of a trade secret through surreptitious aerial photography, which we addressed in *Christopher.*[16]

In an earlier decision, the court explained that against "a certain type of reconnaissance," even taking "no measures to protect" a trade secret may still be reasonable or the method of taking improper.[17] In other words, there was nothing "reasonable" required of Compulife to protect its datasets and copyrighted code from the intrusion and theft facilitated by automated bots that far exceeded the capacity of a human being acting alone.

These cases illustrate the propensity of courts to side with trade secret owners when trade secrets are threatened by new technologies that present novel "improper means" for stealing trade secrets and that question the reasonableness of trade secret owners' secrecy measures in the context of technological innovations.

Gen AI is thus the latest technological innovation to present potential challenges to trade secret protections. While the advent of Gen AI may require different solutions for protecting confidential information, it only requires reasonable ones.

b. Neither Generally Known nor Readily Ascertainable.

Of course, to be a trade secret, the information must be "secret." Specifically, it cannot be "generally known" or "readily ascertainable,"[18] meaning that the information is not easily accessible and is "difficult, if not impossible" to obtain.[19] Put another way, "readily ascertainable" means that the information is easy to discover from another source through legitimate methods, such as in reviewing trade journals, reference resources, or other published materials. "Readily ascertainable" relates to whether the trade secret owner has adequately safeguarded the information at issue with the specific objective of maintaining confidentiality.

For example, in *Nationwide Mut. Ins. Co. v. Mortensen*, the court found that trade secret protections could not apply to information in unprotected physical documents found in hard copy files, even though the information at issue was elsewhere archived digitally in a password-protected database, because the information at issue was also "readily ascertainable" from the hard copy files.[20]According to the court, "[i]t is not the medium that matters here, but whether the information itself was adequately protected—and it was not. Because this same information was readily available from another source, it does not qualify as a trade secret as a matter of law."[21]

Some observers posit that Gen AI will render trade secrets “readily ascertainable,” thereby eviscerating trade secret status and legal protection. They reason that Gen AI will allow users to discover any trade secrets in the platform's training data or otherwise facilitate the reproduction of a party's trade secrets through skillful prompt engineering.[22] But that misapprehends how Gen AI works and ignores existing legal protections.

To begin, Gen AI platforms are not all-knowing or exhaustive repositories of existing secret information. Gen AI outputs are not the equivalent of extracted text or data harvested from an organization's internal secret files and systems. Instead, Gen AI platforms generate *new text* based on the application of pattern creation algorithms to large language models and data sets that themselves are based on publicly available information. At present, these outputs are more apt to generate *new trade secrets* rather than to make any existing trade secrets “readily ascertainable,” because the Gen AI outputs reflect *newly created* data patterns, not mere recall of existing data or heretofore secret information.

Importantly, datasets used to train Gen AI models are not rife with trade secret information. Gen AI programs are trained on large volumes of information gleaned from the internet and other public sources. But these sources of public information and “readily accessible” data typically do not include confidential information and trade secrets. It is axiomatic that “[a] trade secret that becomes public knowledge is no longer a trade secret.”[23] And “[o]nce information has been published on a website...there is no further act required...to make the information available to the public.”[24] Such “publication of [] information over the internet” almost certainly destroys trade secret status.[25] In short, the data sets that support large language models, insofar as they are developed from the internet and other public repositories, do not widely include trade secrets.

In extremely rare situations, trade secret protection can apply to “obscure or transient” information that is “technically public” but practically inaccessible to competitors[26], but these exceptions do not change the reality that datasets derived from publicly available information do not contain “secrets.” The existence of non-secret information in training data for Gen AI models is therefore no threat to trade secrets.

And even in the rare instance in which a trade secret is included in training data, as a consequence of being available through a public source, it almost certainly will continue to remain hidden. “The guiding ‘concern is whether the information has retained its value to the creator in spite of the publication.'”[27] *For example,* in *Syncsort*, the court held that brief internet postings of trade secret information to websites in Korea and Japan were “sufficiently obscure or transient or otherwise limited” so that it was not made “generally known to the relevant people [like] potential competitors.”[28] Accordingly, if an obscure piece of information that is claimed as a trade secret is difficult to be discovered on the internet, it will be similarly challenging to ascertain through a Gen AI platform. Users of Gen AI platforms have very limited knowledge about the data sets on which a Gen AI model is trained, the cut-off date of the harvested information, and the programing models. In other words, it is difficult to identify a needle in a haystack in the ocean of information on the internet or in the training data for a Gen AI platform. The user – whether conducting a Google search or creating a prompt for a Gen AI platform – simply does not know where (or how) to look.

Gen AI's outputs are also imperfect. The input-output exchange, much like a human conversation, is full of bias, variety, imprecision, and error. Any law student who has talked to a professor, or a lawyer who questions a witness, knows just how hard it is to ask the right question and elicit a useful answer. Gen AI is no different: notwithstanding the volume of information it might access, it mimics human language with all its imperfections. And Gen AI platforms may "hallucinate." The outputs may be factually incorrect, "imagined," or simply unhelpful. While a Gen AI platform may produce a response to a prompt seeking the recipe for Coca-Cola, the answer cannot be confirmed as correct or even close to the actual secret recipe. The output may be interesting, but it is *not* a bona fide reproduction of an as yet undisclosed trade secret.

In addition, the very training data itself may constitute a protected trade secret, because compilations of training data might qualify for trade secret protection. It is possible for training data and each Gen AI model's finetuning, rules, and checkpoints to meet the requirements for trade secret protection. The information is secret, valuable, and closely guarded.[29] And courts have also found that "testing and know how" and "dead ends and trial and errors" data may be protected if the tests are not so obvious as to be "readily ascertainable."[30] Therefore, even if an existing trade secret is buried in the training data, it might itself be a part of a newer and different trade secret.

Along these lines, in some circumstances, data compilations may constitute a trade secret even if the constituent elements of the compilation are publicly available. Courts have routinely affirmed "combination trade secrets" wherein "some or all of the components of the trade secret are well-known" but have been arranged in "a unique combination" that "adds value."[31] "[T]he simple fact that [information] taken [was] publicly available does not automatically" mean it is not a protected trade secret.[32] In fact, in the recent *Compulife* cases, *all* of the information at issue was publicly available and yet it was found to be a trade secret.[33]

In sum, while Gen AI may increase access to information, and especially the efficient synthesis of large amounts of information, it neither relies on trade secrets, regurgitates them on command, nor reliably ascertains them.

c. Improper Means

Trade secrets remain protected unless they can be discovered by "proper means."[34] In other words, trade secrets are protected from misappropriation or discovery by "improper means,"[35] such as unauthorized use, acquisition, or disclosure.

The use of innovative technology is not *per se* illegal or improper in the trade secret context. The DTSA prohibits "espionage through electronic" means,[36] and courts have routinely protected trade secret rights threatened by innovative technologies.

In *Christopher*, in the face of a novel use of aerial photography, the court explained that "thou shall not appropriate a trade secret through deviousness."[37] In *UAB "Planner5D" v. Facebook, Inc.*, *et al.,* the court denied a motion to dismiss trade secret claims based on allegations that defendant Princeton University had engaged in "improper means" to "bypass the structure of [plaintiff's] website to scrape...data files" in violation of terms of use.[38] The court found that the complaint sufficiently alleged that "[b]ecause [plaintiff's] website hid the locations and contents of its data files, and because Princeton had to design and deploy hacking software to obtain this information, Princeton knew or should have known that

[plaintiff] intended for the data files to remain confidential" and that the terms of service expressly prohibited what Princeton allegedly had done.[39] In other words, it constituted "improper means" for the defendant in *UAB "Planner5D"* to use specialized technology tools to harvest information that was meant to remain confidential.

In *Compulife 1*, the court explained that it was the very use of technology in excess of human capacities that rendered the conduct improper:

> Although Compulife has plainly given the world implicit permission to access as many quotes as *humanly* possible, a robot can collect more quotes than any human practicably could. So, while manually accessing quotes from Compulife's database is unlikely to ever constitute improper means, using a bot to collect an otherwise infeasible amount of data may well be – in the same way that using aerial photography may be improper when a secret is exposed to view from above.[40]

The court in *Compulife 2* explained further that defendants had not used the technology to "take innocent screenshots of a publicly available site," but instead copied Compulife's code and "commit[ed] a scraping attack that acquired millions of variable-dependent insurance quotes," which would have been impossible without the use of the code and scraping technology.[41]

Courts have thus consistently protected trade secret owners when technological advances have facilitated new and different "improper means" for trade secret theft. It is possible that Gen AI might be used in the future to misappropriate trade secrets, and the scope of such uses and threats is not yet fully clear. However, there is no reason to believe that courts will reverse their prior approach of protecting trade secret owners when their secrets are challenged by new technologies.

III. Implications for the Future

The future for trade secrets remains bright. For trade secret owners, courts, and practitioners, the rise of Gen AI is simply the latest in a series of technology advances that have applied to trade secrets: aerial photography, the internet, automated data scrapping, and now Gen AI. Courts have always applied existing law to innovative technology tools, and Gen AI should be no different.

Going forward, as Gen AI continues to develop and become more ubiquitous, it may be that what was once hard to ascertain becomes more easily discoverable, and that reasonable measures for safeguarding secrecy must evolve accordingly.

But that does not mean that Gen AI is an existential threat to trade secrets. It is just the latest in a long line of challenges and opportunity that new technologies present for trade secrets.

Kilpatrick – Generative AI

Kilpatrick's Generative AI practice works with clients to tackle their most pressing AI concerns and challenges to achieve results in line with overall business strategies and goals. Our multidisciplinary team, with backgrounds in intellectual property, privacy, cybersecurity, federal legislation and regulation, commercial transactions, and dispute resolution, monitors and proactively addresses risks, compliance requirements, and opportunities related to generative AI. For more information, please visit our website: Kilpatrick – Generative AI.

Kilpatrick Connect – AI Legal Consulting

There is no development as consequential or with more legally significant implications for your business as the recent advancements in AI. Kilpatrick Connect is a legally focused AI consulting and advisory offering built upon Kilpatrick's AI, legal, and industry expertise and delivered through a confidential attorney-client relationship. We understand the transformative capabilities of AI and its profound impact on your business, and Kilpatrick Connect provides a safe, secure, and economical hub to address AI-related questions, issue resolution, and strategy development. For more information on Kilpatrick Connect, please visit our website, Kilpatrick Connect – AI Legal Consulting.

Footnotes

---

[1] 18 U.S.C. § 1839(3).

[2] *Id.* at § 1839(3)(A)–(B).

[3] *Id.* at § 1839(5).

[4] *Id.* at § 1839(6)(A).

[5] *Id.* at § 1839(5).

[6] *Id.* at § 1839(6)(B).

[7] *Id.* at § 1839.

[8] The Uniform Trade Secrets Act ("UTSA"), which has been adopted with slight variations in every state except New York, contains materially and substantively identical definitions. *See Compulife Software Inc. v. Newman*, 959 F.3d 1288, 1311 n.13 (11th Cir. 2020) (*Compulife 1*) (identifying the "largely identical" and "substantially equivalent" definitions between the DTSA and Florida's UTSA).

[9] 18 U.S.C. § 1836(b)(2)(IV)(AA).

[10] 431 F.2d 1012, 1017 (5th Cir. 1970).

[11] *Id.* at 1016–17.

[12] *Id.* at 1016.

[13] *See Kewannee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475–76 (1974).

[14] *Compulife Software, Inc. v. Newman*, 111 F.4th 1147, 1163 (11th Cir. 2024) (*Compulife 2*).

[15] *Id.* at 1162.

[16] *Id.* at 1163.

[17] *Compulife 1*, 959 F.3d at 1312.

[18] 18 U.S.C. § 1839(3)(B).

[19] *Allstate Ins. Co. v. Fougere*, 79 F.4th 172, 189 (1st Cir. 2023) (affirming finding that spreadsheets containing large amounts of publicly available data were too extensive to be "readily ascertainable" from alternative sources).

[20] 606 F.3d 22, 29 (2d Cir. 2010).

[21] *Id.*

[22] *See, e.g.,* John G. Sprinkling, *Trade Secrets in the Artificial Intelligence Era*, 76 S.C. L. Rev. 181, 207 (2024) (predicting that Coke will lose "all protection" for its formula because it will become readily ascertainable to "an advanced AI program"); *see also* David S. Levine, *Generative Artificial Intelligence and Trade Secrecy*, 3 J. Free Speech L. 559, 580 (2023) (predicting that Gen AI will make "accessibility" a non-issue).

[23] *BondPro Corp. v. Siemens Power Generation, Inc.*, 463 F.3d 702, 706 (7th Cir. 2006) (holding that a trade secret published in a patent application was no longer a trade secret).

[24] *Oja v. U.S. Army Corps of Engineers*, 440 F.3d 1122, 1131 (9th Cir. 2006).

[25] *DVD Copy Control Assn., Inc. v. Bunner,* 116 Cal. App. 4th 241, 10 Cal. Rptr. 3d 185, 193 (2004) (finding no trade secret protections for a program that was posted on "hundreds of [w]eb sites"); *see also Arkeyo, LLC v. Cummins Allison Corp.*, 342 F.Supp. 3d 622, 632 (E.D. Pa. 2017) ("The posting of materials on the internet without any confidentiality protections makes the information publicly available and renders the materials incapable of trade secret status.").

[26] *See e.g., Hurry Fam. Revocable Tr. v. Frankel,* No. 8:18-CV-2869-CEH-CPT, 2023 WL 23805, at *8–*9 (M.D. Fla. Jan. 3, 2023) (holding a trade secret did not lose protection even when posted on the court's public docket); *Syncsort Inc. v. Innovative Routines, Int'l, Inc.*, No. CIV. 04-3623 WHW, 2011 WL 3651331, at *15 (D.N.J. Aug. 18, 2011) (despite online postings of software command language, "there is no evidence that information became widely available or that competitors or other unauthorized persons accessed or even attempted to access the information").

[27] *Syncsort*, 2011 WL 3651331, at *13 (citation omitted).

[28] *Id.*

[29] *See infra* Sec. 1; *see also* 18 U.S.C. § 1839(3).

[30] *Olaplex, Inc. v. L'Oreal USA, Inc.*, 855 Fed. Appx. 701 (Fed Cir. 2021) (dismissing these allegations due to insufficient pleading but recognizing that they could qualify for protections if sufficiently alleged).

[31] *Penalty Kick Mgmt. Ltd. v. Coca Cola Co.*, 318 F.3d 1284, 1291 (11th Cir. 2003); *Tewari De-Ox Sys., Inc. v. Mtn. States/Rosen, LLC*, 637 F.3d 604, 613 (5th Cir. 2011) ("A trade secret can exist in a combination of characteristics and components each of which, by itself, is in the public domain, but the unified process, design, and operation of which in unique combination, affords a competitive advantage and is a protectible secret."); *see also Mallet and Co., Inc. v. Lacayo*, 16 F.4th 364, 386, 386 n. 28 (3rd Cir. 2021) (collecting cases affirming combination trade secrets and the protection of public information).

[32] *Compulife 1*, 959 F.3d at 1315.

[33] *See gen.*, *Compulife 1* and *Compulife 2*; *see also Allstate*, 79 F.4th at 189 ("The publicly accessible nature of certain portions of the spreadsheets certainly informs our trade secret analysis . . . [but] it is not dispositive, and it does not defeat Allstate's trade secret claims.").

[34] 18 U.S.C. § 1839(3)(B).

[35] *Id.* at § 1836(b)(2)(A)(ii)(IV)(AA).

[36] 18 U.S.C. § 1839(6)(A).

[37] 431 F.2d at 1017.

[38] No. 19-CV-03132-WHO, 2020 WL 4260733, *8 (N.D. Cal. July 24, 2020).

[39] *Id.*

[40] 959 F.3d at 1314.

[41] 111 F.4th at 1163.

Related People

Joel D. Bush

t 404.815.6074

jbush@ktslaw.com