Keeping ChatGPT a Trade Secret While Selling It Too

Camilla A. Hrdy[1]

Berkeley Technology Law Journal (forthcoming)

I greatly appreciate any comments you have.
Please email any comments to cahrdy@gmail.com

Abstract

Generative artificial intelligence products such as ChatGPT raise novel issues for trade secret law. But one of the most important issues is an old one: How to sell an information good, like computer software, while also maintaining trade secrecy protection for the underlying content? When a company wishes to sell a new technology to the public, the normal recourse is to obtain a patent. Patents require public disclosure and end after a fixed term of years. However, based on decades of precedents established for software, generative AI companies will be able to rely on trade secret law instead—maintaining indefinite protection for their technology, even as they profit from making it widely available to the public, and even after reverse engineering becomes technically feasible. This is what many companies did with closed-source software, and this is what developers of some generative AI models—including ChatGPT—are doing today. They are releasing

[1] Associate Professor of Law, Rutgers Law School. Many thanks to colleagues for their invaluable comments and insights: Ryan Abbott, Jonas Anderson, Sarah Burstein, Michael Carrier, Victoria Cundiff, Rebecca Curtin, Tait Graves, James Grimmelmann, Eric Goldman, Ellen Goodman, Cynthia Ho, Peter Karol, Sonia Katyal, Mark Lemley, Dave Levine, Jake Linford, Orly Lobel, Mike Madison, Mike Mattioli, Tim Murphy, Sarah Rajec, Alexandra Roberts, Elizabeth Rowe, Sharon Sandeen, Andres Sawicki, Jake Sherkow, Cathay Smith, Deepa Varadarajan, John Villasenor, and participants at the 2024 Trade Secrets Virtual Workshop, Works in Progress in Intellectual Property (WIPIP) 2024 at Santa Clara Law, and the M3 Workshop at Suffolk Law School. Many thanks to Devin Owens, J.D. Candidate at Akron Law, for his research and ideas about model extraction attacks.

the models in a "closed-source" format that hides algorithms, code, training data, and underlying model architecture from users. And they are attaching contractual provisions—called "terms of use" or "end user license agreements" (EULAs)—that limit users' ability to reverse engineer information about how the models work or share that information with others. Some of these agreements, including ChatGPT's, even contain noncompete provisions.

If liability for breaching these provisions were limited to breach of contract, there would be less cause for alarm. However, some case law—and some state statutes—indicate that reverse engineering trade secrets in breach of an anti-reverse-engineering clause can give rise to trade secret liability as well, because breach of the contract transforms otherwise-lawful reverse engineering into an "improper means" of acquiring trade secrets. The prospect of trade secret liability for what should be, at worst, breach of contract is alarming. It means prevailing plaintiffs can obtain trade secret law remedies, not just contract law remedies, and it means that liability can extend to third parties who did not even sign the contract. For example, if someone reverse engineers information about ChatGPT in violation of a boilerplate terms of use, and then shares that information with someone else, who publishes the information on the internet, both of these actors could be liable for trade secret misappropriation.

Maintaining some legal protection for information goods is important. Otherwise, companies might not make information goods available to the wider public at all. But trade secrecy protection should not last after actual secrecy has ended. Fortunately, there is a solution. In the Defend Trade Secrets Act (DTSA) of 2016, Congress made clear that reverse engineering is legal under federal trade secret law and cannot be considered an "improper means" of acquiring a trade secret. The mere presence of a contract purporting to prohibit reverse engineering cannot change this rule. A state law that holds otherwise is preempted by federal trade secret law pursuant to the Supremacy Clause of the Constitution. The upshot is that, in many circumstances, reverse engineering a publicly-distributed generative AI model—or a traditional software product—is not trade secret

misappropriation, regardless of the presence of a boilerplate anti-reverse-engineering clause.

This doctrinal approach will not spell the end of trade secrecy protection for generative AI. Companies can still rely on trade secrecy before reverse engineering becomes feasible. Companies can still rely on claims for breach of contract. And companies can still bring trade secret claims against insiders who are under a duty of confidentiality, such as employees, business partners, and those who obtain negotiated licenses with the AI developer. But this approach will make sure that, once a widely-available product can easily and cheaply be reverse engineered by members of the general public, companies cannot maintain trade secret protection indefinitely through contract.

Introduction

Generative artificial intelligence ("generative AI") is a species of artificial intelligence, which has been around for a long time.[2] But generative AI has new capabilities that are extremely compelling to businesses, as well as to members of the general public. The most famous example of a generative AI is ChatGPT, a generative AI product[3] developed and distributed by OpenAI.[4] ChatGPT, which is technically a form of generative AI called a "large language model," has both extraordinary generative capabilities and a unique facility with human language. For most users,

[2] Artificial intelligence means very loosely using computers to perform activities normally associated with human intelligence. Generative AI is a subset of AI to the extent it does that. *See* Hon. Xavier Rodriguez, *Artificial Intelligence (AI) and the Practice of Law*, 24 SEDONA CONF. J. 783, 788-789 (2023); *see also* Ryan Abbott and Elizabeth Rothman, *Disrupting Creativity: Copyright Law in the Age of Generative Artificial Intelligence*, 75 FLA. L. REV. 1141, 1146 (2023); Gaetan de Rassenfosse, Melissa Wasserman, & Adam Jaffee, *AI-Generated Inventions: Implications for the Patent System*, 96 S. CAL. L. REV. 101, 104 (2023).

[3] I often use the term "product" to describe generative AIs like ChatGPT, though I mean for this term to encompass services too. *Accord, e.g.,* Andersen v. Stability AI Ltd., No. 23-CV-00201-WHO, 2023 WL 7132064, at *1 (N.D. Cal. Oct. 30, 2023) (describing Stable Diffusion as a "software product").

[4] OpenAI has close ties to Microsoft, which owns a very large stake in OpenAI, though does not control the company. Microsoft offers its own AI, AzureOpen, AI Service, based on OpenAI's technology. https://blogs.microsoft.com/blog/2023/01/23/microsoftandopenaiextendpartnership/

ChatGPT takes the form of an interactive "chat bot," accessed through a smart phone application or a web browser, which can instantly spit out responses to users' prompts.[5] These responses are usually informative and sometimes shockingly creative and insightful. They often match or exceed the quality of human-generated work.[6]

Generative AI products like ChatGPT[7] raise novel issues for trade secret law.[8] But the most practical challenge is an old one: How to protect "information goods" under trade secret law, while also profiting from widely distributing them to the general public? Generative AI, like books, music, and software,[9] is an information good. By design, information goods embed significant information about the product that is visible to users or potentially accessible to users through a process of "reverse engineering."[10] Companies face a special trade-secret-law challenge when

---

[5] Sources I used to try to understand generative AI include: Rebecca Heilweil, *What is generative AI, and why is it suddenly everywhere? Between ChatGPT and Stable Diffusion, AI suddenly feels mainstream,* VOX, Jan 5, 2023, 8:00am EST; Jacob Schneider, *Generative AI's Output: How Is It Created, and What IP Rights Should It Receive?* JD SUPRA, October 3, 2023; Amy Winograd, *Loose Lipped Large Language Model Spill Your Secrets: The Privacy Implications of Large Language Models,* 36 HARV. J.L. & TECH. L. J. 615, 616-18 (2023); Maura Grossman, Paul Grimm, Daniel Brown & Molly Xu, *The GPT Judge: Justice in a Generative AI World,* 23 DUKE LAW & TECH. J. 1, 8 (forthcoming), https://ssrn.com/abstract=4460184; Katherine Lee, A. Feder Cooper & James Grimmelmann, *Talkin' 'Bout AI Generation: Copyright and the Generative-AI Supply Chain*, J. COPYRIGHT SOC'Y (forthcoming), https://ssrn.com/abstract=4523551. On AI and machine learning, generally, *see also, e.g.,* Charlotte Tschider, *Beyond the "Black Box,"* 98 DENVER L. REV. 683, 689-99 (2021); Daryl Lim, *AI & IP: Innovation & Creativity in an Age of Accelerated Change*, 52 AKRON L. REV. 813, 820-23 (2018).

[6] *But see, e.g.,* Jonathan H. Choi & Daniel Schwarcz, *AI Assistance in Legal Analysis: An Empirical Study*, Minnesota Legal Studies Research Paper No. 23-22 (Aug. 13, 2023) (finding assistance from Chat GPT-4 enhanced performance on law school exams for students at the bottom of the class but not for students at the top of the class).

[7] There are many similar products to ChatGPT and more every day. 10 *ChatGPT Alternatives & Competitors (Free and Paid): ChatGPT might be the best-known AI, but it's not the only one out there,* PC WORLD, Sep. 29, 2023.

[8] *See* David S. Levine, *Generative Artificial Intelligence and Trade Secrecy*, 3 JOURNAL OF FREE SPEECH LAW 559 (2023). *See also* Camilla A. Hrdy, *Generative AI: Emerging Trade Secrecy Issues*, CHICAGO KENT LAW REVIEW, AI & THE LAW SYMPOSIUM ISSUE (forthcoming).

[9] Software means loosely a computer program that employs code that is written to perform specified pre-determined functions, though the line between AI and software can be hard to draw because software can incorporate AI, and AI can be linked to a software system. *See* Nicholson Price & Arti Rai, *Clearing Opacity Through Machine Learning*, 106 IOWA L. REV. 775, 777 (2021).

[10] SUZANNE SCOTCHMER, INNOVATION AND INCENTIVES 31-35 (2004) (discussing "information goods" like music and software); *see also* Pamela Samuelson and Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L. J. 1575, 1579, 1595 (2002) (describing

they distribute information goods to the public on a mass scale—as OpenAI is doing with ChatGPT. The reason is simply that public distribution tends to destroy secrecy, and without secrecy there can be no trade secret.

However, with software, companies overcame the public distribution challenge by employing a two-part solution.[11] First, software companies maintain *factual secrecy*[12] by releasing software in a "closed-source" structure that keeps back-end[13] features like source code hidden from users of the software.[14] Second, software companies use contracts to maintain *legal secrecy*, even for features that can potentially be discerned by users and that users would not ordinarily consider secret. Software companies achieve this by structuring sales of the software as "licenses" and attaching "end user license agreements" (EULAs) or "terms of use," which significantly limit what users can do with the software.[15]

"information technology products" as embedding more information and "applied know-how within the product distributed in the market" than traditional manufactured goods); Amy Kapczynski & Talha Syed, *The Continuum of Excludability and the Limits of Patents*, 122 YALE L. J. 1900, 1908-1910 (2013) (asserting that it is possible to sell information itself or to sell an "information-embedded good," which vary in the degree to which they can be protected by secrecy or by exclusive rights).

[11] *See* Mark Lemley*, Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1243 (1995).

[12] By factual secrecy, I mean not plainly visible or readily ascertainable to users of the product because they can be easily reverse engineered. "Readily" means with ease, quickly, and with little expense. *See* text and notes 358-363 *supra*.

[13] Case law involving software has sometimes distinguished "front-end" features like overall functionality which "is readily deducible to anyone using the program" and "back-end" features, like source code, which are not revealed to users. Agency Solutions.Com, LLC v. TriZetto Grp., Inc., 819 F. Supp. 2d 1001, 1017-1019 (E.D. Cal. 2011).

[14] *See id*. at 1243-44; *see also* Michael J. Madison, *Reconstructing the Software License*, 35 LOYOLA U. CHI. L.J. 275, 280-282 (2003); Sonia K. Katyal, *The Paradox of Source Code Trade Secrecy*, 104 CORNELL L. REV. 1183, 1195-1203 (2019); Jeanne Fromer, *Machines as the New Oompa Loompas*, 94 N.Y.U. L. REV. 706 , 717 (2019). *See also* ROGER M. MILGRIM & ERIC E. BENSEN, MILGRIM ON TRADE SECRETS §§ 1.03, 1.05, 1.09 (Matthew Bender & Co. 2023) (identifying case law recognizing trade secret protection for software code).

[15] *See* Lemley, *supra* note 11, at 1245*; see also, e.g.,* Mark Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 459 (2006); AARON PERZANOWSKI & JASO SCHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY 2 (2016); Nancy S. Kim, *Revisiting the License v. Sale Conundrum,* 54 LOY. L.A. L. REV. 99, 101 (2020); Mark Lemley, *The Benefit of the Bargain*, 2023 WIS. L. REV. 237 246, 256-258 (2023). *See also* RAYMOND T. NIMMER, 2 INFORMATION LAW § 11:12 (West 2022) (discussing use of nondisclosure and non-reverse engineering terms in mass-market transactions involving "sales of products … in which no confidentiality can ordinarily be retained in fact[.]").

Many generative AI companies are following the same playbook that worked for software. First, they are distributing generative AI models using a "closed-source" structure that hides the model's inner workings from users.[16] ChatGPT users, for example, generally have no idea how the underlying generative AI models works or how it reached its conclusions. Most users are not given access to the "model" at all. They interact with the user interface, which is a technically a separate software system from underlying generative AI model that is generating responses to users' queries.[17] From users' perspective, ChatGPT is the ultimate "black box."[18] Second, generative AI companies are utilizing contracts to shore up, and go beyond, trade secrecy protection—just as companies did for software.[19] End users of ChatGPT are subject to a robust Terms of Use that significantly restricts what they can do with the underlying technology.[20] For example, ChatGPT users are prohibited from "reverse engineering"[21] ChatGPT to learn its secrets

[16] By "closed-source" I mean generative AI models for which users are not given access to algorithms, training data and/or underlying code. I focus here on closed-source models, but importantly even "open-source" models do not necessarily reveal all information needed to understand the model's functionality or exactly how it was developed, and a license may be required for open-source models too. *See* Khari Johnson, *Meta's Open Source Llama Upsets the AI Horse Race,* WIRED, July 26, 2023, 7:08AM.

[17] Lee, Cooper, & Grimmelmann, *supra* note 5, at 5, 41-42 (discussing "closed source" generative AI models). *See* discussion in Part I *supra*.

[18] *See, e.g.,* Saurabh Bagchi, *What Is an AI 'Black Box'?* THE CONVERSATION, May 28, 2023; Editorial, ChatGPT is a black box: how AI research can break it open, NATURE, 671-672, July 25, 2023; Daniel Hardt*, Everyone uses ChatGPT, but it is a black box*, COPENHAGEN BUSINESS SCHOOL, October 10, 2023

[19] *See* Deepa Varadarajan, *The Trade Secret-Contract Interface*, 103 IOWA L. REV. 1543, 1545 (2018) (arguing that companies can elide trade secret law rules through strategic use of contract law and giving as an example the practice of conditioning user access on "non-negotiable licenses … when selling access to mass-market software.").

[20] Importantly, I use the term "end user" to describe a member of the general public who obtains access to a generative AI model like ChatGPT through an end user license agreement or terms of use, but who *does not have a prior relationship or underlying confidentiality obligations to the AI developer.* I distinguish end users from "insiders"—such as employees, business partners, or other businesses that obtain more extensive access to the model and agree in exchange to adhere to ongoing mutual confidentiality obligations. For ChatGPT, there is a totally separate terms of use for those who negotiate an "Enterprise License" with OpenAI. This is called the "Business Terms," and it contains extensive mutual confidentiality obligations. *See* discussion in Part II.

[21] I use the term reverse engineering broadly to refer to taking apart, inspecting, or investigating a product in order to learn or replicate its underlying components, regardless of the method used to do so. *See* Samuelson & Scotchmer, note 10 *supra*, at 1577 (defining reverse engineering broadly as "the process of extracting know-how or knowledge from a human-made artifact.").

or replicate its functionality.[22] Reverse engineering is legal under trade secret law,[23] but companies often seek to prohibit reverse engineering through contract law, and courts often enforce these clauses.[24] More surprisingly, the ChatGPT Terms of Use also contains a provision that will likely be construed as a *noncompete*.[25] The provision is not labeled as a noncompete, but it prevents ChatGPT users from using the model's outputs to develop "any artificial intelligence models *that compete with [Open AI's] products or services*."[26] The enforceability of ChatGPT's noncompete provision is highly uncertain, especially in light of the Federal Trade Commissions recent rulemaking banning noncompetes entered with workers.[27] Although noncompetes may be enforced when entered with other businesses, courts have struck down very similar provisions, even in business-to-business agreements.[28] As I'll discuss, this noncompete is unlikely to be enforced, for a variety of reasons: It applies to individual end users who are not sophisticated or represented by counsel, and it is governed by California law—which bans noncompetes.[29]

If liability for breaching these provisions were limited to breach of contract, there would be less cause for alarm. Contracts do not generally apply outside privity, and remedies tend to be

---

[22] https://openai.com/policies/terms-of-use *See also* Part II.

[23] 18 U.S.C. § 1839(6)(2016); Kewanee v. Bircron, 416 U.S. 470, 476 (1974).

[24] *See, e.g.,* Yang Chen, *Enforceability of Anti-Reverse Engineering Clauses in Software Licensing Agreements: The Chinese Position and Lessons from The United States and European Union's Laws*, 43 U. PA. J. INT'L L. 783 (2022) (discussing case law regarding enforceability of anti-reverse engineering clauses in U.S. as well as in E.U. and in China). *But see* Samuelson & Scotchmer, *supra* note 10, at 1626-27,1660 (noting that although software licenses often prohibit reverse engineering, whether such contracts are or should be enforceable is an unsettled question of law on which courts in the U.S. and abroad disagree).

[25] Noncompetes are heavily regulated when entered by workers. Workplace noncompetes are unenforceable in some states, and in all states, are subject to "reasonableness" standards. *See,* e.g., Camilla A. Hrdy & Christopher B. Seaman, *Beyond Trade Secrecy: Confidentiality Agreements That Act Like Noncompetes*, 133 YALE L. J. 669 (2023) (discussing enforceability of noncompetes and "de facto" noncompetes in the employment context).

[26] https://openai.com/policies/terms-of-use (emphasis added). *See also* discussion in Part II.

[27] The Federal Trade Commission recently announced that it will consider entering a noncompete with a worker to be a violation of the FTC Act. Federal Trade Commission, Non-Compete Clause Rule, issued April 23, 2024, 16 CFR Part 910, https://www.ftc.gov/system/files/ftc_gov/pdf/noncompete-rule.pdf

[28] I have found at least one case holding that a very similar provision was unenforceable due to its lack of a time limit. *See* notes 261 to 262 *supra*.

[29] *See* Part II.

weak in comparison to other regimes.[30] However, some case law indicates that breaching an anti-reverse-engineering clause, in particular, can give rise to *both* contract and trade secret liability, because breach of the contract qualifies as an "improper means" of acquiring trade secrets. Some state statutes explicitly identify breach of such a contract as an "improper means" of acquiring trade secrets.[31] The prospect of trade secret liability for what should be only breach of contract is alarming. It means prevailing plaintiffs can obtain trade secret law *remedies*, not just contract law remedies. Moreover, it means that liability can extend to third parties who did not even sign the contract. For example, if someone reverse engineers information about ChatGPT and shares it with someone else, who publishes it on the internet, both of these actors could potentially be liable for trade secret misappropriation. Trade secret liability can even expose some defendants to criminal liability, assuming they have the requisite intent. This is something that contract law alone obviously does not do.[32]

Maintaining some level of legal protection for information goods is important and likely encourages public distribution and disclosure, because without some legal protection, companies might not make information goods available to the wider public at all.[33] But legal protection for information goods can go too far. When contracts are used to generate trade secret law liability, even for information goods that are no longer factually secret—whose information is plainly visible to users or easy to ascertain[34]— this is a problem. Companies should not be free to "contract around" trade secret law rules by banning reverse engineering, imposing noncompetes, or requiring confidentiality even when none exists in fact.[35] This sort of over-protection is bad for

---

[30] Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets As Ip Rights*, 61 STAN. L. REV. 311, 323–24 (2008). *But see* Hrdy & Seaman, *supra* note 25, at 701-702 (discussing tortious interference with contract claims brought against companies that induce others to breach confidentiality agreements).

[31] *See* notes 318 to 319 *supra*.

[32] 18 U.S.C §§ 1831-1832 (2016) (criminal penalties). That said, it is unlikely a prosecutor would bring a criminal claim for someone whose only bad act was to breach a term of use. Similar questions have arisen with the Computer Fraud and Abuse Act (CFAA) and courts have been very skeptical that breaching a terms of use alone would lead to criminal liability under the CFAA. *See* Orin S. Kerr, *Focusing the CFAA in Van Buren,* 2021 SUP. CT. REV. 155, 170-174 (2021).

[33] *See* Lemley, *supra* note 30, at 313, 339-340 (arguing that one benefit of trade secrecy ironically, is to encourage "disclosure" of information inside and outside the firm, because "[w]ithout trade secret law, the efforts those companies take to protect their secrets may be excessive[.]").

[34] *See* note 12 *supra*.

[35] Lemley, *supra* note 30, at 350-51.

innovation and competition policy. It hinders others' ability to build on and improve foundational tools, it harms consumers by reducing choice and raising prices, and it upsets the disclosure goals of the patent system.[36] Patents are supposed to be the main option for products that are sold to the general public and whose inner workings can be discerned by users.[37] Unlike trade secrets, patents require disclosure and after a term of years.[38] Permitting secrecy when patenting should be the only option upsets the balance between secrecy and disclosure through patents.[39] Over-protection could also dramatically hinder regulators' attempts to gain transparency into how AI works and makes decisions. If courts begin to label certain information as "trade secret" or "confidential," this will make it easier to resist regulators' attempts to demand disclosure and make it easier to gain exemptions from public records requests.[40] This could have real impacts on attempts to gain transparency into how generative AIs are developed and trained, and into how they make their decisions.[41]

---

[36] Samuelson & Schotchmer, *supra* note 10, at 1583 (discussing various justifications for reverse engineering). *See also, e.g.,* Joseph P. Fishman & Deepa Varadarajan, *Similar Secrets*, 167 U. PA. L. REV. 1051, 1056-57 (2019) (arguing that trade secret law can place barriers on cumulative innovation especially when it hinders peoples' ability to improve upon products to derive different end products).

[37] Lemley, *supra* note 30, at 341-342.

[38] 35 U.S.C. §§ 112, 154 (2018).

[39] Lemley, *supra* note 30, at 341-342 (arguing that trade secrecy, to the extent it comes with an actual secrecy requirement, "channels" inventions into the patent system that companies could not otherwise keep secret).

[40] *See* Deepa Varadarajan, *Business Secrecy Expansion and FOIA*, 68 UCLA L. REV. 462 (2021) (discussing Supreme Court's recent expansion of types of information that can qualify for an exemption from the Freedom of Information Act).

[41] *See, e.g.,* Frank Pasquale, *The troubling consequences of trade secret protection of search engine rankings*, in THE LAW AND THEORY OF TRADE SECRETS 381–405 (Dreyfuss & Strandburg 2016 eds) (expressing concern regarding trade secrecy protection for search engine algorithms); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018) (trade secrecy protection prevents disclosure of algorithms used in criminal justice system); Sander Vogt, *Show Me Your Secrets: How the Use of Trade Secrets Relates to the Demand for Transparent Artificial Intelligence*, 5 J. ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW 223, 225 (2022) (discussing tension between governments' transparency goals and trade secrets); Ulla-Maija Mylly, *Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information*, INTERNATIONAL REVIEW OF INTELLECTUAL PROPERTY AND COMPETITION LAW (2023) (tension between the EU AI disclosure obligations and trade secrets); *see also* Elizabeth A. Rowe & Nyja Prior, *Procuring Algorithmic Transparency,* 74 ALABAMA LAW REVIEW 303 (2023) (solution to lack of AI transparency in criminal justice system is negotiation with the government over appropriate disclosure terms and conditions).

There is a solution. Courts should not allow generative AI companies to use contracts as the basis for trade secret law claims—as opposed to only breach of contract claims—after factual secrecy[42] has ended. Once a product is made available to the general public on the open market, and embedded information is plainly visible to users or can be easily reverse engineered by them, that information is not a trade secret. The mere presence of confidentiality agreements and anti-reverse engineering clauses cannot magically transform non-secret information into a trade secret.[43] There are various doctrines supporting this premise. The doctrines are complex, but the overall message is quite simple. First, reverse engineering is legal under trade secret law. Second, information that can easily be reverse engineered from a product on the open market is not a trade secret. Third, a company that continues to widely distribute a product to the public that can be quickly and cheaply reverse engineered—whether it's a wheel, a book, software, or a generative AI—cannot logically argue that it has taken "reasonable" measures to keep that product a secret.[44]

These arguments were strong prior to the passage of a federal trade secret statute in 2016, called the Defend Trade Secrets Act ("DTSA").[45] And they are far stronger now. When Congress passed the DTSA in 2016, Congress explicitly included a provision stating that reverse engineering is not an "improper means" of acquiring a trade secret.[46] This language gives rise to many novel preemption arguments that have yet to be raised—let alone tested—but that could tip the balance in favor of reverse engineering and free competition.[47] One of these preemption arguments—which I make in this article—is that state trade secret law cannot make someone liable for reverse engineering because the DTSA specifically states that reverse engineering is not an improper means of acquiring a trade secret.[48] If a state law did so, this would generate a direct conflict

[42] Again, by factual secrecy, I mean not plainly visible or readily ascertainable to users of the product because they can be easily reverse engineered. *See* text and notes 358-363 *supra*.
[43] *See* Part III.
[44] *See* Part III.
[45] *See* citations in note 287 *supra*.
[46] *See* 18 U.S.C. § 1839(6)(B)(2018) ("[T]he term 'improper means'… does not include reverse engineering, independent derivation, or any other lawful means of acquisition[.]").
[47] " 'Preemption' generally describes a situation in which federal law 'preempts,' or supersedes, a state or local law." Camilla A. Hrdy, *The Reemergence of State Anti-Patent Law*, 89 U. COL. L. REV. 133, 158 (2018). *See also* citations in note 411 supra.
[48] *See* discussion in Part III.D.

between state and federal trade secret law, necessitating preemption under the Supremacy Clause of the Constitution.[49]

This doctrinal approach will not ensure the end of ChatGPT's secrets today. Companies can still rely on trade secrecy in the period before reverse engineering becomes readily achievable. Companies can still rely on claims for breach of contract. And companies can still bring trade secret claims against insiders who are under a duty of confidentiality, such as employees, business partners, and sophisticated entities in a negotiated license with the AI originator. This layer of protection is a very good thing. Without some legal protection for their novel generative AI products, companies might not distribute them to the general public at all. But this doctrinal approach will make sure that, once reverse engineering is technically feasible, companies cannot maintain artificial trade secrecy protection forever.

In Part I, I explain that many features of generative AI are currently hidden from users and can that be kept factually secret despite widespread distribution to the public. These features – including algorithms, source code, training data, and potentially a model's' overall technical architecture – will likely benefit from substantial trade secret protection.[50] I posit that some of these features are vulnerable to reverse engineering using methods like data scraping,[51] "model

---

[49] *See* discussion in Part III.D. *See also* U.S. Const. Art. VI ("This Constitution, and the laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the authority of the United States, shall be the supreme law of the land.").

[50] *See* Sharon Sandeen & Tanya Aplin, *Trade secrecy, factual secrecy and the hype surrounding AI* in RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND ARTIFICIAL INTELLIGENCE 442–59 (Abbott, ed., 2022) (discussing how trade secrecy might protect some factually secret features of AI systems used in autonomous vehicles and credit scoring, such as algorithms and source code); *see also* QUINN EMANUEL, THE RISING IMPORTANCE OF TRADE SECRET PROTECTION FOR AI-RELATED INTELLECTUAL PROPERTY (2020) [hereafter "QUINN"] (discussing trade secrecy for AI-related technology); Gregory Gerard Greer, *Artificial Intelligence and Trade Secret Law*, 21 UIC REV. INTELL. PROP. L. J. 252 (2022) (discussing the degree to which trade secret law provides an alternative to patents for protecting AI); Ana Nordberg, *Trade Secrets, Big data and Artificial Intelligence Innovation: a Legal Oxymoron?* in THE HARMONIZATION AND PROTECTION OF TRADE SECRETS IN THE EU: AN APPRAISAL OF THE EU DIRECTIVE (eds. Jens Schovsbo, Timo Minssen, Thomas Riis 2020) (exploring the scope of trade secret protection for AI); Sarah Speight, *Protecting artificial intelligence via trade secrets*, WORLD INTELLECTUAL PROPERTY REVIEW, Sept. 1, 2023 (discussing trade secrecy protection for AI).

[51] Michael Goodyear, Circumscribing the Spider: Trademark Law and the Edge of Data Scraping, 70 Kan. L. Rev. 295, 298-99 (2021) ("'Scraping' consists of using a computer program to inspect, collect, and aggregate data from different webpages.").

extraction attacks,"[52] or other newly-developed techniques that enable users to extract information from generative AI models.[53] This vulnerability will likely increase over time, making it much harder, if not impossible, to maintain factual secrecy. However, in Part II, I show how contracts can be used to generate legal trade secrecy protections for generative AI, even after reverse engineering becomes possible and factual secrecy ends. Using the example of ChatGPT and OpenAI, I discuss the three major clauses in ChatGPT's terms of use, each of which will help keep ChatGPT's inner workings legally protected through contract law, and potentially also trade secret law.

In Part III, I argue that courts should not let the presence of contracts turn what should only be contractual liability into trade secret law liability. There are some software cases that have allowed this, holding that reverse engineering in violation of an anti-reverse engineering clause is an improper means of acquiring trade secrets.[54] But I argue those cases are either wrong, easily distinguishable, or effectively overruled in light of the passage of the DTSA.[55] The case of generative AI provides courts with a novel avenue for revisiting these software precedents and correcting their overprotective stance. Courts should not blindly follow wrong precedents or precedents that have effectively been overruled by the DTSA. They should not be deterred from finding a better path forward. The stakes for competition, innovation, and public transparency are too high. Under a proper interpretation of three major trade secret law doctrines—reverse engineering, not-readily-ascertainable, and reasonable secrecy precautions—contracts cannot be used to maintain trade secrecy in perpetuity for information goods that are widely available to the general public.

I. Turning to Trade Secrecy

Generative AI's like ChatGPT are created by training algorithms[56] on a very large universe of data, called "training data."[57] Generative AI algorithms use this data ("the inputs") to generate

---

[52] *See* notes 206 to 207 *infra* and accompanying text.
[53] *See* Part III.A.
[54] *See* Part III.A.
[55] *See* Part III.D.
[56] An algorithm is a set of instructions for solving a problem or accomplishing some end. Maura Grossman, Paul Grimm, Daniel Brown & Molly Xu, *The GPT Judge: Justice in a Generative AI World,* 23 DUKE LAW & TECH. J. 1, 7 (forthcoming).
[57] The details of the training process, exactly how content is transformed into "data" and how AI is trained on this data, is extremely complex. *See, e.g.,* Pamela Samuelson, *Generative AI Meets*

new content that is at some level derived from or based on the training data ("the outputs").[58] The process of training on massive amounts of data allows the algorithms to learn and improve to the point that they can eventually generate their own content. The outputs are not, generally speaking,[59] the same as the inputs; they are newly generated.[60]

Companies spend millions of dollars developing and training generative AI models.[61] They don't do this for free. They want to make money off their massive investments.[62] Intellectual property will be a crucial way that AI companies can seek to prevent others from copying and competing with them. AI companies' reliance on intellectual property rights, such as copyrights, patents, and trade secrets, will generate serious tensions and potential problems for public policy. For example, what if a competitor wishes to replicate or build on a generative AI model that is protected by one or more forms of intellectual property—can they do so, or must they seek a license?[63] What if an employee of an AI company wishes to leave and work for a competitor—can they share or use information they learned from their original employer?[64] What if a member of

---

Copyright, 381 SCIENCE 158, 159 (2023); Matthew Sag, *Copyright Safety for Generative AI*, 61 HOUSTON LAW REVIEW 295, 313-316 (2023).

[58] I use inputs to refer the information used to train generative AI models, and outputs to refer to the content that a generative AI model produces, often in response to human prompts. *C.f.* Mark Lemley & Bryan Casey, *Fair Learning,* 99 TEX. L. REV. 743, 777 (2020).

[59] That said, some commentators have begun to discuss the phenomenon of so-called "memorization"—where a large language model "memorizes" large amounts of underlying original expression contained in the training data.. *See, e.g*., A. Feder Cooper and James Grimmelmann, The Files are in the Computer: Copyright, Memorization, and Generative AI, Chi. Kent. L. Rev. (forthcoming); Matthew Sag, A response to Lee and Grimmelmann, AI https://matthewsag.com/a-response-to-lee-and-grimmelmann/

[60] *See* citations in note 5 *supra*.

[61] Thomas H. Davenport & Nitin Mittal, How Generative AI Is Changing Creative Work, Harv. Bus. Rev. (Nov. 14, 2022); *see also* Jonathan Vanian, ChatGPT and generative AI are booming, but the costs can be extraordinary, CNBC, March 13, 2023.

[62] OpenAI is in part a nonprofit, but not really. Matt Levine, *OpenAI Is A Strange Nonprofit*, BLOOMBERG OPINION: MONEY STUFF, Nov. 21, 2023.

[63] *See, e.g,* Suzanne Scotchmer, *Standing on the Shoulders of Giants: Cumulative Research and the Patent Law*, 5 J. ECON. PERSP. 29, 32–35 (1991) (assessing whether patents can impede cumulative innovation by later innovators). *See also* Robert P. Merges, *Of Property Rules, Coase, and Intellectual Property,* 94 COLUM. L. REV. 2655, 2655–60 (1994) (discussing transaction costs that can prevent efficient bargaining over patents and other IP rights).

[64] Camilla A. Hrdy & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV. 1, 1 (2021) (discussing trade secrecy as a limitation on employees' ability to share and use information when they leave the job); *see also* Orly Lobel, TALENT WANTS TO BE FREE: WHY WE SHOULD LEARN TO

the public wants to reverse engineer a generative AI model to figure out how it works—can they do so, and under which laws are they liable?[65] Or what if a government wants to regulate generative AI by forcing companies to disclose information about how the models were trained—and what if some or all of this information is considered a trade secret that cannot be freely disclosed to the public? [66]

This article will not address all of these issues, but it will comprehensively discuss the implications of trade secrecy protection for generative AI models. In this part, I argue that many features of generative AI will qualify for protection as trade secrets, despite widespread public distribution. I then argue, however, that in the coming months or years, generative AI is likely to be increasingly vulnerable to reverse engineering. All else being equal, reverse engineering *should* eventually destroy information's trade secret status. In Part II, I go on to show how contracts can be used to extend the life of trade secrecy protection, even after reverse engineering becomes feasible and even after factual secrecy has ended.

A. The Public Distribution Challenge

A trade secret is defined under the Defend Trade Secrets Act (DTSA), and the Uniform Trade Secrets Act (UTSA), as "information"[67] that is not "generally known" or "readily ascertainable through proper means,"[68] that derives "independent economic value" from secrecy

---

LOVE LEAKS, RAIDS, AND FREE RIDING 1-12 (2013) (discussing trade secret law and other legal limitations on employee mobility and knowledge sharing).

[65] Samuelson & Scotchmer, supra note 10, at 1586 (discussing reverse engineering, when "a second comer obtains the innovator's product and starts to disassemble and analyze it to discern of what and how it was made.").

[66] *See* Christopher Morten, *Publicizing Corporate Secrets*, 171 U. PENN. L. REV. 1319, 1319 (2023) (arguing that federal agencies that collect trade secrets in the course of regulating private companies have more power to disclose trade secrets for the public benefit than is commonly believed).

86 Pages Posted: 6 Apr 2022 Last revised: 23 Jan 2024

[67] 18 U.S.C. § 1839(3) (2016). *See also* UTSA § 1 (providing that potentially protectable "information," can include "a formula, pattern, compilation, program, device, method, technique, or process").

[68] 18 U.S.C. § 1839(3) (2016); UTSA § 1.

sufficient to give the owner an actual or "potential" economic advantage over others,[69] and that the putative owner has taken "reasonable measures" to keep secret.[70]

Unlike patent law, trade secret liability is only triggered by some kind of "bad act," called "misappropriation." Misappropriation of a trade secret includes, generally speaking, either using or disclosing a trade secret in breach of a duty to the trade secret holder to maintain its secrecy, or acquiring a trade secret through "improper means."[71] There are a few main categories of civil trade secret defendants.[72] The most common category is current or former employees of the trade secret holder, who breach confidentiality provisions in their employment agreements, as well as potentially third parties who hire those former employees to obtain their trade secrets.[73] The second most-common category is the trade secret holder's business partners, vendors, suppliers, sophisticated licensees, and others who obtained trade secrets while under a legally-cognizable duty of confidentiality, as well as potentially third parties with whom this information is shared.[74] Finally, in the rarest category, essentially *anyone*—both insiders and outsiders—can be liable if they use an "improper means" to acquire trade secrets. [75] There are two main forms of liability based on acquisition by improper means: direct and indirect.[76] Direct liability occurs when someone acquires trade secrets using improper means; indirect liability occurs when someone acquires trade secrets when they know or should know the trade secrets were acquired by improper means.[77]

---

[69] 18 U.S.C. § 1839(3)(B) (2016); UTSA § 1. *See also* Camilla A. Hrdy, *The Value in Secrecy*, 91 FORDHAM L. REV. 557, 559, 568-76 (2022) (explaining various components of the modern independent economic value requirement).

[70] 18 U.S.C. § 1839(3)(A); UTSA § 1.

[71] 18 U.S.C. § 1839(5); UTSA § 1.

[72] These defendants could potentially be liable for criminal trade secret theft as well, assuming they have the requisite intent. 18 U.S.C. §§ 1831-1832 (1996).

[73] 18 U.S.C. § 1839(5)(A)-(B).

[74] 18 U.S.C. § 1839(5)(A)-(B). As I'll discuss, individual users of ChatGPT—as opposed to businesses and developers who obtained Enterprise Licenses—are actually *not* subject to an express confidentiality clause, so it's questionable whether they fall into this category.

[75] 18 U.S.C. § 1839(5)(A)-(B).

[76] *See* ELIZABETH ROWE & SHARON SANDEEN, CASES AND MATERIALS ON TRADE SECRET LAW 282-284 (2012) (discussing direct and indirect pathways to misappropriation).

[77] In all of these situations, use or disclosure of the trade secret would also generate liability, but it is important that acquisition alone can generate liability if improper means are involved. *See generally* 18 U.S.C. § 1839(5) (2018).

The easiest way to protect a generative AI model as a trade secret would be to use it only in-house.[78] However, while some businesses will surely develop generative AI tools for their own internal use,[79] other companies will decide to sell or license these tools to other businesses and developers, and even members of the general public. Companies big and small are already doing this. OpenAI—which has by far the largest lead in this market—distributes ChatGPT to the general public and already has millions of users.[80]

OpenAI publicly distributes ChatGPT in two main ways. First, OpenAI allows individuals—literally anyone—to access ChatGPT, either for free (to get an older model) or on a subscription basis (to access the latest, more advanced model).[81] Individual end users have to sign OpenAI's mass-market terms of use, called simply "Terms of Use."[82] As I'll discuss in depth in Part II, this Terms of Use creates significant limitations on what users can do, though comes with no underlying obligations of confidentiality on either side.

Second, OpenAI allows businesses and developers to purchase an "Enterprise License" that allows licensees to incorporate ChatGPT into their own businesses or make new applications and ed products based on ChatGPT.[83] Enterprise licensees pay negotiated fees and agree to a special terms of use called the "Business Terms," which contains various restrictions on what licensees can do with OpenAI's information and a mutual confidentiality obligation.[84] In exchange, Enterprise licensees gain access to ChatGPT's application programing interface (APIs).[85] This allows them to integrate ChatGPT into their own products and apps and to customize

---

[78] Fromer, *supra* note 14, at 706 (discussing trade secrecy implications of increasing use of AI and automation within businesses).

[79] *See, e.g.,* Andrew McAfee, Daniel Rock, & Erik Brynjolfsson, *How to Capitalize on AI: A guide to realizing its benefits while limiting its risks*, HARVARD BUSINESS REVIEW, 43-48 (Nov.-Dec. 2023) (advising businesses on when and how to adopt generative AI in to improve operations).

[80] Peter Henderson, Xuechen Li, Dan Jurafsky, Tatsunori Hashimoto, Mark A. Lemley, Percy Liang, Foundation Models and Fair Use, August 2023, at 4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4404340

[81] The subscription fee is currently $20 a month. https://openai.com/chatgpt

[82] https://openai.com/policies/terms-of-use

[83] https://openai.com/enterprise *See also* Generative AI End-User License Agreements: What Users Need to Know, JDSUPRA, Aug. 7, 2023 https://www.jdsupra.com/legalnews/generative-ai-end-user-license-3308704/

[84] https://openai.com/policies/business-terms

[85] An application programming interface (API) allows computer programmers to use prewritten computing tasks for use in their own programs. Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183, 1191 (2021). Enterprise licensees get other benefits too. They can get early access to new versions

OpenAI's pre-trained GPT model and tailer it for their own needs.[86] Many companies are incorporating ChatGPT into their preexisting software. The result can be a whole new product. For example, in the legal industry, developers can incorporate ChatGPT technology into their legal research engines.[87] In the sports and wellness industry, the hot new athletics company, "Whoop," has integrated ChatGPT's analytics and chat functionality into its fitness watches. Whoop users can chat with "Whoop Coach," which is powered by ChatGPT, to gain new insights on their health and receive personalized recommendations.[88]

This is all amazing news for users. But widespread public distribution to individuals, businesses, and developers presents a challenge for AI companies that hope to rely on trade secret law. Like software, generative AI is an information good. It embeds information that is plainly visible or potentially accessible to users. This is a problem because trade secrecy requires, well, secrecy. If distributing a product destroys that secrecy, then there is no more protection under trade secret law.[89] As the Supreme Court has made clear, selling—or licensing—a product and keeping trade secrets is perfectly possible, so long as the information does not "lose its secret character."[90] But to the extent information is "self-disclosing," like "the wheel, say, or the paper clip," "inventors of such products will get patent protection or nothing."[91]

---

of ChatGPT before they're available to the general public, and they get more technical support. https://openai.com/blog/introducing-chatgpt-enterprise

[86] Marty Swant, With developer APIs for ChatGPT and Whisper, OpenAI is opening the floodgates with a familiar playbook, DIGIDAY, March 3, 2023, https://digiday.com/media-buying/with-developer-apis-for-chatgpt-and-whisper-openai-is-opening-the-floodgates-with-a-familiar-playbook/; Thomas Davenport & Nitin Mittal, *How Generative AI Is Changing Creative Work*, HARVARD BUSINESS REVIEW, Nov. 14, 2022; Winograd, *supra* note 5, at 617-618; Filip Kaiser & Claudia Slowkik, *How Much Does It Cost to Use GPT Models? GPT-3 Pricing Explained*, 16 February, 2023.

[87] Steven Lerner, "*They're Not Cheap": Law Firm CIOs On Generative AI Tools*, LAW360 PULSE, October 17th, 2023, 2:49 PM EDT. *See also, e.g.,* https://lawdroid.com/copilot/

[88] https://www.theverge.com/2023/9/26/23888984/whoop-coach-chatgpt-ai-fitness

[89] Camilla A. Hrdy & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV. 1 (2021).

[90] Kewanee v. Bicron, 416 U.S. 470, 485, n. 13 (1974). As I discuss in notes 332 to 335 *infra* and accompanying text, the distinction between selling and licensing a product or service is not dispositive for whether trade secret rights are maintained.

[91] *See* Lemley, *supra* note 30, at 313.

Companies wishing to distribute their AI products widely might initially consider obtaining patents instead of relying purely on secrecy.[92] Trade secret law does not create exclusive rights against the world—independent development and reverse engineering are legal.[93] Patents, in contrast, give the owner of the patent the right to stop literally anyone from making, using, or selling the invention in the United States for a period of roughly twenty years for utility patents and fifteen years for design patents.[94] But generative AI companies will likely choose to rely heavily on trade secrecy, rather than relying solely on patents. There are a variety of reasons for this, which I've discussed in detail elsewhere.[95] In the end, the calculus will likely look a lot like it did for software, where companies have often opted for trade secrecy over patenting for hidden information like source code and algorithms.[96] The upshot is that companies are likely to opt for trade secrecy for many types of information relating to generative AI ranging, from code to overall technical architecture.

B. Which Features of Generative AI Can Qualify as Trade Secrets?

Some types of information are more conducive to trade secrecy than others. Scholars often draw a distinction between "self-disclosing" and "non-self-disclosing" products.[97] In general, companies are generally more likely to rely on trade secrecy for non-self-disclosing products, and to obtain patents for self-disclosing products that cannot be kept secret after they are widely

---

[92] Some aspects of generative AI models could be patentable. Examples might include a series of complex algorithms that yield specific technological improvements, a truly novel model architecture, or the software user interface. U.S. PATENT & TRADEMARK OFFICE, PUBLIC VIEWS ON ARTIFICIAL INTELLIGENCE AND INTELLECTUAL PROPERTY POLICY October 2020; *The Story of AI in Patents*, WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO): TECHNOLOGY TRENDS 2019 (2019).

[93] 18 U.S.C. § 1839 § (6).

[94] *See* 35 U.S.C. § 154(a)(2018)*; see also* 35 U.S.C. § 173 (2018) ("Patents for designs shall be granted for the term of 15 years from the date of grant.").

[95] *See* Camilla A. Hrdy, *Trade Secrecy Meets Generative AI*, CHICAGO KENT LAW REVIEW, AI & THE LAW SYMPOSIUM ISSUE (forthcoming).

[96] *C.f.* Katyal, *supra* note, at 1212-1216 (discussing the choice between patent and trade secret with respect to software code and arguing that factors such as term length, conduciveness to secrecy, and costs of patenting shifted the balance towards trade secrecy for software). *See also* QUINN, *supra,* at 1 (discussing AI's amenability to trade secrecy).

[97] *See* Lemley, *supra* note 30, at 313.

distributed.[98] In Part II, I will challenge this notion, because in fact contracts can be used to maintain legal secrecy even after factual secrecy has dissipated.[99] But when discussing *factual* secrecy, as opposed to legal secrecy, the distinction between self-disclosing and non-self-disclosing products is very useful.

Some features of generative AI are self-disclosing. The way the user interface of ChatGPT looks, for example, or the *outputs* that a user sees when they ask ChatGPT a question. This information cannot, all else being equal, be protected as a trade secret because it is generally known or readily ascertainable.[100] But many features of a generative AI are non-self-disclosing or only *partially* self-disclosing. They can be kept factually secret even after a generative AI product is widely distributed on the open market, because they are not plainly visible to users of the product and are hard (though not impossible) to reverse engineer.[101]

Importantly, not all developers choose secrecy. Some generative AIs are fully released. They are "open-source."[102] An example is Meta's Llama.[103] But many generative AI models, including ChatGPT, are "closed-source." They are only accessible to the general public through a user interface.[104] "Most users of generative AI do not interact with a model directly. Instead, they use an interface to a system, in which the model is just one of several embedded, inter-operating

---

[98] *See, e.g.,* Tabrez Y. Ebrahim, *Artificial Intelligence Inventions and Patent Disclosure* 125 PENN ST. L. REV. 147, 183-184 (2020).

[99] *Accord* Lemley, *supra* note 30, at 350-51; Varadarajan, *supra* note 19, at 1567.

[100] Even here, there is a chance contracts can be used to generate secrecy obligations that turn this into a trade secret. This is not a correct view of the law—but there is case law that has allowed company to protect even plainly visible features by imposing confidentiality obligations. *See, e.g.,* text and notes 370 to 373, 390 to 395 *supra*.

[101] Continuing secrecy for publicly distributed products is not unique to generative AI. Pharmaceutical drugs, for example, also benefit from continuing secrecy even after public sale and patenting of key components. *C.f.* W. Nicholson Price II & Arti K. Rai, *Manufacturing Barriers to Biologics Competition and Innovation*, 101 IOWA L. REV. 1023, 1042-1048 (2016).

[102] Lee, Cooper, & Grimmelmann, *supra* note 5, at 41.

[103] Meta released code and other details about development, including the "training recipes" which are available on Github. https://ai.meta.com/blog/code-llama-large-language-model-coding/ Llama, though open-source in the sense of releasing code and training data, does have a license agreement that users must sign. https://ai.meta.com/llama/license/

[104] Lee, Cooper, & Grimmelmann, *supra* note 5, at 5.

components."[105] In other words, users do not actually get access to the model at all. They have access to the software through which the model is deployed.[106]

This closed-source structure makes these models particularly amenable to trade secrecy. Several features cannot be accessed by ordinary users at all.

1. Algorithms

Generative AI functions by employing algorithms, and it does so in many different respects. Algorithms are used to train generative AI models and are also used in the software systems that AI models are embedded in.[107] Algorithms are what Charlotte Tschider calls "natural" trade secrets. They are not generally revealed to end users; they may not be comprehensible even to those who created them; and they tend to be survive attempts at reverse engineering.[108] According to one commentator, "[i]n today's algorithmic world, trade secrets are the best form of intellectual property protection for algorithms"; algorithms, as "mathematical instructions," are "ineligible for patent and copyright protections. Therefore, trade secret law is the only option for algorithms, and secrecy is the only way to keep others from using your created algorithms." [109] This is an over-simplification because some complex algorithms may in fact be patentable.[110] But the point is well taken. Trade secrets are a comparatively effective way to protect algorithms. Unlike for patents, there is no question that even a single algorithm can be appropriate subject matter, assuming it meets the elements. Trade secret law protects "information" writ large.[111] Unlike for patents, trade secret law also does not require the creator of information to be a human being, which could be relevant for algorithms that are created by generative AI itself.[112]

---

[105] *Id*. at 15-16.
[106] *Id*. at 41-42.
[107] Tschider, *supra* note 5, at 687-688. *See, e.g.,* Vogt, *supra* note 40 ("Algorithms serve as the foundational structure of almost any AI system.").
[108] Tschider, *supra* note 5, at 709-10 (arguing that "complex algorithms" are "natural trade secrets[.]"). *See also* W. Nicholson Price II*, Regulating Black-Box Medicine*, 116 MICH. L. REV. 421, 430 (2017) (discussing opacity of algorithms); Price & Rai, *supra* note 9, at 790 (same).
[109] Greer, *supra*, at 263.
[110] A series of complex algorithms that yields specific technological improvements, a truly novel model architecture, or the software user interface might be patentable. "USPTO VIEWS," note 92 *supra* . The patent office has issued many AI patents already. *See, e.g., The Story of AI in Patents*, WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO).
[111] 18 U.S.C. § 1839(3) (2016); UTSA, § 1.
[112] 18 U.S.C. § 1839(4) (2016).

Courts have frequently protected algorithms related to AI in the past.[113] But a few challenges may arise. One is trade secret law's "identification" requirement. When a party claims a specific algorithm as a trade secret, courts often require them to specifically identify this algorithm and share it with the court and the other party.[114] For example, in RealD Spark LLC v. Microsoft Corp, the plaintiff, RealD, asserted that it owned trade secrets in "image recognition algorithms," but did not provide the actual algorithm to the court in response defendant Microsoft's motion for production.[115] The court concluded that because the plaintiff was alleging that "a particular algorithm" was a trade secret—as opposed to a general concept for an algorithm—"the algorithm itself should be disclosed."[116]

Companies naturally may not wish to disclose their algorithms. Courts can ensure secrecy for these disclosures, placing the parties under protective orders; sealing some or all of the record; or redacting portions of their orders to avoid disclosing trade secrets.[117] For example, in *RealD Spark*, the court ordered RealD to "provide the 'image recognition algorithms' it asserts are trade secrets to Microsoft," but it also ordered the parties to label the algorithms as "HIGHLY CONFIDENTIAL—ATTORNEYS' EYES ONLY" pursuant to the protective order the court had put in place.[118]

Another potential problem, recently discussed by John Villasenor, is that some of the algorithms used in generative AI may have been generated *by the AI itself*.[119] "The complexity in

---

[113] *See, e.g.,* Glover v. Imubit, Inc., 2019 Tex. Dist. LEXIS 72440, *1-2 (N.D. Ill. 2023) (finding employer would likely prevail in proving it owned trade secrets in "processes, procedures, algorithms, and technologies relating to artificial intelligence and machine learning…").

[114] *See* The Sedona Conference, *Commentary on the Proper Identification of Asserted Trade. Secrets in Misappropriation Cases*, 22 SEDONA CONF. J. 223 (2021). *See also, e.g.,* Torsh, Inc. v. Audio Enhancement, Inc., 2023 U.S. Dist. LEXIS 204359, *15-16 (La. E. D. Ct. 2023) ("If plaintiff contends that higher-level architecture of the software is a trade secret, it must detail the combination of the specific algorithms employed.").

[115] Microsoft also provided evidence, like old patents, showing that "face-recognition algorithms" were long known to people in the field. Reald Spark LLC v. Microsoft Corp., 2023 U.S. Dist. LEXIS 80221, * 11-12 (D.Ct. W.D. Wash. 2023).

[116] Reald Spark LLC, 2023 U.S. Dist. LEXIS 80221, at * 11-12.

[117] *See* UTSA, § 5. *See also, e.g.,* Apex.AI, Inc. v. Langmead, No. 5:23-CV-02230-BLF, 2023 WL 4157629, at *1–2, *3-4 (N.D. Cal. June 23, 2023) (granting motion to seal portions of application for TRO in case involving software tools for use in autonomous and software-defined vehicles).

[118] Reald Spark LLC, 2023 U.S. Dist. LEXIS 80221, at * 14.

[119] John Villasenor, *Artificial Intelligence, Trade Secrets, and the Challenge of Transparency*, Unpublished Manuscript, on file with the author. *See also* Camilla Hrdy, *Beyond the AI Black*

the trade secret analysis," Villasenor writes, "lies in the fact that, unlike the chocolate-maker who identifies a way to refine a recipe, the AI system designer may not initially be aware of what the AI-generated algorithmic improvements are..."[120] Villasenor rightly concludes that this issue is not fatal. Trade secret law has *never* required the owner of the trade secret to itself have full knowledge of the secret. Indeed, this is the assumption underlying almost all employee-generated trade secrets. Trade secrets are created by human employees but likely owned by a corporation.[121] The key, rather, is that trade secret owners effectively describe these algorithms in sufficient when enforcing them. They must provide enough detail about the algorithms for the other side and the court to determine their trade secrecy status—even if they may not fully understand the details of the information they seek to protect.[122]

That said, a plaintiff will need to demonstrate that the employee accused of taking the algorithms actually had access to them. It would not be enough to allude to the fact that an employee worked at a company where algorithms were being developed; the employee must have been in a position to take them. A version of this issue arose in DigitalGlobe, Inc. v. Paladino. The plaintiffs—companies engaged in "satellite mapping" using "geospatial predictive analysis"[123]—accused a former employee (Paladino) of misappropriating trade secrets, including "algorithms and methods for applying machine learning to large volumes of geospatial data." [124] The court denied plaintiffs' motion for a preliminary injunction, however, because plaintiffs did not show that Paladino had access to the algorithms and methods at issue.[125] The Plaintiff's CEO stated in his deposition that Paladino was on a team that was focused on "advances and artificial intelligence and machine learning" but did not give evidence that Paladino himself had access. [126]

Box: Links to Articles and Excerpts From Interview With Charlotte Tschider, WRITTEN DESCRIPTION, Jan. 23, 2024 https://writtendescription.blogspot.com/2024/01/beyond-ai-black-box-links-to-articles.html

[120] John Villasenor, *Artificial Intelligence, Trade Secrets, and the Challenge of Transparency*, Unpublished Manuscript, on file with the author.

[121] *See* Catherine Fisk, *Removing the 'Fuel of Interest' from the 'Fire of Genius': Law and the Employee-Inventor, 1830-1930*, 65 U. CHI. L. REV. 1127, 1127 (1998).

[122] John Villasenor, *Artificial Intelligence, Trade Secrets, and the Challenge of Transparency*, Unpublished Manuscript, on file with the author.

[123] DigitalGlobe, Inc. v. Paladino, 269 F. Supp. 3d 1112, 1116 -17 (D. Colo. 2017)

[124] *Id*. at 1116-1118.

[125] *Id*. at 1126.

[126] *Id*. at 1126-1127.

Finally, at the end of the day, algorithms still have to meet the elements of a trade secret. They cannot be generally known in the field and must derive "independent economic value" from secrecy.[127] This could be a challenge. For example, what if others outside the company would not understand or be able to benefit from the algorithm?[128] What if an algorithm has become outdated, such as that any economic value it had is gone?[129] On the flip side, what if algorithms are not *yet* developed at all?[130]

This exact issue—failure to prove an algorithm derived economic value from secrecy—presented a hurdle for the plaintiff in the high-profile case, Neural Magic v. Meta.[131] The plaintiff Neural Magic had been working on developing various algorithms that would allow machine learning-based neural networks to run faster on standard computer processors. Neural Magic hired a computer scientist named Aleksander Zlateski, who eventually left Neural Magic for defendant Meta. At the request of another employee at Meta, Zlateski wrote source code which allegedly incorporated Neural Magic's algorithm innovations for running neural networks. Zlateski's colleague re-wrote this code and published the code on GitHub, an open-source software development platform. Neural Magic alleged that the code Zlateski shared was based on Neural Magic algorithms, which Zlateski developed while employed at Neural Magic. [132] In the early stages of the litigation, the district court denied plaintiff Neural Magic's request for a preliminary injunction because it appeared that "the approaches and concepts" that Neural Magic asserted to be trade secrets were likely "widely known by people of skill in the industry" and "known and used by" Zlateski prior to joining Neural Magic. Moreover, the court wrote, it appears "Neural Magic does not derive any economic value from them[,]" given that Neural Magic "does not yet have a product on the market or customers and has not earned any revenue from the sales of any product."[133] The court therefore initially denied Neural Magic's required for preliminary

[127] Hrdy, *supra* note 69, at 568-76.
[128] Sandeen & Aplin, *supra*, at 14.
[129] Fox Sports Net N., L.L.C. v. Minnesota Twins P'ship, 319 F.3d 329, 336 (8th Cir. 2003) ("[O]bsolete information cannot form the basis for a trade secret claim because the information has no economic value.").
[130] Hrdy, *supra* note 69, at 602-604 (noting that courts have sometimes found early-stage prototypes that are not yet on the market lack independent economic value).
[131] Neural Magic, Inc. v. Facebook, Inc., No. CV 20-10444-DJC, 2020 WL 13819257, at *4–5 (D. Mass. May 29, 2020).
[132] *Neural Magic, Inc*., 2020 WL 13819257, at *2–4.
[133] *Id.* at *4–5.

injunction, due partly to Neural Magic's failure to prove that its algorithms possessed the requisite independent economic value due to secrecy.[134] That said, the case did eventually proceed, and seemed like it would go to trial.[135] The case settled this past summer.[136]

2. Source Code

Generative AI, like software, relies in large part on code. In the case of ChatGPT, code is used both in underlying large language model and for the software system constituting the user interface. Both are closed- source and not released to the public.[137] Source code is a classic trade secret. It can be kept factually secret even after the software is made available to end users. Technologically speaking, this is because companies can sell software in a way that only reveals the "object code" or "executable code"—which can only be read by machines— but not the source code—which can be read by human coders.[138] Thus, source code is kept as a trade secret, even if the object code is not.[139]

Importantly, companies can also rely on copyright law to protect source code. But trade secret claims will not generally be preempted so long as there is an additional allegation besides copying, such as breach of a duty or using improper means to acquire the source code. [140] Trade secrecy provides an important additional layer of protection for code. Copyright law can potentially be used to prohibit others from copying source code that is utilized in implementing

---

[134] *Id*. at *5.
[135] Neural Magic, Inc. v. Meta Platforms, Inc., 659 F. Supp. 3d 138 (D. Mass. 2023).
[136] Blake Brittain, Meta settles startup's lawsuit over artificial-intelligence trade secrets, REUTERS, Aug. 9, 2023, https://www.reuters.com/legal/transactional/meta-settles-startups-lawsuit-over-artificial-intelligence-trade-secrets-2023-08-09/
[137] *See* note 14 *supra*.
[138] Object code is the result of compiling source code, which turns human-readable code into machine-readable code. Executable code is a type of object code that is ready to be executed directly by the computer's operating system. *See* Katyal, *supra* note at 1193-1195, 1207-1208, 1229-1239. *See also*, e.g., Fabkom, Inc. v. R.W. Smith & Associates, Inc., 1996 WL 531873, at *3-4, 7-9 (SDNY 1996) (plaintiff took reasonable measures to preserve secrecy of source code because the software was "distributed to its customers only in its executable object code form" and plaintiff provided the software "to clients only after they have signed a confidentiality agreement.").
[139] That said, if the object code is *also* kept secret from users, then it can potentially be a trade secret. Trandes Corp. v. Guy F. Atkinson Co., 996 F.2d 655, 662-664, note 8 (4th Cir. 1993).
[140] *See, e.g.,* Katyal, *supra* note, at 1207, 1228; Lim, *supra*, at 835. *See also* Computer Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 719–717 (2d Cir. 1992) (17 U.S.C. § 301 did not preempt trade secret claim).

generative AI or related software.[141] But copyright law only protects "substantially similar" iterations of the code, and it also includes a "fair use" defense. Trade secret law has neither of these limitations. As Deepa Varadarajan has repeatedly emphasized, trade secret law protects the information writ large, regardless of whether the defendant's end product is different from the information that the defendant obtained from the plaintiff,[142] and trade secret law contains no "fair use" defense.[143] This means that if a someone obtains access to trade secret source code—whether through their employment or as an end user through a product—they can copy the information to make a completely new product, for any purpose, yet still liable under trade secret law.

An oft-cited case recognizing that trade secrecy is available for source code, along with copyright protection, is Data Gen. Corp. v. Grumman Sys. Support Corp. The plaintiff (Data General) sued defendant Grumman Systems Support Corporation (Grumman), alleging that defendant stole source code embedded in Data General's software. A district court, applying Massachusetts common law in 1994, upheld a jury verdict finding that the source code was protectable as a trade secret, since access to the software was restricted, even those who obtained the software "were unable to discover" the code given that it "was distributed only in its object code form, which is essentially unintelligible to humans."[144]

There is some debate over whether source code is still as secret-in-fact as it was in 1994. Some scholars have asserted that discerning source code from object code is hard, costly, and time consuming,[145] but Samuel J. LaRoque argues that object code can now more readily discovered using a process called "disassembly" or "decompilation."[146] La Roque argues this process is

---

[141] 17 U.S.C. § 101 (defining literary work in a way that includes computer code). *See also, e.g.,* Katyal, *supra*, at 1198-1201 (discussing rise of copyright protection for code). *See also* Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183 (2021) (fair use for software APIs).

[142] *See, e.g.,* Joseph P. Fishman & Deepa Varadarajan, *Similar Secrets*, 167 U. PA. L. REV. 1051, 1056-57 (2019)

[143] Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401 (2014).

[144] Data Gen. Corp. v. Grumman Sys. Support Corp., 825 F. Supp. 340, 359 (D. Mass. 1993), affirmed in Data Gen. Corp. v. Grumman Sys. Support Corp., 36 F.3d 1147 (1st Cir. 1994). *See also, e.g.,* Amimon Inc. v. Shenzhen Hollyland Tech Co., 2021 U.S. Dist. LEXIS 229162, *1-2 (S.D.N.Y. 2021).

[145] Lemley, *supra* note 11, at 1244; Katyal, *supra,* at 1216, 1234.

[146] Samuel J. LaRoque, *Reverse Engineering and Trade Secrets in the Post-Alice World*, 66 KAN. L. REV. 427, 438-439 (2017). *See also, e.g.,* Fromer, *supra* note 14, at 716 ("[E]ven though businesses could keep their source code secret, sales of the corresponding object code have left the source code plausibly vulnerable to legitimate discovery via reverse engineering.").

getting easier and easier, and that companies may have to reexamine their assumption that they can keep source code secret by revealing only object code.[147] There is case law, albeit very fact-specific, supporting the view that object code can sometimes easily be decompiled to discern source code.[148]

Setting aside the risk of reverse engineering for now, there is plentiful case law suggesting that source code used to implement generative AI can be a trade secret.[149] For example, in the recent case Apex.AI, Inc. v. Langmead, the plaintiff Apex.AI, which develops "software tools for use in autonomous vehicles and software-defined vehicles," obtained a temporary restraining order (TRO) against a former consultant—who was hired to develop an automated process for plaintiff and "had access to virtually all of ApexAI's software, source code, and other intellectual property"[150]— after he began marketing the process through his own company, allegedly "plac[cing] Apex.AI's proprietary source code" on his own platform.[151] The court found Apex.AI. likely owned trade secrets in its products' "source code, and related technology," and ordered the defendant to stop using or disclosing ApexAI's source code and other asserted trade secrets pending further litigation.[152]

As with algorithms, the specific source code will likely have to be revealed to the court and the other party. Surviving a motion to dismiss probably will not necessitate revealing the source code.[153] But as the case proceeds through discovery, the plaintiff will probably have to share the

---

[147] LaRoque, *supra*, at 438.

[148] *See* Arkeyo, LLC v. Cummins Allison Corp., 342 F. Supp. 3d 622, 630 (E.D. Pa. 2017) (plaintiff lost trade secrecy in software when it left a zip file on the internet that "contained mostly executable code" rather than "human readable source code," because the executable code "could be translated into source code through the relatively simple process of decompilation—a process as simple as translating French into English.").

[149] *See, e.g., NEXT Payment Sols., Inc. v. CLEAResults Consulting, Inc.*, No. 17 C 8829, 2018 WL 3637356, at *13 (N.D. Ill. July 31, 2018) (finding computer software was a trade secret where it was confidential and plaintiffs "derived economic value from [its software] not being generally known or accessible.").

[150] Apex.AI, Inc. v. Langmead, 2023 U.S. Dist. LEXIS 82291, *1-2 (N.D. Cal. May 10, 2023).

[151] *Id*. at * 2.

[152] *Id*. at * 3, 5-6 (granting motion for ex parte TRO in part and order to show cause why preliminary injunction should not issue).

[153] *See, e.g.,* AutoMed Techs., Inc. v. Eller, 160 F. Supp. 2d 915, 920–21 (N.D. Ill. 2001) (noting that "plaintiff will ultimately need to identify which specific designs, software or research defendants allegedly misappropriated.").

source code in great detail.[154] As one court recently put it, "[i]f plaintiff alleges misappropriation of source code, it must identify the specific lines of code or programs claimed to be a trade secret by, for example, printing out the code on paper with numbered lines and identifying the allegedly misappropriated lines by page and line number …"[155] Again, these disclosures can all be done pursuant to a protective order and other precautionary measures.[156]

3. Training Data

Generative AI's most important trade secrets may be the training data that is used to train the models. This could include the training data itself, and also information regarding which training data was used, or which training data should be used, to train a model.

"[Generative AI's] rely on large amounts of data to 'learn' how to perform tasks and make decisions. This data, referred to as 'training data,' is used to train AI algorithms to recognize patterns and make predictions based on those patterns. The accuracy of the AI algorithm is directly dependent on the quality and quantity of the training data that it is exposed to."[157] Identifying, collecting, and obtaining permissions for training data "is expensive. It requires a substantial investment of multiple resources: time, data storage, and computing power."[158] This is not a simple process. Creating a training dataset entails many steps: collecting individual works; converting those works into "data" ("digitally encoded files in standard, known formats"); and then compiling that data into "vast and carefully structured collections of related data."[159] The process may also entail securing licenses, either to individual works or to entire datasets. [160]

Keeping training datasets secret is likely to provide developers of generative AI of with a major economic advantage over would-be competitors. Likewise, information about precisely which data was used, or which datasets work best, could be very valuable. The developer of an

---

[154] *Torsh, Inc*., 2023 U.S. Dist. LEXIS 204359 at *11-12. *Compare* T2 Modus, LLC v. Williams-Arowolo, 2023 U.S. Dist. LEXIS 170656, *18-19 (E.D. Tex. 2023) (not requiring plaintiff to produce the source code in response to Request for Production).
[155] *Torsh, Inc*., 2023 U.S. Dist. LEXIS 204359 at *15-16.
[156] *Reald Spark LLC*, 2023 U.S. Dist. LEXIS 80221, at * 20.
[157] Andrew Torrence & Bill Tomlinson, *Training Is Everything: Artificial Intelligence, Copyright, and Fair Training*, DICKINSON LAW REVIEW, (forthcoming 2023), at 6, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4437680&__cf_chl_tk=P_bRiQx8krXjzg2oO7YBglkqGumTYTaATCtB3CTHlKU-1704647560-0-gaNycGzNETs
[158] Cooper, Lee, & Grimmelmann, *supra* note 5, at 35-36.
[159] *Id*. at 4.
[160] *Id*. at 32-35.

AI model is likely to have significant information about which data was used, which is technically distinct from the data itself. Importantly, sometimes the owner of the dataset is *not* be the AI developer.[161] The owner of the training dataset may be a totally different company.[162] One or both of these entities could keep the training datasets as trade secrets, so long as they take the necessary measures to preserve secrecy and the datasets do not become generally known across the industry. [163]

There are potential challenges to protecting datasets as trade secrets. As Sharon Sandeen and Tanya Aplin observe, some of the training data is "publicly accessible through public records, directories, or registers, or through search engines and social media platforms."[164] It is also possible to ascertain at least some of the works that were used to train a generative AI model.[165]

That said, the fact that some training data is public is not fatal to trade secrecy. An entire training dataset can still be protectable as a "combination" trade secret, even if specific pieces of that information are public or can be easily discerned.[166] The trade secrecy rules are similar to copyright law's treatment of "compilations."[167] Courts apply divergent standards for protecting combination secrets, but the general rule that the whole combination must impart an economic advantage due to its secrecy.[168] This is similar in practice to how copyright law treats compilations

---

[161] 18 U.S.C. § 1839(4) (defining "owner" of trade secret).

[162] Cooper, Lee, & Grimmelmann, *supra* note 5, at 4-5 (discussing different actors along AI supply chain).

[163] *See* Hrdy, *supra* note 69, at 579 ("Multiple firms can possess the same trade secret and use it competitively in private, so long as so long as it is not "generally known" to people in the industry.").

[164] Sandeen & Aplin, *supra,* at 11.

[165] There are emerging resources that can be used to figure out whether a work was used to train an AI. Andrew Wilson-Bushell, *Training generative AI: separating fact from fiction*, WORD INTELLECTUAL PROPERTY REVIEW, Jan. 9, 2023, at 1. *See also* https://haveibeentrained.com/ Also, as I discuss *infra*, "model extraction attacks" can be used to ascertain some of the training data. *See* Sag, *supra*, at 326-327.

[166] 18 U.S.C. § 1839 (3)(2016) (specifying that trade secrets can encompass information such as "compilations").

[167] Cooper, Lee, & Grimmelmann, *supra* note 5, at 33-34, 52-53.

[168] *See, e.g.,* Catalyst & Chem. Servs., Inc. v. Global Ground Support, 350 F.Supp.2d 1, 8-10 (D.D.C.2004), aff'd 173 Fed. Appx. 825 (Fed Cir. 2006) ("[A] combination qualifies as a trade secret only when there is an added value to the combination over the value of the individual parameters, i.e., when 'the whole is more than the sum of the parts.' ") (applying District of Columbia UTSA) (internal citations omitted).

of facts: The individual facts are not protectable, but the overall arrangement and selection can be.[169]

Proving that a whole combination of training data has value due to its secrecy might be difficult if most or all of the data is public. To quote Sandeen and Aplin, "if almost all of the information is public and easy to ascertain, it will be very hard to argue that the combination derives independent economic value from secrecy."[170] But courts are often lenient about protecting combinations of otherwise-public information as trade secrets. For example, one recent case held spreadsheets can be protectable as trade secrets, even if they contain information that could be obtained from public sources.[171]

To the extent that a training dataset is deemed protectable *only* as a combination trade secret, this protection would come with serious limitations. For example, defendants might not be liable if they use or disclose only *parts* of the combination of training data. True, unlike copyright law, trade secret law generally extends liability to end products that are "derived from" trade secrets—even if the end product is quite different from the starting information.[172] However, for combination trade secrets, protection is effectively weaker, because many courts hold that acquiring, using, or disclosing *only some* of the information making up the combination is not actionable.[173] This could be a significant limitation. For example, imagine a former employee of OpenAI leaves their job to go work at Google, and they use *some*, but not all, of the data on which ChatGPT was trained to develop new generative AI for Google. The employee should not be liable

[169] Feist Publications, Inc. v. Rural Telephone Service Co., 499 US 340, 345, 349 (1991); *see also, e.g.,* Thomson Reuters Enter. Ctr. Gmbh v. Ross Intelligence Inc., 1:20-cv-613-SB (U.S. D. Ct. D. Del. Sep. 25, 2023).
[170] Sandeen & Aplin, *supra*, at 13-14. *See also* Hrdy, *supra* note 69, at 598.
[171] *See* Allstate Ins. Co. v. Fougere No. 22-1258 (1st Cir. Aug. 29, 2023).
[172] *See* note 278 *infra*.
[173] There is significant disagreement in the case law on this point. *Compare* American Airlines, Inc. v. KLM Royal Dutch Airlines, Inc. 114 F.3d 108, 109-111 (8th Cir. 1997) (defendant not be liable because had access to only four of the five elements claimed as trade secret) *with* Caudill Seed & Warehouse Co. v. Jarrow Formulas, Inc., 53 F.4th 368, 384–86 (6th Cir. 2022) (discussing split among authorities over whether trade-secret law requires a plaintiff to show "acquisition and use of the entirety of a combination trade secret" and rejecting defendant's argument "that trade-secrets law requires showing acquisition of each atom of a combination trade secret[.]").

for using only part of OpenAI's training dataset, assuming that the combination of all the training data is all that is asserted as a trade secret.[174]

That said, there will likely be a lot of information about what data was used to train a model that is secret in its own right, and that is economically valuable due to not being known. If the OpenAI employee in the example above shares a small amount of information with Google about how ChatGPT was trained, this information could still be economically valuable due to secrecy, even if it only gives an incomplete picture. In that case, there would be no need to rely on a combination trade secret.

Another challenge, again, is identification and the disclosure risks this entails. Depending on precisely what is claimed as a trade secret, the plaintiff might have to reveal the entire training dataset to the court and the other side. For example, in RealD Spark LLC v. Microsoft Corp., mentioned above, the plaintiff, RealD, alleged that the "[d]atasets to support SocialEyes' image recognition methods" were trade secrets. During discovery, RealD provided a "nearly 3,000-page range" of documents to identify its training datasets. The court accepted the plaintiff's assertion that it "took pains to collect a large and varied set of data to train its algorithms," but this identification was not sufficiently specific. At minimum, the plaintiff needed to explain where exactly the training data was discussed within those 3,000 pages, assuming it was there at all.[175] Again, even with a protective order in place, this creates a risk of disclosure that could deter some companies from bringing these lawsuits.

4. Overall System Architecture

Another potentially valuable trade secret that an organization can protect is the overall design of a specific generative AI.[176] How a specific generative AI was developed and trained—what Katherine Lee, A. Feder Cooper, and James Grimmelmann call the overall "technical architecture"[177]— can potentially be a trade secret, to the extent that it derives independent economic value from secrecy and is the subject of reasonable secrecy precautions.

---

[174] Charles Tait Graves and Alexander Macgillivray, *Combination Trade Secrets and the Logic of Intellectual Property*, 20 SANTA CLARA HIGH TECH. L.J. 261, 261 (2004) ("[To] have misappropriated a combination trade secret, a defendant must know about and intend to misappropriate the entire combination, and not have independently derived it.").

[175] Reald Spark LLC v. Microsoft Corp., 2023 U.S. Dist. LEXIS 80221, * 15-17 (D.Ct. W.D. Wash. 2023).

[176] Sandeen & Aplin, *supra*, at 9-10. *See also* QUINN, *supra* note 50 at 6-8.

[177] Lee, Cooper, & Grimmelman, *supra* note 5, at 4.

A model's technical architecture can have several components, depending on which form of model it is and how it was developed.[178] When building a large language model, for example, a "neural network" is typically used. A neural network is a computational model consisting of an interconnected network of nodes ("neurons") that, in a sense, mimics the human brain.[179] Building such a neural network entails an extraordinary number of choices. A key choice is which "weight parameters" to use in determining the strength of the connections between the nodes. Weight parameters can vary tremendously. More sophisticated models can have "billions of parameters (with trillions of connections between them)."[180] This information could be a trade secret, in whole or in part, to the extent that it derives independent economic value from secrecy. In some situations, even the simple fact that a neural network was utilized could help others to build a similar or improved model. Knowing which weight parameters were used to build that network would be more valuable still.

That said, a key challenge in these cases will be distinguishing specific details about model architecture—which may be a trade secret—from that which is already well known in the industry. As Lee, Cooper and Grimmelmann write, "[w]hile "generative AI" might be a relatively new term-of-art, a lot of the technology that powers today's generative-AI systems has a long history."[181] Some of the fundamental technology is concertedly not a trade secret. For example, the "transformer" architecture, which was an important new development for large language models like ChatGPT, has already been published; Google has obtained a patent for this technology.[182] There are surely many trade secrets left over, even after publication of the basic transformer architecture,[183] but some plaintiffs may claim to own trade secrets in what is in fact general

[178] Lee, Cooper, & Grimmelmann, *supra* note 5, at 11 ("Different model architectures vary widely in size and complexity, and in turn have different capabilities for encoding relationships in the data.").
[179] Tschider, *supra* note 5, at 689-690; Lee, Cooper, & Grimmelmann, *supra* note 5, at 10-11.
[180] Lee, Cooper, & Grimmelmann, *supra* note 5, at 10-11 ("[A] model architecture is also composed of vectors of numbers, which are typically called parameters or weights…. Simpler, more traditional statistical models like linear regression have relatively few parameters, while modern-day deep neural networks can have billions of parameters (with trillions of connections between them).").
[181] Lee, Cooper, & Grimmelmann, *supra* note 5, at 21.
[182] U.S. Patent No. 10,452,978 (granted 2019). *See also* Alex Zhavoronkov, Can Google Challenge OpenAI With Self-Attention Patents? FORBES Jan. 23, 2023.
[183] Lee, Cooper, & Grimmelmann, *supra* note 5,, at 22-24. *See also id*. at 27 (mentioning "publication of the transformer architecture in 2017").

knowledge. Courts will have to do the work of sorting through these claims and distinguishing the good from the bad ones.

Several AI-related cases have been dismissed due to the fact that plaintiffs provided generic descriptions of AI technology, which courts found could not possibly be secrets. For example, Lamont v. David Krane, Google Ventures, et al, a pro se plaintiff alleged that Google Ventures relied on plaintiff's trade secrets when Google Ventures moved to "artificially intelligent solutions in its Cloud platform" and "invested $4.5M on artificial intelligence research in Montreal."[184] However, the plaintiff's vague descriptions of the asserted trade secrets—like "the use of an Expert System," "the use of a Knowledge Base to insert bad choices," "the use of inference engines to reiterate another choice"—were patently insufficient to show that Google Ventures relied upon anything in particular that it obtained from the plaintiff, or that was not a matter of general knowledge.[185]

Companies can also own "modification" trade secrets relating to model architecture.[186] After initial development and training, generative AI's are often refined and improved. As Lee, Cooper, and Grimmelmann explain, "[t]he model that results from [the] initial training process is called a "base" or "pre-trained model," because it is often just a starting point. A model can also be fine-tuned to improve its performance or adapt it to a specific problem domain. This process, too, involves extensive choices — and it need not be carried out by the same entity that did the initial training."[187] For example, third-party developers who have access to a pre-trained generative AI like ChatGPT can build on the pre-trained model. They can "fine-tune" it "based on their own data, creating a custom version tailored to their application."[188] Once adopted within a specific business, models will likely have to be updated to achieve optimal performance.[189] Any of these modifications and improvements can themselves be protected as trade secrets, because they are likely to enhance the overall value of the model to the owner and to others. These modification secrets may be owned by a different entity from the entity that developed the original model. The

[184] Lamont v. Krane, 2019 U.S. Dist. LEXIS 81451, *8-9 (N.D.Cal. 2019).
[185] *Id*. at *3. *See also* Loop AI Labs Inc. v. Gatti, 195 F. Supp. 3d 1107, 1114-1115 (N.D.Cal. 2016) (dismissing case when plaintiff failed to provide enough details to distinguish asserted AI-related trade secrets from general knowledge in trade).
[186] Metallurgical Indus. Inc. v. Fourtek, Inc., 790 F.2d 1195, 1199 (5th Cir. 1986).
[187] Lee, Cooper, & Grimmelmann, *supra* note 5, at 4; *see also id*. at 38-39.
[188] https://openai.com/blog/customizing-gpt-3
[189] *See* Iavor Bojinov, *Keep Your AI Projects on Track*, HARV. BUS. REV. 53-59 (Nov. Dev. 2023).

company that performs fine-tuning, for instance, could own separate trade secrets in these modifications, such as new specific datasets, prompts, and methods used to improve and customize the AI.

C. The Risk – and Promise – of Reverse Engineering

The death-knell for generative AI trade secrets is—or should be— the arrival of easy, quick, and cheap reverse engineering. The term "reverse engineering" generally means extracting information and know-how from a product, which is available on the open market, by observing it, picking it apart, and doing tests on it, as well as taking specific actions to learn information, like decompiling or disassembling source code underlying a computer program.[190] In the context of trade secrecy, "reverse engineering" can be complete—meaning all of the asserted trade secret information can easily be extracted from a product—or it can be *partial*, meaning that only some of the asserted trade secrets are discernible. For example, when a physical good is sold, some information might be easy to learn from mere inspection, such as color and size, but other information, like "tolerances," might be hard to figure out. Likewise, for software, some information, like object code, can be readily accessible, whereas other information, like source code, would take longer and be more expensive to reverse engineering.[191]

Reverse engineering is one of the most important ways that trade secrets embedded in information goods end. As James Pooley has observed, companies engage reverse engineering for all sorts of reasons, ranging from repairing a product, to achieving interoperability, to developing a complementary service, to deliberately "creating a clone of the product."[192] Reverse engineering for the explicit purpose of competition is arguably the most important type of reverse engineering from the perspective of competition and innovation policy. As Pamela Samuelson and Suzanne Scotchmer put it, "reverse engineering undertaken for the purpose of making a competing product … is the most common and most economically significant reason to reverse-engineer in this

---

[190] Pamela Samuelson and Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L. J. 1575 (2002) (defining reverse engineering broadly as "the process of extracting know-how or knowledge from a human-made artifact.")

[191] *See generally* ROGER M. MILGRIM & ERIC E. BENSEN, MILGRIM ON TRADE SECRETS §§ 1.03, 1.05, 1.09 (Matthew Bender & Co. 2023) (discussing trade secrecy in tolerances and code).

[192] Jim Pooley "identifies six reasons for engaging in reverse engineering: learning, changing or repairing a product, providing a related service, developing a compatible product, creating a clone of the product, and improving the product." *Id*. at 1582, n. 23 (citing JAMES POOLEY, TRADE SECRET LAW § 5.02 (1997)).

industrial context."[193] In their view, the act of reverse engineering is good public policy, even when (and *especially* when) undertaken for purposes of competing. When a product available on the market can legally be reverse engineered in full or in part, this makes it easier to compete, increasing consumers' options and lowering prices.[194] This also advances technological development (so-called "cumulative innovation") since improvements can proceed outside the control of the original developer. [195] And it maintains "balance" in intellectual property law by forcing developers of new inventions who cannot maintain trade secrets to obtain patents.[196] More broadly, permitting legal reverse engineering—for whatever purpose—respects peoples' rights to do what they want with products the lawfully acquire. [197] For all these reasons, Sameulson and Scotchmer argue, legal reverse engineering has historically been the default rule.[198]

With the major exception of a product that is the subject of valid patent, reverse engineering is usually legal.[199] In trade secret law, this is *always* the rule. Obtaining trade secrets by reverse engineering a lawfully obtained product is simply not trade secret misappropriation.[200] Moreover, once a trade secret *can* easily be reverse engineered from a lawfully-obtained product, it is supposed to lose protection entirely, even against insiders like employees and former business partners. Doctrinally, this is because the former-trade-secrets are deemed "generally known" or "readily ascertainable through proper means," or because the owner is deemed to have failed to

[193] Id. at 1582.
[194] Id. at 1583.
[195] Id.
[196] *Id*. at 1583-84.
[197] Id. at 1583 ("Further justification for the law's recognition of a right to reverse- engineer likely derives from the fact that the product is purchased in the open market, which confers on its owner personal property rights, including the right to take the purchased product apart, measure it, subject it to testing, and the like.").
[198] *Id*. at 1582 ("Reverse engineering is generally a lawful way to acquire know-how about manufactured products.")
[199] *See, e.g.,* Kewanee v. Bircron, 416 U.S. 470, 476-90 (1974) (reverse engineering is legal under trade secret law, and strongly suggesting that a state trade secret law that prevented reverse engineering would be preempted by patent law). *See also* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets As Ip Rights*, 61 STAN. L. REV. 311, 311 (2008) (discussing how trade secrecy can help channel some inventions into the patent system, by ensuring only truly-secret inventions can be kept as trade secrets).
[200] 18 U.S.C. § 1839 (5)-(6) (2016); *see also* UTSA, § 1, cmt..

take "reasonable" secrecy precautions to protect information that is highly vulnerable to reverse engineering.[201]

Typically, reverse engineering becomes easier and cheaper over time, and even the best-kept secrets can eventually end. For example, as mentioned above, some argue software code is getting easier and easier to reverse engineer through processes like decomplication.[202] In his recent article, Jake Sherkow makes a similar argument with regard to DNA secrecy, asserting that "advances in and the democratization of DNA sequencing technology, independent of any act on the part of DNA sequence data owners, have diminished the trade secret protectability of DNA sequence information."[203]

In the earlier stages, however, reverse engineering a new technology tends to be harder. When it comes to generative AI, at present, it is unclear how vulnerable generative AI's are to reverse engineering. Scholars have rightly opined that in general AI is highly conducive to trade secrecy because AI is "exceptionally difficult to reverse engineer[.]"[204] However, we do not know for how long this will be the case. Reverse engineering generative AI is at present difficult, costly, and time-consuming. But eventually it could become easier, cheaper, and quicker. Given the explosive rate of technological change in generative AI today, it is not impossible that partial, if not complete, reverse engineering will be possible in the near future.

There are various methods that could be used to reverse engineer a generative AI model. On the lower-tech end, one can simply use strategic prompting—crafting specific prompts (queries) in the hopes of eliciting particular outputs. On the higher-tech end is the "model extraction attack."[205] A model extraction attack aims to replicate the functionality of an AI model

---

[201] 18 U.S.C. § 1839(3) (2016). *See* Part III.

[202] Samuel J. LaRoque, *Reverse Engineering and Trade Secrets in the Post-Alice World*, 66 KAN. L. REV. 427, 439-440 (2017) (arguing that software companies increasingly face challenges in protecting software as trade secrets because reverse engineering software code through decompilation has become more feasible over time).

[203] *See* Jacob S. Sherkow, *The Myth of DNA Trade Secrets,* 75 Hastings Law Journal (forthcoming 2024).

[204] John Hillman, *Smart Regulation: Lessons from the Artificial Intelligence Act*, 37 EMORY INT'L L. REV. 775, 789-790 (2023) ("The 'black box' nature of many AI systems makes reverse engineering nearly impossible."). *See also,* Tschider, *supra* note 5, at 687-688, 709-712 (arguing that "AI algorithms establish a natural trade secret" due to their "black box" nature, because even the creators do not understand AI algorithms or have the ability to fully explain how they work).

[205] *See* Devin P. Owens, *Trade Secrecy Will Not Protect Artificial Intelligence* (unpublished student paper) (on file with author).

by querying it extensively and using the responses to train a new model that mimics the original model's behavior. This typically entails using AI to input a massive number of queries to an AI system, and analyzing the AI's responses in order to infer its underlying elements, such as overall architecture, how the model was developed and trained, and even some of the training data. [206] A model extraction attack could potentially allow someone with only "black-box" access to a closed-source model like ChatGPT to learn information about how it works, using only the inputs and outputs available through the user interface.[207]

IP scholars have noted the possibility of a model extraction attacks in the past, but back then, it was a more speculative technology.[208] This is no longer the case. Model extraction attacks are already happening. For example, model extraction attacks have been used to discern which training data was used to train an AI.[209] In an ongoing lawsuit between the New York Times and OpenAI, OpenAI is apparently alleging that the Times used something like a model extraction attack in its attempt to prove that OpenAI used copyrighted New York Times content to train ChatGPT. The Times is arguing that ChatGPT was trained on copyrighted New York Times content and will provide nearly verbatim versions of New York Times articles when prompted. In responsive pleadings, OpenAI claims that, in fact, the New York Times hired someone to "hack" ChatGPT and perform strategic prompting in order to elicit the outputs the Times wanted. OpenAI

[206] Milad Nasr, Nicholas Carlini, Jonathan Hayase, Matthew Jagielski, A. Feder Cooper, Daphne Ippolito1, Christopher A. Choquette-Choo, Eric Wallace, Florian Tramèr, Katherine Lee, Scalable Extraction of Training Data from (Production) Language Models, Nov, 28, 2023, https://arxiv.org/pdf/2311.17035.pdf (asserting that through a technique called "extractable memorization," it is possible to "efficiently extract" "training data … by querying a machine learning model without prior knowledge of the training dataset.").

[207] Florian Tramèr, Fan Zhang, Ari Juels, Michael K. Reiter, Thomas Ristenpart, *Stealing Machine Learning Models via Prediction APIs*, 25TH USENIX SECURITY SYMPOSIUM, USENIX SECURITY 601 (August 10, 2016). *See also* Winograd, *supra* note 5, at 625-626 (discussing a "training data extraction attack" whereby an "adversary" "deliberately causes a model to leak memorized information" to extract users' private information).

[208] Arti K. Rai, Isha Sharma, Christina Silcox, *Accountability, Secrecy, and Innovation in Ai-Enabled Clinical Decision Software*, 7 J.L. & BIOSCIENCES 1 (2020) (citing Tramer et al); *see also* Fromer, *supra*, at 724, 720-724, n. 109 (citing Tramer et al).

[209] Matthew Sag, *Copyright Safety for Generative AI*, 61 HOUSTON LAW REVIEW 295, 326-327 (2023).

also alleged that these actions were taken in violation of OpenAI's terms of use, an issue I discuss in the next part.[210]

To my knowledge, it is not currently possible to fully "reverse engineer" a generative AI model like ChatGPT. But it is possible to learn significant amounts about the model, including how it was developed and trained, and what data it was trained on. These techniques will likely improve over time. This has three major implications for trade secrets. First, the person doing the reverse engineering should not themselves be liable for trade secret misappropriation, assuming that this is really reverse engineering and not "improper means."[211] Second, at some point, trade secrets should end altogether—even for insiders like employees— once they are so easy to discern that the law considers them "generally known" or "readily ascertainable."[212] Third, if a company continues to disseminate a generative AI model that can easily be reverse engineered, it has arguably failed in its attempt to use "reasonable" secrecy precautions, which is a requirement for maintaining trade secrecy protection.[213] There is significant legal and factual uncertainty surrounding all of these issues.[214] But the consequence of quick, cheap, and easy reverse engineer should, as a general matter, be that trade secrecy is destroyed.

However, in the next part, I show how contracts can help AI developers avoid many of these consequences. Contractual prohibitions—particularly, anti-reverse-engineering clauses—can generate another layer of protection for trade secrets that would otherwise enter the public domain. Terms of use and end user license agreements can help to generate breach-of-contract liability, as well as potentially trade secret liability, for actions that would otherwise be legal.

II. Turning to Contracts

In the 1980s and 90s, software companies figured out how to sell their software and keep it secret too. They did so, first, by keeping certain features factually secret, and, second, by structuring their sales as licenses and binding end users to contracts that retained the legal fiction

---

[210] The New York Times Co. v. Microsoft Corp., et al., No. 1:23-cv-11195 (SHS) (OTW), Memorandum of Law in Support of OpenAI Defendants' Motion to Dismiss (S.D.N.Y. 2023), at 2 https://fingfx.thomsonreuters.com/gfx/legaldocs/byvrkxbmgpe/OPENAI%20MICROSOFT%20NEW%20YORK%20TIMES%20mtd.pdf

[211] I discuss this possibility in Part III.A *infra*.

[212] 18 U.S.C. § 1839(3).

[213] 18 U.S.C. § 1839(3).

[214] *See* discussion in Part III.

of confidentiality and placed restrictions on what users could do. [215] Some generative AI companies, including OpenAI, are pulling out the same playbook that worked for software. First, as just shown, they are keeping generative AIs factually secret[216] by deploying them in a "closed-source" format that hides back-end features from users.[217] Second, they are using contract law to obtain broader rights than trade secrecy alone would afford. In this part, I explain Open AI uses contracts to restrict what users of ChatGPT can do with the technology.[218]

A. Individual Terms of Use vs. Enterprise License Business Terms

First, I need to draw an important distinction. Two distinct terms of use apply to ChatGPT, depending on the agreement the user enters. Individual end users of ChatGPT generally click to agree[219] to a "Terms of Use" when they sign up to use ChatGPT.[220] These contracts are, in effect if not in name, "contracts of adhesion"—"boiler plate" contracts that are drafted by one side by a company that uses them in many transactions.[221] They are not negotiated. They are "take it or leave it." The end user, who is effectively the consumer of the service, has far less knowledge and essentially no bargaining power.[222]

There is a different terms of use—called the "Business Terms"—which applies to businesses or developers that sign up for a ChatGPT "Enterprise License," which was discussed

---

[215] *See* citations in notes 11 and 15 *supra*.
[216] Factual secrecy means not visible to users or easy to discern through reverse engineering. *See* note 12 *supra*.
[217] Lee, Cooper, & Grimmelmann, *supra* note 5, at 5, 41-42 (explaining "closed source" deployment of many generative AI models).
[218] End user license agreements are usually used to govern use of software. Terms of use often govern use of websites. *See* note 15 *supra*.
[219] This is a "clickthrough" and is probably enforceable. "Courts around the country have recognized that [an] electronic 'click' can suffice to signify the acceptance of a contract," and that "[t]here is nothing automatically offensive about such agreements, as long as the layout and language of the site give the user reasonable notice that a click will manifest assent to an agreement." Meyer v. Uber Technologies, Inc., 868 F.3d 66 (2d Cir. 2017) (quoting Sgouros v. TransUnion Corp., 817 F.3d 1029, 1033-34 (7th Cir. 2016)). *See also* Eric Goldman, Online Contracts, ERIC GOLDMAN, INTERNET LAW: CASES & MATERIALS 56-57 (2022 edition) (giving taxonomy of online contracts and suggesting "clickthrough" terminology).
[220] https://openai.com/policies/terms-of-use
[221] *See* Orly Lobel, *Boilerplate Collusion: Clause Aggregation, Antitrust Law & Contract Governance*, 106 MINN. L. REV. 877, 889 (2021).
[222] *Id.*

in Part I.[223] The Enterprise License is typically the result of a negotiation between OpenAI and the business or developer seeking an Enterprise License.[224]

The Enterprise License and the Terms of Use for individuals are materially different. The individual license is more like a sale of a pre-fixed, "take it or leave it" product on the open market, whereas the Enterprise License is a negotiated agreement between comparatively sophisticated entities resulting in more complete access to both ChatGPT and to OpenAI. Legally speaking, this difference matters a lot—both for purposes of contract protection and for purposes of trade secrecy protection. Courts will likely treat the Business Terms much more favorably, to the extent it is negotiated as part of an Enterprise License between businesses with equal bargaining power who have the knowledge and ability to negotiate on key terms. In contrast, courts will likely more heavily scrutinize the "mass-market" Terms of Use, which is entered between OpenAI and an end user who has little bargaining power or relevant legal knowledge.[225] This suggests the Business Terms would be more likely to survive challenges based on doctrines like unconscionability.[226]

At a substantive level, the Terms of Use and the Business Terms contain similar features, but they differ in material respects. In particular, the Business Terms contains a mutual confidentiality clause, whereas the individual Terms of Use has no confidentiality clause at all. This means an Enterprise licensee, unlike an individual user, will almost certainly be deemed to have a duty of confidentiality to OpenAI. Breaching the Business Terms is thus much more likely to generate trade secret liability based on a traditional theory of misappropriation—acquisition, use, and/or disclosure of OpenAI's information in breach of a *duty to maintain secrecy*.[227] The

---

[223] https://openai.com/policies/business-terms

[224] https://openai.com/chatgpt/enterprise https://openai.com/blog/introducing-chatgpt-enterprise https://community.openai.com/t/open-ai-licences-for-our-enterprise-customers/381951/4 OpenAI will apparently deny some requests to negotiate an Enterprise License. https://community.openai.com/t/is-chatgpt-enterprise-expensive-is-there-a-minimum-budget-who-qualifies/545691

[225] Commentators often draw a distinction between negotiated business-to-business contracts, on the one hand, and non-negotiated mass-market contracts, on the other, when discussing issues like enforceability and preemption. *See* Lemley, *supra* note 11, at 1239 (distinguishing "bargained agreements for custom software, and unbargained 'shrinkwrap licenses' imposed on mass-market purchasers."). *See also* Hrdy & Seaman, *supra* note 25, at 682-83 (distinguishing employee agreements from business-to-business agreements).

[226] *See* note 232 *supra*.

[227] Recall that trade secret "misappropriation" includes not just acquiring trade secrets by improper means (which itself includes acquiring trade secrets in breach of a duty to maintain secrecy) but

individual Terms of Use, in contrast, creates a much weaker foundation for a traditional trade secret law claim. This claim would instead be based purely on an acquisition by "improper means" theory, and would likely rely in large part, if not entirely, on the fact that an end user accessed trade secrets in breach of a specific provision in the Terms of Use—such as an anti-reverse-engineering clause. I discuss this argument in detail in Part III.A.

B. The Contractual Provisions Protecting ChatGPT's Secrets

The ChatGPT terms of use contains several provisions that seek to preserve OpenAI's trade secrets and confidential information. Below I discuss the three main provisions—an anti-reverse engineering clause, a noncompete clause, and (for Enterprise licensees only) a confidentiality clause. California law applies to all three provisions.[228] As I'll discuss in more depth in Part III, case law from software suggests that breach of some of these provisions could lead to *both* contract and trade secret law liability.

1. No Reverse Engineering

First, all ChatGPT users are subject to an anti-reverse-engineering clause that prohibits a wide variety of methods of reverse engineering ChatGPT's secrets. The Terms of Use states that ChatGPT users will not "[m]odify, copy, lease, sell or distribute any of our Services"; "[a]ttempt to or assist anyone to reverse engineer, decompile or discover the source code or underlying components of our Services, including our models, algorithms, or systems (except to the extent this restriction is prohibited by applicable law)"; or "[a]utomatically or programmatically extract data or Output…"[229]

Anti-reverse-engineering clauses are standard in software agreements.[230] Courts and commentators diverge on whether anti-reverse-engineering clauses can serve as the basis for a

---

also using or disclosing trade secrets after obtaining those trade secrets under a duty to maintain secrecy. *See generally* 18 U.S.C. § 1839(5)(2016) (defining misappropriation). *See also* note 288 *supra*.

[228] https://openai.com/policies/terms-of-use

[229] https://openai.com/policies/terms-of-use; *see also* https://openai.com/policies/business-terms Both provisions contain the caveat "except to the extent these restrictions are contrary to applicable law." This caveat likely refers to the risk of copyright preemption *See An anti-reverse engineering clause that actually works*, EPICLAW, April 20, 2020.

[230] Madison, note 15 *supra*, at 281.

trade secret claim.[231] But purely as a matter of contract law, anti-reverse-engineering agreements are typically enforced. They can be scrutinized under the relevant jurisdiction's contract rules and can be found unenforceable under doctrines like "unconscionability." To quote Deepa Varadarajan, "[t]o demonstrate unconscionability, a party must show both the lack of a 'meaningful choice' when assenting to the contract (i.e., procedural unconscionability), as well as contract terms that "are unreasonably favorable to the other party" (i.e., substantive unconscionability)."[232] But courts rarely find a term is unconscionable simply because it is "a 'take it or leave it' proposition" and "not vigorously bargained for"—that is, a contract of adhesion.[233] When a term is substantively more restrictive—which an anti-reverse-engineering agreement arguably is—courts tend to require more notice and signs of true bargained-for assent by users.[234] This means courts might likely look less favorably on the anti-reverse-engineering clause that applies individual ChatGPT users, as opposed to the Business Terms.

There are also potential preemption challenges to enforcing anti-reverse-engineering clauses under contract law, such as preemption by patent law,[235] copyright law,[236] and trade secret law.[237] These arguments have not been very successful in the past. Courts tend to view contracts

---

[231] *See, e.g.,* Lemley, *supra* note 11*,* at 1248-1259; PETER S. MENELL, ROBERT P. MERGES, MARK A. LEMLEY & SHYAMKRISHNA BALGANESH, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE: 2023, VOL. I: PERSPECTIVES, TRADE SECRETS & PATENTS 102 (2023).

[232] *See* Varadarajan, *supra* note 19, at 1587 (arguing that unconscionability doctrines and should limit enforceability of contracts used to protect trade secrets and confidential information).

[233] Murti v. Thor Motor Coach, 2023 Cal. Super. LEXIS 13443, *16-17 (Cal. Sup. Ct. 2023).

[234] *Id.* ("[T]he more substantively oppressive the contract term, the less evidence of procedural unconscionability is required to conclude that the term is unenforceable, and vice versa.").

[235] Some scholars also argue anti-reverse-engineering clauses should be preempted by patent law when they are "non-negotiated mass market" license terms and the reverse engineering is done to achieve interoperability. *See* Daniel Laster, T*he Secret Is Out: Patent Law Preempts Mass Market License Terms Barring Reverse Engineering for Interoperability Purposes*, 58 BAYLOR L. REV. 621, 624-25 (2006).

[236] *See* Guy A. Rub, *Moving from Express Preemption to Conflict Preemption in Scrutinizing Contracts over Copyrighted Goods*, 56 AKRON L. REV. 301, 302 (2023) (discussing general trend of non-preemption though noting recent case law holding that certain contracts were expressly preempted by the Copyright Act).

[237] The UTSA and the trade secret statutes of most states do not displace (preempt) contract remedies. *See* Hrdy & Seaman, *supra* note 25, 699-703 (discussing non-preemption of contracts under UTSA § 7 (1985) ("This [Act] does not affect . . . contractual remedies, whether or not based upon misappropriation of a trade secret."). I discuss the new federal preemption argument in Part III.D.

as private bargains that are not disturbed by the existence of intellectual property rights, absent some clear legislative intent.[238] Both the Federal Circuit and the Eighth Circuit have held that anti-reverse-engineering clauses attached to software licenses are not typically preempted by copyright law,[239] even though reverse engineering software is in some instances "fair use" under the Copyright Act.[240]

Given this history, courts will likely enforce the ChatGPT anti-reverse-engineering clauses as a matter of contract law.[241] There is case law to support this prediction. [242] For example, in Triage Logic Mgmt. & Consulting, LLC v. Innovative Triage Servs., a North Carolina state court recently upheld a similar clause in a software license that provided that "Licensee shall not: … modify, disassemble, decompile, reverse engineer, or otherwise re-create the System, in whole or

[238] *See* Hrdy & Seaman, *supra* note 25, at 703-706 (discussing "pro-contract" approach in IP preemption case law).

[239] *See, e.g.,* Bowers v. Baystate Technologies, Inc., 320 F.3d 1316, 65 U.S.P.Q.2d 1746 (Fed. Cir. 2003) (software license that prevented reverse engineering not preempted by copyright law); Davidson & Associates v. Jung, 422 F.3d 630, 638-39 (8th Cir. 2005) (terms of use and end user license agreements restricting users' ability to reverse engineer video game software not preempted by copyright law). *See also* Chen, *supra* note 24, at 803-805, 806-809 (discussing trend of courts enforcing anti-reverse- engineering clauses).

[240] Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510, 1520 (9th Cir. 1992), as amended (Jan. 6, 1993) (holding reverse engineering through disassembly of copyrighted object code was fair use given that this was "the only means of gaining access to … unprotected aspects of the program, and because [defendant] has a legitimate interest in gaining such access … Where there is good reason for studying or examining the unprotected aspects of a copyrighted computer program, disassembly for purposes of such study or examination constitutes a fair use."). *But see* Atari Games Corp. v. Nintendo of Am. Inc., 975 F.2d 832, 844-44 (Fed. Cir. 1992). ("Reverse engineering, untainted by the purloined copy of the 10NES program and necessary to understand 10NES, is a fair use. …[But] [t]his fair use did not give Atari more than the right to understand the 10NES program and to distinguish the protected from the unprotected elements of the 10NES program. Any copying beyond that necessary to understand the 10NES program was infringement. Atari could not use reverse engineering as an excuse to exploit commercially or otherwise misappropriate protected expression.").

[241] Chen, *supra* note 24, at 805.

[242] *See, e.g.,* Red.com, Inc. v. Jinni Tech Ltd., No. SACV 17–00382–CJC(KESx), 2017 WL4877414, at *7 (C.D. Cal. Oct. 11, 2017) (plaintiff adequately pled a breach of contract claim based on allegation that defendant reverse engineered plaintiff's software code to make storage device that was compatible with plaintiff's cameras in contravention of clause prohibiting reverse engineering).

in part."[243] The court found this anti-reverse engineering clause was enforceable. It was neither an illegal restraint on trade akin to noncompete agreement[244] nor preempted by copyright law.[245]

Importantly, these cases involved *contract law* claims based on breach of an anti-reverse engineering clause, not *trade secret law* claims based on breach of an anti-reverse engineering clause. The more frightening consequence for anyone who reverse engineers ChatGPT is that they might be exposed to trade secret law liability as well as contract law liability. As I'll discuss in detail in Part III, some courts have held that breach of an anti-reverse-engineering clause can indeed establish trade secret misappropriation though an acquisition by "improper means" theory, even in situations where the defendant had no prior relationship to the trade secret holder or underlying duty of confidentiality. Indeed, as I'll discuss, some state trade secret statutes explicitly allow for this interpretation.[246] If this argument is accepted, then anti-reverse-engineering clauses can potentially shield trade secrets from *ever* becoming readily ascertainable through "proper means," when the only way to access trade secrets is by reverse engineering them in breach of an agreement.[247] I'll argue that this is a wrong interpretation of the law, especially now that federal law states that reverse engineering is a lawful means of obtaining a trade secret.

2. No Competition

Second, the Terms of Use contains what will likely be construed as a noncompete clause. The provision is not labeled as a noncompete, but it prohibits users from using ChatGPT outputs "to develop models that compete with OpenAI."[248] The language in the Business Terms is slightly more limited. It states that Enterprise licensees cannot use "Output … to develop any artificial intelligence models that compete with our products and services"; however, Enterprise licensees *can* use "Output" to "develop artificial intelligence models" so long as they are "primarily intended to categorize, classify, or organize data" and are "not distributed or made commercially available to third parties[.]"[249] Notably, OpenAI is not the only AI developer deploying these clauses.

---

[243] Triage Logic Mgmt. & Consulting, LLC v. Innovative Triage Servs., LLC, 2020 NCBC 57, 41-42 (N.C. Super. Ct. 2020).
[244] *Id*. at 41-42.
[245] *Id.* (citing, e.g., SAS Inst., Inc. v. World Programming, Ltd., 874 F.3d 370, 381 (4th Cir. 2017).
[246] *See* Part III.
[247] *See* Part III.
[248] https://openai.com/policies/terms-of-use
[249] Enterprise licensees are also allowed to "fine tune" pre-trained GPT models on their own data. https://openai.com/policies/business-terms

Meta—which releases its Llama model in an *open-source* format—has a similar provision in its EULA.[250]

A noncompete is far more burdensome than a standard confidentiality agreement, because a noncompete prohibits competition altogether. That said, the ChatGPT clauses are *not* a full ban on competition. They do not prohibit licensees from competing with OpenAI under any circumstances. They simply prevent them from using the outputs of ChatGPT to do so. This is analogous to a blacksmith who makes someone a sword and says "you cannot use this sword to kill me, but you can still kill me with a different sword."[251]

Still, this is a restriction on competition, and I suspect it would be classified as a noncompete, triggering the relevant jurisdiction's noncompete rules. As noted above, the choice of law provision says California law applies.[252] California famously bans noncompetes.[253] Employers in California generally cannot enter noncompetes with workers, with some exceptions, such as where an employee agrees not to compete as a part of the sale of a business.[254] California's ban has not typically been applicable outside the employment context.[255] The Federal Trade Commission's recent ban on noncompetes also applies only to agreements between employers and workers.[256] Still, even for business-to-business noncompetes, courts would still apply a "reasonableness" test to judge a noncompete agreement's enforceability.[257]

Courts are likely to be skeptical of OpenAI's noncompete provision—especially with regard to individual users who did not negotiate an Enterprise License. Under the laws of most

---

[250] Meta's provision states: "You will not use the Llama Materials or any output or results of the Llama Materials to improve any other large language model (excluding Llama 2 or derivative works thereof)." https://ai.meta.com/llama/license/#:~:text=You%20are%20granted%20a%20non,modifications%20to%20the%20Llama%20Materials *See also* note 103 *supra*.

[251] There is no footnote for this. I made it up.

[252] https://openai.com/policies/terms-of-use

[253] *See* Cal. Bus. & Prof. Code § 16600 (2023).

[254] Edwards v. Arthur Andersen LLP, 44 Cal. 4th 937, 946-947 (Cal. 2008).

[255] This could change. The California ban was just amended to be even stronger. Assembly Bill 1076 clarifies that the ban can cover contracts where the person restrained from practicing their trade was not a party to the contract. *See* Cal. Bus. & Prof. Code § 16600(c) (2023).

[256] Federal Trade Commission, Non-Compete Clause Rule, issued April 23, 2024, 16 CFR Part 910, https://www.ftc.gov/system/files/ftc_gov/pdf/noncompete-rule.pdf

[257] *See, e.g.,* Quidel Corp. v. Superior Court, 57 Cal. App. 5th 155, 166-168 ("Noncompetition clauses have been deemed valid outside the employment arena[,]" but courts apply "a test of reasonability, contemplating whether the arrangement promoted competition.").

jurisdictions, a noncompete must be "reasonable" in terms of time, geography, and scope and reasonably related to protecting "legitimate interests."[258] Even assuming OpenAI has "legitimate interests" to protect, such as its immense investment in developing ChatGPT and the underlying model, there are few indicators of overall reasonableness. There is no limitation on the types of "Output" that licensees cannot use to compete. The Output does not have to be a trade secret or confidential information. It can be anything generated by ChatGPT. [259] What if an app developer asks ChatGPT what types of training data work best for producing generative AI, and follows that general suggestion to build a new model? What if ChatGPT makes up a business plan, and the user follows it? The chain of possible triggering events is effectively limitless. Also, individual users never received specific notice, let alone separate consideration, that might justify enforcing a promise to never use ChatGPT's outputs to compete with OpenAI.[260]

Most importantly, there is no time limit. The prohibition on competition lasts forever. Some case law—and not even from California— suggests that perpetual noncompete clauses in software agreements cannot survive a "reasonableness" standard. They are unenforceable. For example, in *Triage Logic Mgmt. & Consulting, LLC,* a North Carolina court recently found a noncompete clause in a software license agreement to be an illegal restraint on trade and unenforceable under North Carolina law. The clause provided that "the Licensee shall not… develop similar software, services or product offerings substantially similar to the System."[261] The court classified the clause as a noncompete, even if it did not use the words "do not compete," and found the provision to be an unenforceable restriction on trade under North Carolina law because it lacked a time limit.[262]

---

[258] *See* RESTATEMENT (SECOND) OF CONTRACTS § 188 (AM. L. INST. 1981).

[259]The Terms of Use's noncompete clause states simply that users cannot "[u]se Output to develop models that compete with OpenAI." "Output" is defined to include any output that a user receives from ChatGPT. https://openai.com/policies/terms-of-use

[260] One could argue getting to use ChatGPT itself is consideration, but courts often require separate consideration to enforce a noncompete. Michael J. Garrison & John T. Wendt, *Employee Non-Competes and Consideration: A Proposed Good Faith Standard for the "Afterthought" Agreement,* 64 U. KAN. L. REV. 409, 414, 427 (2015).

[261] Triage Logic Mgmt. & Consulting, LLC v. Innovative Triage Servs., LLC, 2020 NCBC 57, 26-27 (N.C. Super. Ct. 2020).

[262] The court wrote: "[T]here is no end date for the non-competition provision … An indefinite and perpetual restraint on trade in the context of a software licensing agreement seems to be counter to the antitrust laws of this State." s*Id*. at 43-51.

This does not bode well for the noncompete clauses in OpenAI's Terms of Use. I imagine a California court would treat this clause even less favorably. That said, it is possible courts might enforce the noncompete clause in the Business Terms, as opposed to the one that applies individual users. In general, the analysis applied to noncompetes in business-to-business arrangements is more lenient than in employee or end user cases. Courts tend to assess the overall effects on competition, rather than the effect on a particular individual's ability to work their trade and compete. [263] I could perceive courts scrutinizing the Business Terms in a nuanced way, focusing on the fact that business users and app developers are given privileged access to ChatGPT, including potentially access to its APIs, and should not be able to use this access to build competing models.

Importantly, even if the noncompetes are unenforceable, they can still shield OpenAI from competition, because some users might be scared off. Noncompetes have a well-known "chilling effect." Risk-adverse businesses and developers may choose to forego plans to compete due simply to the existence of the clause.[264]

3. Confidentiality

Finally, users of ChatGPT who obtain an Enterprise License are subject to a mutual confidentiality obligation. The Business Terms has a confidentiality provision that limits both sides' disclosure and use of "Confidential Information"–-defined as "any business, technical or financial information, materials, or other subject matter … that is identified as confidential at the time of disclosure or should be reasonably understood by Recipient to be confidential under the circumstances[.]"[265] It obligates Recipients to "(a) only use Recipients Confidential Information to exercise its rights and fulfill its obligations under this Agreement, (b) take reasonable measures to protect the Confidential Information, and (c) not disclose the Confidential Information to any third party except as expressly permitted in this Agreement."[266] There are some exceptions for

[263] *See, e.g.,* Innovation Ventures, LLC v. Custom Nutrition Lab'ys, LLC, 912 F.3d 316, 341–42 (6th Cir. 2018) (distinguishing enforceability of "employment noncompete agreements" and "noncompete agreements between businesses"). *See also* 3 LOUIS ALTMAN & MALLA POLLACK, CALLMANN ON UNFAIR COMPETITION, TRADEMARKS & MONOPOLIES, § 16:47 (4th Ed. 2022).
[264] Hrdy & Seaman, *supra* note 25, at 3026 (citing Meirav Furth-Matzkin & Roseanna Sommers, *Consumer Psychology and the Problem of Fine-Print Fraud*, 72 STAN. L. REV. 503, 503 (2020)).
[265] https://openai.com/policies/business-terms
[266] https://openai.com/policies/business-terms

information that "(a) is or becomes generally available to the public through no fault of Recipient, (b) was in Recipient's possession or known by it prior to receipt from Discloser, (c) was rightfully disclosed to Recipient without restriction by a third party, or (d) was independently developed without use of Discloser's Confidential Information."[267]

The main purpose of this agreement is ostensibly to protect the confidentiality of *licensees'* information. "Confidential Information" explicitly includes "Customer Content," which includes both users' "inputs" into ChatGPT and the "outputs" received from ChatGPT.[268] Indeed, one major benefit of the Enterprise License, from businesses' perspective, is said to be that they can reduce the risk that their employees will use ChatGPT and give up their company's trade secrets.[269] However, the confidentiality provision in the Business Terms is written to be mutual. It protects *OpenAI's* trade secrets and confidential information as well.[270]

From a legal perspective, this mutual confidentiality agreement has important implications for businesses and developers who are in an Enterprise License relationship with OpenAI. First, it places them under a duty of confidentiality with regard to information they receive from OpenAI.[271] Trade secret "misappropriation" includes using or disclosing a trade secret that was obtained under a duty to maintain secrecy, so licensees would be subject to this type of trade secret claim.[272] Second, the confidentiality agreement helps satisfy OpenAI's requirement to take reasonable secrecy precautions to protect trade secrets, making it more likely OpenAI can successfully bring a trade secret claim, versus just a contract claim.[273] Third, the confidentiality provision can expand protection beyond trade secrets to cover a broader range of non-public

---

[267] https://openai.com/policies/business-terms
[268] https://openai.com/policies/business-terms
[269] https://openai.com/blog/introducing-chatgpt-enterprise *See also* https://www.eweek.com/artificial-intelligence/chatgpt-enterprise/
[270] Again, the agreement refers to confidential information as being "disclosed by one party" "to the other party." It's not written to be specific to the licensee's information. Also, there are other parts of the agreement that show this is intended to cover OpenAI's information too. Section 11.1 refers to "either party's breach of its confidentiality obligations under Section 4 (Confidentiality)[.]" https://openai.com/policies/business-terms
[271] *See* Hrdy & Seaman, *supra* note 25, at 689.
[272] 18 U.S.C. § 1839(5)(B)(ii)(II).
[273] *See* Hrdy & Seaman, *supra* note 25, at 688-89.

information.[274] As shown above, the provision is drafted broadly to cover "Confidential Information"—including but not limited to trade secrets.[275]

Precisely what "Confidential Information" Enterprise licensees receive from OpenAI is hard to discover. Information disclosed by OpenAI under the Enterprise License might include information that OpenAI deliberately shares—like software updates, a newer version of the GPT model that has not yet been widely released, or business information, such as information about OpenAI's customers.[276] Confidential Information might also include information that OpenAI did *not* deliberately share, but that someone with Enterprise access might be able to extract from the underlying AI model—such as algorithms, source code, training data, and overall technical architecture. As noted in Part I, some of this information may well qualify as trade secrets. If so, then an Enterprise licensee uses or discloses this information, they might be liable for trade secret misappropriation too, not just breach of contract.[277]

Trade secret liability would extend not just to iterative copying of OpenAI's information, but also to improvements and products "derived from" that information.[278] Liability would extend, for instance, to scenarios where a developer uses information acquired under the license to develop a new product that falls outside the scope of the permission in the Enterprise License. Importantly, the Business Terms expressly allows developers to do certain things with OpenAI's information. They can develop and fine tune their own artificial intelligence models based on ChatGPT—as in

---

[274] *Id.* at 689.

[275] Contracts can protect a broader sphre of "confidential" information that is not a trade secret. *See* Hrdy & Seaman, *supra* note 25, at 669. *See also* Rex Alley, Note, *Business Information and Nondisclosure Agreements: A Public Policy Framework*, 116 NW. U. L. REV. 817, 817-21 (2021); Hrdy & Seaman, *supra* note 25, at 669.

[276] https://openai.com/blog/introducing-chatgpt-enterprise

[277] *See* Hrdy & Seaman, *supra* note 25, at 669, 685-93. *See also, e.g.,* Hampton Roads Connector Partners v. Land to Sand Site Services, Civil No. 2:23 cv 174, 2023 WL 8539536, * 10 (E.D. Va. Oct. 17, 2023) (holding that because defendants "acted outside the scope of their authorization to use the Project System when they downloaded [plaintiff's] materials[,]" and did so in breach of the parties' confidentiality agreement, "the downloading was done by 'improper means' under the DTSA and [Virginia UTSA].")

[278] *See, e.g.,* Gourmeta, Inc. v. Weilenmann, 1993 U.S. Dist. LEXIS 1201, *14-15 (Ill. N. D. Ct. 1993). This is different from copyright law which requires proving substantial similarity between the original product and the end product. *See, e.g.,* Mark Lemley, Essay, *The Fruit of the Poisonous Tree in IP Law*, 103 IOWA L. REV. 245, 267 (2017); *see also, e.g.,* Camilla A. Hrdy, *Should Dissimilar Uses of Trade Secrets Be Actionable?,* 167 U. PA. L. REV. ONLINE 78 (2019).

the Whoop example above.[279] But if the licensee acts outside of this permission, they could be liable for both breach of contract and trade secret misappropriation.

The story is different for individual users of ChatGPT. The current version of the ChatGPT "Terms of Use," which becomes effective January 31, 2024, does not contain a confidentiality provision. The original Terms of Use, which was instituted in March 2023, did contain a confidentiality provision, but it was unilateral. It only applied to OpenAI's and "third parties;" information, not to users' information.[280] The original Terms of Use stated, in relevant part, that users of ChatGPT would be given access to "nonpublic information that OpenAI, its affiliates, or third parties designate as confidential or should reasonably be considered confidential under the circumstances, including software, specifications, and other nonpublic business information."[281] Users had to agree: to use this information "only as needed to use the Services as permitted under these Terms"; to not disclose this information "to any third party"; and to "protect [this information] in the same manner that you protect your own confidential information of a similar nature, using at least reasonable care."[282]

The original provision drew criticism because it was "unilateral" and came across as hypocritical. It seemed as if OpenAI was trying to make sure its own information was kept confidential,[283] but it was not giving the same promise to users. ChatGPT was left free to absorb and train on users' informational inputs, while users' were vulnerable to all sorts of trade secrecy and privacy concerns. The confidentiality provision gave "confidentiality protection solely for OpenAI's information…[N]either the inputs provided to OpenAI nor the output it produces [were] treated as confidential by OpenAI…. Many companies are likely to be caught off guard by this

[279] As mentioned above, licensees can "develop artificial intelligence models" so long as they are "primarily intended to categorize, classify, or organize data" and are "not distributed or made commercially available to third parties[.]" https://openai.com/policies/business-terms

[280] https://openai.com/policies/mar-2023-terms

[280] https://openai.com/policies/mar-2023-terms

[281] https://openai.com/policies/mar-2023-terms

[282] https://openai.com/policies/mar-2023-terms

[283] The main purpose of the original confidentiality provision was presumably to protect information relating to ChatGPT's underlying technology, but it might also have been intended to protect the information of "third parties" who might have inadvertently fed sensitive data into ChatGPT. *See* Levine, *supra* note 8, at 575.

provision."[284] OpenAI's response was not to create a mutual confidentiality provision that would protect both OpenAI and users of ChatGPT. Instead, the new Terms of Use has an "Opt-Out" provision that lets users opt out of having their data trained,[285] but it contains no confidentiality clause at all.[286] As discussed in Part III, the absence of a confidentiality provision may create a risk to OpenAI's ability to protect trade secrets related to ChatGPT.

III. How Courts Can Change the Status Quo

Once an information good is widely distributed to the general public, and once information embedded in that good is visible to users or easy to discern with little time and effort, that information is no longer factually secret. It should not be protectable as a trade secret. Yet terms of use and end user license agreements can make information legally protectable by inserting anti-reverse-engineering clauses. If liability for breaching such clauses were limited to breach of contract, the harm would not be as great. However, in software cases, breaching contractual provisions has sometimes given rise to liability under *trade secret law* as well as contract law. [287] In particular, some courts have concluded that acquiring trade secrets in breach of an anti-reverse engineering clause constitutes acquisition of trade secrets by "improper means"— even though the underlying act would otherwise constitute lawful reverse engineering, and even though the person doing the reverse engineering had no prior relationship or underlying confidentiality obligations

[284] Kate Downing, OpenAI's Massive Data Grab, Law Offices of Kate Downing, March 10, 2013, https://katedowninglaw.com/2023/03/10/openais-massive-data-grab/ *See also, e.g.,* Russel G*., Chat GPT Terms & Conditions Are Scary,* MEDIUM, May 11, 2023 (discussing concerns about users' privacy and other restrictions imposed on ChatGPT users).

[285] https://openai.com/policies/terms-of-use

[286] https://openai.com/policies/terms-of-use

[287] *See* Samuelson & Scotchmer, *supra* note 10, at 1609, n. 163 (discussing the argument that acts that qualify as reverse engineering, like decompilation and disassembly of software are illegal under trade secret law when done by "violating anti-reverse-engineering clauses of shrinkwrap license contracts under which they were distributed."). *See also* Pamela Samuelson, *Reverse Engineering Under Siege*, 45 COMMUNICATIONS OF THE ACM 1, 1 (2002) (arguing that this argument is wrong, that "reverse engineering is a lawful way to acquire trade secrets," and that courts should "reject the premise that breach of a mass market license forbidding reverse engineering is an improper means to obtain a trade secret.").

to the trade secret holder. [288] The breach of contract, in other words, supplies the "bad act" supporting trade secret liability.[289]

This same reasoning will likely be applied to attempts to reverse engineer generative AI. Companies will argue that because their terms of use prohibit reverse engineering, doing so constitutes both breach of contract and acquisition of trade secrets through "improper means."[290] The prospect of trade secret liability for what should be only breach of contract is alarming. It means prevailing plaintiffs can obtain trade secret law remedies, not just contract law remedies. For example, if a person extracts trade secrets from a generative AI model, that person could be liable for breaching an anti-reverse engineering clause, and also face heightened damages, attorneys fees, and a variety of injunctive remedies under federal and state trade secret laws.[291]

Moreover, third parties who are not in privity with the trade secret owner—who did not sign any contract at all—could be liable for trade secret misappropriation too, if they obtain information from someone whom they know or should know used "improper means" to acquire the information.[292] For example, if someone who extracts trade secrets from a generative AI model shares this information with another person who knows or *should know* the secrets were obtained in breach of an anti-reverse-engineering clause, then the third party could also be liable. [293] To make this still more specific, imagine that someone reverse engineers trade secret information in breach of a "click-to-agree" license provision that forbids reverse engineering, and shares this with a third party, who never signed a license at all. Imagine the third party posts the information on

---

[288] If the person did have an underlying confidentiality obligation, then the trade secret holder could rely on a more traditional trade secret liability theory based on breach of a duty to maintain secrecy. *See* Hrdy & Seaman, *supra* note 25, at 686 (noting that "misappropriation" "includes—though is not limited to—'disclosure or use of a trade secret' 'by a person who knows or has reason to know' that the trade secret was 'acquired under circumstances giving rise to a duty to maintain the secrecy . . . or limit the use of the trade secret.' ") (quoting 18 U.S.C. § 1839(5)(B)(ii)(II) (2018)).

[289] I discuss this case law and reasoning in detail below. *See* note 314 *infra* and accompanying text.

[290] *See* note 210. *See also* https://openai.com/policies/terms-of-use

[291] *See* UTSA, §§ 2(a), 3 (remedies available under UTSA); *see also* 18 U.S.C. § 1836(b)(3) (2016) (remedies available under DTSA). *See also* Alan J. Tracey, *The Contract in the Trade Secret Ballroom-A Forgotten Dance Partner?,* 16 TEX. INTELL. PROP. L.J. 47, 69-70 (2007) (comparing trade secret and contract remedies and explaining the advantages to trade secret remedies).

[292] 18.U.S.C. § 1839(5)(2016).

[293] 18.U.S.C. § 1839(5)(2016).

the internet. If a court decides the third party knew or should have known that this information encompassed, or was *derived from,* trade secrets when they posted the information on the internet, then the third party could be liable for trade secret misappropriation as well.[294] Trade secret liability can even expose some defendants to criminal liability, assuming they have the requisite intent. This is something that contract law alone obviously does not do.[295]

In this part I argue that this reasoning is wrong. Courts should not accept that breach of an anti-reverse-engineering clause, on its own, generates "improper means" establishing trade secret misappropriation. More broadly, courts should not permit trade secret holders to protect information, at least under trade secret law, after it can easily be reverse engineered by the general public based on investigation of publicly-distributed products or services. There are three doctrinal levers through which this can be accomplished: the universal rule that reverse engineering is legal under federal and state law; the nearly-universal rule that "readily-ascertainable" information is not a trade secret; and the requirement that trade secret owners must demonstrate they took "reasonable measures" to protect information they claim to be trade secrets. I discuss each doctrinal levers in depth below, explaining how courts have treated the issue in the past, and how courts should treat the issue in hypothetical future cases involving generative AI.

I then argue that passage of the DTSA makes my arguments far more compelling than they were before the DTSA's effective date of May 11, 2016.[296] Because the DTSA explicitly states that reverse engineering is not an improper means of acquiring trade secrets as a matter of federal law,[297] it should no longer be possible to simply point to an anti-reverse engineering clause in a terms of use in order to establish that acquisition of trade secrets was accomplished by improper means. This is the only logical interpretation of the DTSA's statutory language, and it is arguably the only lawful interpretation of state trade secret laws as well. I show that the DTSA gives rise to

---

[294] This is the fact pattern in *DVD CCA v. Bunner,* which I discuss *infra*. *See also* Samuelson, note 287 *supra*, at 1 (summarizing these facts). *See also* note 278 *supra* (explaining that trade secret liability reaches information derived from trade secrets, even if the end product is different).

[295] 18 U.S.C §§ 1831-1832 (2016) (criminal penalties). That said, it is unlikely a prosecutor would bring a criminal claim for someone whose only bad act was to breach a term of use. Similar questions have arisen with the Computer Fraud and Abuse Act (CFAA) and courts have been very skeptical that breaching a terms of use alone would lead to criminal liability under the CFAA. *See* Orin S. Kerr, *Focusing the CFAA in Van Buren,* 2021 SUP. CT. REV. 155, 170-174 (2021).

[296] David S. Levine & Christopher B. Seaman, *The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act*, 53 WAKE FOREST L. REV. 105, 143 (2018).

[297] 18 U.S.C. § 1839(6)(2018).

novel preemption arguments that have yet to be raised—let alone tested—but that could tip the balance in favor of reverse engineering and free competition.

A. Reverse Engineering Is Not An Improper Means of Acquiring Trade Secrets

Reverse engineering is not an improper means of obtaining a trade secret.[298] The DTSA explicitly states that improper means of acquiring a trade secret "does not include reverse engineering, independent derivation, or any other lawful means of acquisition[.]"[299] Even prior to passage of the DTSA in 2016, the relevant stakeholders—including the drafters of the UTSA, the state legislatures that adopted the UTSA, and the Supreme Court of the United States—agreed that obtaining a product on the open market "by a fair and honest means" and picking it apart to learn secrets was not trade secret misappropriation.[300] However, the line between legal reverse engineering—a "fair and honest means" of acquiring trade secrets—and acquisition of trade secrets by "improper means" is blurry. What counts as "improper" depends on the perceived social wrongness of the defendant's actions, and on the degree to which defendant's success in accessing trade secrets was precipitated by the trade secret holder's own failure to protect against this sort of act.[301] Over the decades, courts have found a wide variety of actions to be "improper" under trade secret law, ranging from flying a plane over an unfinished plant to hiring detectives to plow

[298] Samuelson & Scotchmer, *supra* note 10, 1583.
[299] *See* 18 U.S.C. § 1839 (6) (2016).
[300] *See* Kewanee v. Bircron, 416 U.S. 470, 487-493 (1974) (holding state trade secret law was not preempted in part because the risk of someone choosing to rely on trade secret protection is "remote indeed," given that trade secret laws do not prohibit discovery by "fair and honest means" such as independent development or reverse engineering). *See also* UTSA, § 1, cmt. (listing reverse engineering as a lawful means of acquiring trade secrets). For a survey of state trade secret laws, see RUSSELL BECK, TRADE SECRETS LAWS AND THE UTSA: 50 STATE AND FEDERAL LAW SURVEY, https://www.faircompetitionlaw.com/wp-content/uploads/2018/08/Trade-Secret-50-State-Chart-20180808-UTSA-Comparison-Beck-Reed-Riden-2016-2018.pdf *See also* Samuelson & Scotchmer, *supra* note 10, 1583 ("The legal right to reverse-engineer a trade secret is so well-established that courts and commentators have rarely perceived a need to explain the rationale for this doctrine.").
[301] *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. e (AM. L. INST. 1995).

through garbage;[302] but courts have found other actions, such as picking locks to learn lock codes, to be lawful reverse engineering.[303]

How will this rule apply in the context of generative AI? The likely fact pattern is as follows. An end user of a generative AI model will use a certain technique, such as strategic prompting or a model extraction attack,[304] in order to learn information about the underlying model—for example, how it was developed or what training data was used to train the model. The person taking these actions will argue, and perhaps honestly believe, that this is legal reverse engineering. The AI distributor will argue, in contrast, that this is acquisition of trade secrets by improper means and that the person is liable for trade secret misappropriation. The AI distributor will bring trade secret law claims under the DTSA and under applicable state trade secret law.[305] The AI owner will also likely bring a separate claim for breach of contract, assuming the person breached a term of use that prohibits reverse engineering.[306]

When this legal case arises, two factors will significantly complicate courts' task in distinguishing between legal reverse engineering and improper means. First, the main technological avenue for reverse engineering generative AI will likely employ advanced AI techniques or at least some form of computer automation that goes beyond what humans can do on their own. Courts could potentially view these enhanced techniques as "improper means," based

---

[302] *See* Victoria A. Cundiff, *Reverse Engineering the Competition,* paper presented at Law Seminars International Program on trade secrets (2003) (on file with the author) (citing, e.g., E.I. DuPont de Nemours & Co., Inc. v. Christopher, 431 F.2d 1012 (5th Cir. 1970); Tennant Co. v. Advance Machine Co., Inc., 355 N.W.2d 720, 725 (Minn. Ct. App. 1984)).

[303] Chicago Lock Co. v. Fanberg, 676 F. 2d 400, 404 (9 Cir. 1982) (holding it was not improper means to publish key codes to locks obtained from "comparatively small" number off lock smiths who supplied this information because this was "proper reverse engineering.").

[304] *See* text accompanying notes 206 to 207 *supra*.

[305] Hrdy & Seaman, *supra* note 25, at 673, n. 3 ("Since 2016, trade secret owners can bring federal claims under the Defend Trade Secrets Act (DTSA) and also state-law claims based primarily on the Uniform Trade Secrets Act (UTSA).").

[306] Note that the plaintiff in this hypothetical case may well bring other causes of actions—including violation of the Computer Fraud and Abuse Act ("CFAA") or the Digital Millennium Copyright Act ("CFAA"), to the extent the person seeks access to copyrighted content. See Samuelson & Scotchmer, *supra* note 10, at 1578, 1637, n. 304 (noting applicability of Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1994) and Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 5, 17, 28, and 35 U.S.C.) ("DMCA")). These statutes are related, but they are beyond the scope of my arguments, which focus on the appropriateness of trade secret law liability.

simply on the fact that they rely on computers or AI to gain access. If so, then what would otherwise be legal reverse engineering could be deemed improper trade secret misappropriation.

A recent case from the Eleventh Circuit suggests courts might see using AI or automation to discern trade secrets as "improper means," as opposed to lawful reverse engineering. In Compulife Software Inc. v. Newman, the defendant hired a woman named Natal (whom the court called a "hacker"[307]) to obtain access to a database of insurance quotes "by creating a robot" to "scrape" the plaintiff's website.[308] The lower court, via a magistrate judge, held the defendant's actions were legal, given that the website was made "freely available to the public."[309] The Eleventh Circuit reversed, holding the lower court failed to consider whether using a "bot" to obtain the database was "improper means."[310] The fact that "the defendants took the quotes from a publicly accessible site," the Eleventh Circuit wrote, does not "automatically mean that the taking was authorized or otherwise proper."[311] To the contrary, the Eleventh Circuit strongly implied that the fact that defendant used *non-human means*—a "scraping attack" effectuated using a "robot," as the court described it—was itself an improper act, and that the plaintiff could not have been expected to design its website to prevent a non-human intrusion. The court analogized using an automated computer means to extract data from the website to a flying an airplane over an unfinished chemical plant to take photographs—which the Fifth Circuit held in a famous trade secret case was "improper means." Just as the plant owner (duPont) could not have been expected to protect the plant from an aerial espionage, so too could the website owner not be expected to protect against "a robot."[312] The Eleventh Circuit remanded for the lower court to determine whether the "scraping attack" amounted to improper means.[313]

---

[307] Hacking is the "act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data." Hasala Ariyaratne, *The Impact of ChatGPT on Cybercrime and Why Existing Criminal Laws Are Adequate,* 60 AM. CRIM. L. REV. 1, (2023). Notably, in CFAA cases, courts have sometimes recognized that breach of a terms of use alone cannot give rise to criminal liability. *See* note 295 *supra*.

[308] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1298-1300 (11th Cir. 2020).

[309] *Id*. at 1312-1314.

[310] *Id*. at 1314.

[311] *Id*. at 1314.

[312] *Id*. at 1314-1315 (citing cases).

[313] *Id*. at 1313.

This case suggests a court might view any attempt by a ChatGPT user to learn ChatGPT's trade secrets using non-human-means as "improper," regardless of the fact that reverse engineering is lawful under trade secret law. This is not the right approach. There should not be a static, bright-line rule that using AI, computers, or automation to extract trade secrets is unlawful—especially if this is done using only widely-distributed products and publicly-available sources. How courts treat such techniques in the future must depend on the facts of the case and the precise circumstances of the acquisition. Courts' position should also *change over time.* If using non-human methods to extract data becomes more acceptable in the coming years—more like lock-picking has become in the lock-smith community —then a court should deem these methods proper reverse engineering. Past case law should not control every future technological iteration.

There is a second reason that an end user who extracts trade secrets from a publicly-distributed generative AIs—regardless of which technique they use—might be liable for trade secret misappropriation. That reason is of course contracts. Under one interpretation of trade secret law—albeit an incorrect one—otherwise-lawful reverse engineering can be transformed into trade secret misappropriation when done in breach of an anti-reverse-engineering clause, because breach of the contract *itself* constitutes "improper means" of acquiring trade secrets.[314] For example, imagine a member of the public obtains a ChatGPT account, and then extracts information about ChatGPT's training data using strategic prompting. Imagine further that this action is done in breach of an anti-reverse-engineering clause in ChatGPT's terms of use. This hypothetical user could be liable for trade secret misappropriation as well as breach of contract, if a court decides that breach of the clause is itself an improper means of acquiring trade secrets.

This is not a legitimate interpretation of the scope of trade secret law liability. Scholars like Pam Samuelson have observed how problematic it would be if trade secret holders could simply attach mass-market, non-negotiated end user license agreements to their software products, in order to prohibit otherwise-legal reverse engineering—potentially for all time. As Samuelson put it over twenty years ago, courts should recognize "the longstanding rule that reverse engineering

[314] *See* note 287 *supra* and text and notes 337 to 340 and 347-**Error! Bookmark not defined.** *infra*.

is a lawful way to acquire trade secrets and should reject the premise that breach of a mass market license forbidding reverse engineering is an improper means to obtain a trade secret."[315]

When Samuelson wrote that sentence, trade secret law was primarily state law. There was a federal criminal trade secret statute, but no federal civil trade secret cause of action yet.[316] Now there is. This generates a potential conflict between federal and state law regarding which types of actions to discover trade secrets qualify as legal reverse engineering as opposed to improper means. Under federal law—and the trade secret laws of all states—it is extremely clear that reverse engineering, on its own, is not misappropriation; it is a "proper means" of acquiring trade secrets.[317] Some state statutes differ, however, about whether reverse engineering *in breach of a contract* can itself be "improper means." Some states' statutes explicitly refer to breach of an anti-reverse engineering clause as improper means of discovering trade secrets. Texas' trade secret statute, for example, defines improper means to include, among other things, "breach or inducement of a breach of a duty … *to prohibit discovery of a trade secret*[.]"[318] Other states' statutes are less explicit but do refer to breach of duties "imposed …by contract [or] license" as an improper means of acquiring trade secrets.[319]

---

[315] Samuelson, *Reverse Engineering Under Siege*, *supra* note 287, at 1. *see also* Micah Schwalb, Exploit Derivatives & National Security, 9 Yale J. L. & Tech. 162, 183–84 (2007); Pamela Samuelson, *First Amendment Defenses in Trade Secrecy Cases*, in THE LAW AND THEORY OF TRADE SECRECY (ROCHELLE C. DREYFUSS, KATHERINE J. STRANDBURG, EDS., 2010).

[316] *See generally* Christopher Seaman, The Case Against Federalizing Trade Secrecy, 101 VA. L. REV. 317 (2015) (arguing against federalization of trade secret law); James Pooley, The Myth of the Trade Secret Troll: Why We Need a Federal Civil Claim for Trade Secret Misappropriation, 23 GEO. MASON L. REV. 1045 (2016) (arguing that national trade secret protection is both necessary and efficient).

[317] 18 U.S.C. § 1839(6); *see also* citations in note 300. *See also, e.g.,* Evolution, Inc. v. SunTrust Bank, 342 F.Supp.2d 943, 962 (D.Ct. Kansas 2004) ("Nearly every court that has considered the issue of reverse engineering has held that it does not by itself constitute an improper means for purposes of a trade secret violation.").

[318] Tex. Civ. Prac. & Rem. Code Ann. § 134A.006 (West 2023), https://statutes.capitol.texas.gov/Docs/CP/htm/CP.134A.htm (emphasis added).

[319] South Carolina's trade secret law, for example, defines misappropriation via improper means to include, among other things, "… a breach of a duty to maintain secrecy" or of "duties imposed by the common law, statute, contract, [or] license[.]" S.C. Code Ann. § 39-8-60 (2023), https://www.scstatehouse.gov/code/t39c008.php

Meanwhile, the DTSA, the UTSA, and many state trade secret statutes, define improper means as including "breach or inducement of a breach of a *duty to maintain secrecy*…"[320] This language seems to refer to breach of a nondisclosure or confidentiality obligation. The text's reference to a "duty to maintain secrecy" does not obviously encompass breach of any contractual duty, let alone a contractual duty not to reverse engineer.[321] This would be an especially odd interpretation since many of these statutes—including the DTSA and the California UTSA— go on to state directly afterwards that reverse engineering is not an improper means of acquiring trade secrets.[322] That said, even if breach of an anti-reverse engineering provision (as opposed to breach of a confidentiality or nondisclosure provision) is not a specifically-delineated improper means under these laws, the text is *not* written to be exhaustive. Courts can still decide that a particular mechanism of reverse engineering— including reverse engineering in breach of a contract— is "improper," as occurred in *Compulife*.[323]

---

[320] 18 U.S.C. § 1839(5)(2016); UTSA, § 1. *See also* CAL. CIV. CODE § 3426, discussed in note 322infra.

[321] I concede that this distinction is debatable. A New York court recently drew this distinction, observing that while New York law defines misappropriation as including where "a defendant 'used the trade secrets in breach of an agreement' between the parties, the DTSA is narrower, defining "improper means" to include "through a breach of a contractual '*duty to maintain secrecy*.'" *See* Broker Genius, Inc. v. Zalta, 280 F. Supp. 3d 495, 511, n. 5 (S.D.N.Y. 2017) (emphasis added) (quoting § 1839(6)).

[322] The DTSA states that " the term "improper means"—(A)includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means; and (B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition[.]" 18 U.S.C. § 1839(6)(2018). California's UTSA states that: "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means. Reverse engineering or independent derivation alone shall not be considered improper means." Cal. Civ. Code § 3426.1 (West 2023), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=4.&title=5.&part=1.&chapter=&article The UTSA defines improper means as including "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means," see UTSA, § 1, and then goes on to identify reverse engineering as a proper means in a Comment. UTSA, § 1, cmt. ("Proper means include: Discovery by "reverse engineering", that is, by starting with the known product and working backward to find the method by which it was developed. The acquisition of the known product must, of course, also be by a fair and honest means, such as purchase of the item on the open market for reverse engineering to be lawful[.]").

[323] *See* notes 307 to 313 *supra*.

This is indeed what some courts have done. Both before and after the DTSA, some courts have determined that reverse engineering—when done in breach of a contract that prohibits reverse engineering —constitutes improper means of acquiring trade secrets.[324] Importantly, these cases are often in the business-to-business context. The defendant is another business subject to an ongoing duty of confidentiality established through a negotiated agreement that is specific to the parties' transaction. These are, in other words, arrangements between "insiders." Each participant agrees, in exchange for inside access to the other's information, that they will abstain from using or disclosing that information without authorization; and will abstain from reverse engineering the other party's products.[325] In these situations, the reverse engineering provision acts as a crucial supplement to the parties' *mutual* obligations to retain secrecy. The act of reverse engineering in such cases does not resemble picking apart a product that was lawfully purchased on the open market. It is a breach of the parties' ongoing confidentiality obligations. In fact, courts in these cases can typically just as well rely the theory that the defendant acquired, used, and/or disclosed trade secrets in breach of a duty to maintain secrecy.[326] Courts do not strictly need to rely on the theory that breach of an anti-reverse engineering clause, alone, constituted acquisition through "improper means."

End user cases look very different from business-to-business cases or, for that matter, from employee cases. As Mark Lemley puts it, "[c]ontract law is at its strongest where there is an actual agreement between the parties. That is, after all, the basis of a contract."[327] When businesses or employees agree to terms of an agreement that significantly limit what they can do, this is just an ordinary contract that, all else being equal, the law should enforce.[328] But this is not what end user cases look like. In end user cases, the person doing the reverse engineering typically has no prior

---

[324] *See, e.g.,* Rust-Oleum Corp. v. NIC Indus., 2023 U.S. Dist. LEXIS 190585, *31-32 (U.S. D. Ct. D. Oregon 2023) (holding that the defendant, a company with whom plaintiff had negotiated a Sales Agreement, was liable for reverse engineering plaintiff's product because the parties' Sales Agreement prohibited reverse engineering) (applying Oregon Trade Secret Act). *See also, e.g.,* Advanced Analytics, Inc. v. Citigroup Global Markets, Inc., Not Reported in F.Supp.2d. 2009 WL 7133660, * 3, 20 (S.D.N.Y. 2009) (holding that obtaining computer code from a software product in breach of negotiated Mutual Non–Disclosure Agreement, which also included a no-reverse engineering provision, was misappropriation) (applying New York common law).

[325] See discussion of this distinction in Hrdy & Seaman, *supra* note 25, at 682-83.

[326] 18 U.S.C. § 1839(5)(A)-(B)(2018); Hrdy & Seaman, *supra* note 25, at 686.

[327] *See* Lemley, supra note 11, at 1286.

[328] *Id*.

relationship with the trade secret holder, they have no underlying obligation of confidentiality, and they did not specifically negotiate a license with the trade secret holder. The end user has instead entered what the law considers a "contract of adhesion"— a mass-market, non-negotiated EULA or terms of use on which the end user has no expertise and for which they likely received no legal advice.[329] If this agreement happens to contain an anti-reverse engineering provision, this cannot be considered part of a negotiated exchange. It cannot be considered a mere adjunct to an underlying confidentiality or secrecy obligation.

Even if an anti-reverse engineering in an end user license agreement clause is enforceable under contract law—which it may well be, given how contract law currently treats these provisions[330]—breach of this provision should not give rise to trade secret law liability. The reason is that it is extremely hard to distinguish reverse engineering an information good—say, software—from reverse engineering a physical product that a consumer purchased on the open market. Trade secret law does not stop the consumer from picking the physical product apart.[331] Why should it stop the end user from picking apart the software? The situations are too difficult to distinguish from one another.

The fact that distribution of software products—and, now, generative AI products— are structured as "services" and are "licensed" to users rather than "sold" should not magically escape

[329] *Id*. at 1286-87 (discussing the difference between negotiated contracts and "contracts of adhesion" entered with consumers). *See also* Lobel, *supra* note 221, at 889.

[330] *See, e.g.,* Lemley, *Terms of Use*, *supra* note 15, at 459-64 (discussing trend in courts of enforcing "shrinkwrap" and "browsewrap" licenses). *See also* Chen, *supra* note 24, at 802-809 (discussing various preemption arguments and concluding that in general courts have been enforcing anti-reverse engineering clauses, though noting possible new preemption arguments under the DTSA).

[331] To reiterate, trade secret law authorities have long considered picking apart a product obtained on "the open market" to be the definition of reverse engineering, and a "proper means" of obtaining a trade secrets. *See* note 300 *supra.*

this characterization. Unlike in patent law,[332] and unlike in copyright law,[333] in trade secret law, there is no statutory language supporting drawing a distinction between a sale and a license. The statute just says that reverse engineering is a proper means of obtaining trade secrets.[334] Whether the person reverse engineers trade secrets from a product that they own, or from a "service" to which the person has a "license" is *not* dispositive.[335] When someone obtains access to a generative AI product, and has not undertaken any obligation of confidentiality, this person should generally have a successful reverse engineering argument—regardless of the presence of an anti-reverse-engineering clause in a EULA or terms of use. Unlike someone in a business-to-business or

---

[332] In patent law, structuring a sale of an invention as a license can allow an eventual patent applicant to escape the "on sale bar"—meaning the patent can be granted despite a prior license of the invention to a third party. Courts have found that a license of the invention does not necessarily trigger the on-sale bar, all else being equal, because the statute uses the words "on sale." PETER S. MENELL, ROBERT P. MERGES, MARK A. LEMLEY & SHYAMKRISHNA BALGANESH, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE: 2023, VOL. I: PERSPECTIVES, TRADE SECRETS & PATENTS 202 (2023) (discussing 35 U.S.C. § 102)).

[333] In copyright law, if a copyrighted good is transferred to a third party under a license, the licensee does not technically become an "owner" of the good, and so courts have held that major protections for "owners," like the essential step defense and the first sale defense, don't apply. Guy Rub, *Against Copyright Customization*, 107 IOWA LAW REVIEW 677 (2022); *see also* Camilla Hrdy, Guy Rub: Copyright or Contract? WRITTEN DESCRIPTION, Monday, May 17, 2021, https://writtendescription.blogspot.com/2021/05/guy-rub-copyright-or-contract.html

[334] *See* note 300 *supra.* The Commentary to the UTSA mentions a "purchase" but only as illustrative of proper means. *See, e.g.,* UTSA, § 1, cmt. (stating that "acquisition of the known product must, of course, also be by a fair and honest means, *such as purchase of the item on the open market* for reverse engineering to be lawful[.]") (emphasis added).

[335] To be clear, the distinction is *relevant*. In deciding whether information is "readily ascertainable," and in deciding whether a trade secret holder took "reasonable" measures to keep certain information secret, courts would absolutely ask whether the trade secret holder utilized contractual restrictions, such as a nondisclosure agreement or an anti- reverse-engineering clause, to control access to their information. But the license-versus-sale distinction is not dispositive. The licensor of a service can lose trade secrets just as well as the seller of products. *See generally* Life Spine, Inc. v. Aegis Spine, Inc., 8 F.4th 531, 535-538 (7th Cir. 2021) (holding sale of spinal implants to hospitals and surgeons not "readily ascertainable" even though they were available for hospitals and surgeons to purchase on the open market in part because plaintiff retained control over distribution and use of the spinal implants and only distributed them through distributors who signed confidentiality agreements). *See also, e.g.,* Andrew Beckerman-Rodau, *The Choice Between Patent Protection and Trade Secret Protection: A Legal and Business Decision*, 84 J. Pat. & Trademark Off. Soc'y 371, 389-396 (2002) (discussing strategy of preserving trade secrecy in a technology by ensuring it will "only be sold to a limited number of third parties" or "licensed pursuant to a contractual agreement which forbids reverse engineering and which requires the licensee to maintain the technology in strict secrecy.").

employment relationship, their only "bad act" is reverse engineering in the face of a contract that prohibits the same. This can support a breach of contract claim, assuming the contract is held to be enforceable.[336] It cannot support a trade secret misappropriation claim.

This has not, unfortunately, stopped software owners from suing end users for trade secret misappropriation when they reverse engineer software in breach of an anti-reverse engineering clause. Two of the major cases addressing this issue were decided under California trade secret law. The first case is the California Supreme Court case, DVD Copy Control Association v. Bunner.[337] The basic fact pattern was that someone (Jon Johansen) reverse engineered putative trade secrets in violation of a no-reverse-engineering clause in an end user license agreement; then another person—Andrew Bunner, who did not undertake a no-reverse-engineering obligation—posted the information on his website.[338] DVD Copy Control Association sued Bunner for trade secret misappropriation, arguing that Bunner had disclosed trade secrets knowing they were obtained (by Johansen) using "improper means."[339] The lower court, with almost no discussion, accepted the plaintiff's argument that if the information were obtained through reverse engineering—*and if this reverse engineering were done in breach of a contract*—this would constitute acquisition of trade secrets by "improper means."[340] The case was appealed up the

---

[336] Courts have often enforced contracts that go beyond intellectual property protections under various theories. But there are limitations on enforceability. *See* Hrdy & Seaman, supra note 25, at 699-725 (discussing limits on enforceability of confidentiality agreements). On enforceability of anti-reverse engineering clauses, see Chen, *supra* note 24, at 802-809. *But see, e.g.,* Daniel Laster, *The Secret Is Out: Patent Law Preempts Mass Market License Terms Barring Reverse Engineering for Interoperability Purposes*, 58 BAYLOR LAW. REV. 621, 624-25 (2006) (arguing that patent law preempted anti-reverse engineering clauses).

[337] DVD Copy Control Ass'n, Inc. v. Bunner, 31 Cal.4th 864 (Cal. 2003).

[338] The facts were a bit complicated. The Plaintiff, DVD Copy Control Association, licensed software capable of decrypting content on DVDs. Jon Johansen, a Norwegian resident, reverse engineered information embedded in software in violation of a license that prohibited reverse engineering. The software was distributed by another company that was a licensee of DVD Copy Control Association. Johansen then used that information to write a movie and DVD decryption program called DeCSS. DeCSS eventually appeared on other Web sites, including a Web site maintained by Andrew Bunner. DVD Copy Control Assn., Inc. v. Bunner, 31 Cal. 4th 864, 871–72, 75 P.3d 1, 7 (2003), as modified (Oct. 15, 2003)

[339] *Id*.

[340] "[R]everse engineering," the court stated, "could be considered 'improper means' … if whoever did the reverse engineering was subject to the click license agreement which … prohibited reverse engineering." DVD Copy Control Ass'n, Inc. v. McLaughlin, 2000 WL 48512, at * 2 (Sup. Ct. Santa Clara County 2000).

California Supreme Court. The Court accepted, *for purposes of the appeal*, that there were trade secrets; that Johansen acquired those trade secrets by "improper means"; and that "Bunner knew or had reason to know that [the subject matter he posted on his website] disclosed trade secrets acquired by improper means."[341] But the Court specifically declined to decide the crucial question—whether Johansen in fact acquired the trade secrets by "improper means" due to the fact that he reverse engineered the software in violation of a no-reverse engineering clause in the end user license agreement.[342]

Fortunately, Judge Moreno wrote in a concurring opinion that the lower court had been incorrect to assume that reverse engineering in breach of the no-reverse engineering clause was trade secret misappropriation. "[N]owhere," Judge Moreno wrote, "has it been recognized that a party wishing to protect proprietary information may employ a consumer form contract to, in effect, change the statutory definition of 'improper means' under trade secret law to include reverse engineering, so that an alleged trade secret holder may bring an action."[343] This concurrence turned out to be important, because it provided insight into the California Supreme Court's thinking on an issue that the Court did not in fact decide.

The second case, decided over a decade later, is Aqua Connect, Inc. v. Code Rebel. In *Code Rebel,* a federal court in the Central District of California cited to Judge Moreno's concurrence in order to explicit reject the argument that reverse engineering becomes improper means merely because done in violation of a contract.[344] In *Code Rebel* the defendant, Code Rebel, downloaded a trial version of plaintiff Aqua Connect's software and reverse engineered it to make a competing product in direct violation of an end user license agreement (EULA) that prohibited reverse engineering. [345] The court rejected the plaintiff's argument that breach of the EULA turned the act of reverse engineering into an improper means of acquiring trade secrets. "[T]he only improper means pled in the [complaint,]" the court wrote, "is reverse engineering, which according to California law, 'shall not be considered improper means' by itself. Though a breach of the EULA may support a cognizable breach of contract claim… the mere presence of the EULA does

[341] *See Bunner*, 31 Cal.4th at 875.
[342] *See Bunner*, 31 Cal.4th at 875, n. 5.
[343] *See Bunner*, 31 Cal.4th at 901 n. 5 (Moreno, J., concurring).
[344] Aqua Connect, Inc.v. Code Rebel, LLC, 2012 WL 469737, at *2 (C.D. Cal. Feb. 13, 2012) (citing *Bunner,* 31 Cal.4th at 901 n. 5 (Moreno, J., concurring)).
[345] *Code Rebel*, 2012 WL 469737, at * 2.

not convert reverse engineering into an 'improper means' within the definition of California trade secret law."[346]

Code Rebel is a very important decision. It did the work the majority of the judges on the California Supreme Court had declined to do in *Bunner*, putting to rest the argument that proper reverse engineering can become "improper" due to the mere presence of a EULA. The court also made clear that software owners in such cases can still bring a breach of contract claim. This is a natural solution, respecting the contract while not turning a breach of contract claim into a trade secret claim.

Unfortunately, even after *Code Rebel*, some courts have gone the opposite direction. For example, in Socal Diesel, Inc. v. Extrasensory Software, Inc., a California appeals court held that a "deliberate," "fraudulent," violation" of a EULA which "expressly prohibit[s]" reverse engineering can "constitute an improper means by which to reverse engineer" a trade secret.[347] The court conceded that California's UTSA states that "[r]everse engineering or independent derivation *alone* shall not be considered improper means."[348] But the court reasoned that the legislature's "[u]se of the word 'alone' indicates that reverse engineering attended by" some other wrongful act "is improper." [349] For example, if an end user of software "agreed to the EULA—which specifically prohibited reverse engineering—*with the intention of breaching it,* that would constitute an improper means of obtaining [plaintiff's] trade secret."[350]

The addition of an "intent" element is not helpful and is not supported by the law. Undertaking reverse engineering is a legal means of obtaining a trade secret. Whether this is done with the intent to breach a contract should not matter. The *Socal* court's focus on the California

---

[346] *Id*. at *2.

[347] Socal Diesel, Inc. v. Extrasensory Software, Inc., No. B290062, 2022 WL 702427, at *9 (Cal. Ct. App. Mar. 9, 2022), reh'g denied (Apr. 8, 2022) (holding for plaintiff and returning case to re-do trial under this newly stated rule).

[348] *Id*. at *9 (quoting Civ. Code, § 3426.1, subd. (a), italics added.)

[349] *Id*.

[350] *Id*. (emphasis added). The court oddly suggested that reverse engineering with "intent" to violate a no-reverse-engineering clause is equivalent to "fraud." *Id*. at *8–9 ("Reverse engineering accomplished by fraud is not reverse engineering alone. Entering into a EULA with the intention of violating its terms is fraud.").

trade secret statute's use of the word "alone" is misguided.[351] There is no basis for reading so much into this word. The court should simply have adopted the *Code Rebel* court's position, finding that "the mere presence of the EULA does not convert reverse engineering into an 'improper means' within the definition of California trade secret law."[352]

The *Code Rebel* position is much stronger now that a federal law, the DTSA, expressly states that the term "improper means" "does not include reverse engineering[.]"[353] As I'll explain in Part III.D., this provision of the DTSA arguably *preempts* state laws that prohibit reverse engineering, including state laws that generate trade secret liability based merely on breach of an anti-reverse-engineering clause. Reverse engineering in violation of an anti-reverse engineering clause cannot be classified as trade secret misappropriation, absent some other prohibited act, such as breach of a duty to maintain secrecy. If this position is adopted, this would mean that individual users of ChatGPT—or any other information goods that are widely distributed on the open market[354]— will not be liable for trade secret misappropriation merely based on reverse engineering.[355]

B. Readily Ascertainable Information Is Not a Trade Secret

There is another, potentially even more powerful doctrinal lever for finding trade secrecy has ended in a publicly-distributed information good: the not-readily-ascertainable requirement. This limitation on trade secret rights has been underused and misunderstood.[356] Below I explain how courts have erred and how they can change their approach.

Products that are distributed on the open market are hard to protect under trade secret law. This is by design. Patents are supposed to be the main option for protecting a new product against

---

[351] Federal trade secret law states that reverse engineering is a proper means. It makes no mention of the word "alone." 18 U.S.C. § 1839(6) (improper means "does not include reverse engineering, independent derivation, or any other lawful means of acquisition[.]").

[352] *Id*. at *2.

[353] 18 U.S.C. § 1839(6)(2016).

[354] This does not include situations where obtaining access to the product requires going through an employee or a business insider who is in a negotiated confidential relationship with the trade secret holder.

[355] Importantly, end users who breach an anti-reverse engineering clause can still potentially be liable for breach of contract, as the *Code Rebel* court recognized. In Part III.D., I question whether those contract claims might be preempted by the DTSA as well. *See* note 345 supra.

[356] *Accord* Charles Tait Graves, *What Is Readily Ascertainable?* (working paper, on file with the author).

competition.[357] Once reverse engineering becomes technologically feasible, trade secrets are supposed to end. If a trade secret can easily and cheaply be discerned by inspecting a publicly-distributed product, that information should be deemed "readily ascertainable by proper means" and thus unprotectable under federal trade secret law and the trade secret laws of most states.[358] Information is deemed readily ascertainable if it can be "readily copied as soon as [a product embodying this information] is available on the market[,]" and copying the information at issue is not time-consuming or expensive.[359] As one court recently put it, "readily" means "in a ready manner" such as "without hesitating" or "without much difficulty."[360] In some cases, courts have held that information is readily ascertainable and not a trade secret if it is plainly visible to users of a product,[361] or if it could be reverse engineered in a matter of hours, days, weeks, or potentially even months.[362] On the extreme end, some courts have held that the mere fact of selling a product on the open market, and making it available to reverse engineer, destroys trade secrets.[363]

Based on these basic principles, if information about a generative AI product is plainly visible to users, or can be gleaned from a generative AI using commonly-known techniques in a

---

[357] *See* Lemley, *supra* note 30, at 313.

[358] 18 U.S.C. § 1836(3); UTSA, § 1. *See also* Life Spine, Inc. v. Aegis Spine, Inc., 8 F.4th 531, 540 (7th Cir. 2021) ("[A] company may not publicly sell or display a product and then claim trade secret protection in information that is 'readily ascertainable' upon examination of the product.").

[359] *See, e.g.,* UTSA, § 1 cmt. *See also* Camilla Hrdy & Sharon Sandeen, *The Trade Secrecy Standard for Patent Prior Art*, 70 AM. U. L. REV. 1269, 1288-89 (2021) (defining "readily ascertainable" and comparing the concept to "generally known").

[360] Card Isle Corp. v. Farid, No. 1:21-CV-1971-TWT, 2023 WL 5618246, at *6 (N.D. Ga. Aug. 30, 2023) (citing Merriam-Webster and other case law).

[361] *See, e.g,* Beardmore v. Jacobsen, 131 F. Supp. 3d 656, 672 (S.D. Tex. 2015) (holding basic functionality of an app that can be seen by users and shared with others in screenshots is not a trade secret).

[362] Alpha Pro Tech, Inc. v. VWR Int'l, LLC, 2017 U.S. Dist. LEXIS 135507, * 22 (E.D. Pa. 2017) (trade secrets relating to laboratory apparel "readily ascertainable" because reverse engineering process would take "approximately two months[.]"; *see also, e.g.,* Flotec, Inc. v. S. Rsch., Inc., 16 F. Supp. 2d 992, 995, 1001 (S.D. Ind. 1998) (finding design of regulators sold on open market readily ascertainable when reverse engineering required "roughly six to eight months.").

[363] A small minority of courts have indicated that federal patent law "preemptively" requires this result, holding that once a product has been sold to a third party, trade secret rights end. *See* Roboserve v. Tom's, 940 F.2d 1441, 1455 (11th Cir. 1991); Acuson Corp. v. Aloka Co., 257 Cal. Rptr. 368, 374 (Ct. App. 1989), reh'g denied and opinion withdrawn (May 3, 1989). *See also e.g.* Charles Tait Graves & Elizabeth Tippett, *UTSA Preemption and the Public Domain: How Courts Have Overlooked Patent Preemption of State Law Claims Alleging Employee Wrongdoing*, 65 RUTGERS L. REV. (2012/2013).

short window of time, then this information should be deemed readily ascertainable and not protectable as a trade secret, period. However, things are not so simple. First, some states, including California, Illinois, and Oregon, have adopted non-uniform versions of the UTSA that do not include the not-readily-ascertainable limitation.[364] Second, even in jurisdictions that do include the not-readily-ascertainable limitation, many courts do not employ the correct analysis. They hold that information that is readily ascertainable from public sources is still a trade secret because the defendant did not get the information that way.[365] Third, most courts seem to agree that what counts as "readily" ascertainable is a question of fact,[366] and therefore courts tend to send the issue to a jury. The jury has significant discretion to decide that information is not "readily" ascertainable, even if it is possible to reverse engineer the information using public sources.[367] The

---

[364] *See* Cal. Civ. Code §§ 3426-3426.11 (West 2023); 765 Ill. Comp. Stat. 1065/1 to 1065/9 (2023); Or. Rev. Stat. §§ 646.461-646.475 (2023). Importantly, in California, the fact that information is readily ascertainable by proper means in theory be raised as an affirmative defense. CACI No. 4403. Affirmative Defense—Information Readily Ascertainable (2023) ("[Name of defendant] did not misappropriate [name of plaintiff]'s trade secret[s] if [name of defendant] proves that the [select short term to describe, e.g., information] [was/were] readily ascertainable by proper means at the time of the alleged [acquisition/use/ [or] disclosure]."), https://www.courts.ca.gov/partners/documents/judicial_council_of_california_civil_jury_instructions_2024.pdf, at 1253. *But see* James Pooley. *The Messy Process of Making and Applying the Law*, IP WATCHDOG, March 29, 2023 (criticizing California cases in which courts have held information that is theoretically readily ascertainable can still be protected, if defendant did not itself obtain the information that way). Notably, other doctrines can be applied to achieve a similar result. For example, information that can be easily reverse engineered may not be the subject of reasonable secrecy precautions or derive economic value from being kept secret. Hrdy, *supra* note 69, at 557.

[365] *See, e.g.,* GateGuard, Inc. v. Amazon.com Inc., No. 21-CV-9321 (JGK), 2023 WL 2051739, at *13–15 (S.D.N.Y. Feb. 16, 2023) ("[T]hese alleged methods of discovering trade secrets constitute 'improper means,' whether or not a third party with authorization to access the device could theoretically "reverse engineer" its design.") (denying motion to dismiss). *See also* Jeanne C. Fromer, *A Legal Tangle of Secrets and Disclosures in Trade: Tabor v. Hoffman and Beyond* (2013) (discussing historic case law where court allowed protection for information that was fully disclosed in a patent, because of how defendant obtained the information).

[366] *See* Life Spine, Inc. v. Aegis Spine, Inc., 8 F.4th 531, 540 (7th Cir. 2021) ("[W]hether the information is public is a question of fact.").

[367] *See, e.g.,* Gib. Servs. v. Res., Inc., 486 S.W.3d 224, 227-228 (Ct. App. Ark. 2016) (holding jury entitled to decide plaintiff's lubricant formulas were trade secret, even though defendant's expert testified that the formulas were "'simple, unsophisticated lubricants,' whose ingredients were 'readily detectable by widely available laboratory testing protocols' and that the "formulas' ingredients could be identified by performing two hours of testing on each lubricant, plus another

determinations of what is, or is not, "readily" ascertainable are so divergent that is hard to derive bright line rules. [368]

Finally, once again, contracts can change the rule altogether, potentially ensuring that information can *never* become readily ascertainable. The statutes clearly state that to be readily ascertainable, information must be readily ascertainable through "proper means."[369] To the extent breach of a contractual duty, alone, is deemed an "improper" means of acquiring trade secrets, then it is theoretically possible to keep information legally secret forever by attaching contractual terms that prohibit reverse engineering or sharing the information. For example, if it becomes possible for anyone to easily reverse engineer a generative AI product, but doing so requires breaching an anti-reverse engineering clause, or users are bound to keep any information they learn from the product confidential, then this information might *never* be deemed readily ascertainable through "proper" means. There are cases supporting this type of reasoning. As one court recently put it, applying the DTSA, "a trade secret is not 'readily ascertainable' simply because a party could purchase the trade secret… through a licensing agreement that places conditions on the scope of the buyer's use of the secret. Under such an agreement, although the buyer gains access to the trade secret, the buyer is restricted in its use of the secret, and therefore it cannot be said that the secret was readily ascertainable [370]

On this view, it would theoretically be possible to maintain trade secrecy *forever* by licensing trade secrets and information goods embodying trade secrets subject to users' promise to

---

six hours to ascertain the ingredients' relative weights, all at a cost of $3,000 to $4,500 per lubricant.").

[368] *See* Charles Tait Graves, *What Is Readily Ascertainable?* (working paper, on file with the author).

[369] 18 U.S.C. § 1836(3); UTSA, § 1.

[370] John Bean Technologies Corporation v. B GSE Group, LLC, 480 F.Supp.3d 1274, 1301 (2020) (holding on summary judgment that trade secrets in ground support equipment not readily ascertainable under DTSA when sold to distributors bound to nondisclosure agreements.). *But see* LinkCo, Inc. v. Fujitsu Ltd., 230 F. Supp. 2d 492, 499 (S.D.N.Y. 2002) (computer system's architecture is "easily ascertainable by the public once the product is marketed. Similar to the architecture of a building, once the combination of LinkCo's elements is seen by the public, the system's architecture will become obvious and easily duplicated.") (applying RESTATEMENT (FIRST) OF TORTS); In re Formsnet LLC, Case No. CGC-21-588988, 2021 Cal. Super. LEXIS 156625 *15-18 (Sup. Ct. Cal, 2021) (real estate software not a trade secret given that "the software features and functionality that FormsNet is claiming as its trade secret have long been available to hundreds of thousands of real estate agents" and there was no evidence a confidentiality provision informed users of their confidentiality obligations).

maintain confidentiality or refrain from reverse engineering. A recent illustration of a case applying this view is Life Spine, Inc. v. Aegis Spine, Inc., where the Seventh Circuit held that the plaintiff, Life Spine, owned trade secrets in a variety of information related to plaintiff's patented spinal implants.[371] The court found "the precise dimensions and measurements" of devices and their "interconnectivity" were not readily ascertainable—even though the implants were sold to hospitals and surgeons on the open market—because the plaintiff sold them through distributors who signed confidentiality agreements, and retained control over customers' use of the spinal implants. As the court put it, would-be competitors could "only learn such information if they have unfettered access to the device and specialized measuring equipment, and Life Spine does not allow third parties such access unless they first sign confidentiality agreements."[372] The court noted the possibility that others who were not bound by such agreements could get access to the implants and reverse engineer them, but the court dismissed this possibility, under the circumstances.[373]

Fortunately, not all courts have accepted the position. For example, in a very recent decision, Card Isle Corporation v. Edible Arrangements, a U.S. district court in the Northern District of Georgia rightly found that the plaintiff did not own trade secrets in the code for integrating the plaintiff's product into a client's website, because this code was fully revealed to users. [374] The court held the defendant, a client and licensee, *did* breach a nondisclosure and anti-reverse engineering agreement by obtaining and using the code outside the scope of this agreement.[375] So the plaintiff did have a cognizable breach of contract claim. But the plaintiff could not get a trade secret claim too. The code (in this case) was not kept hidden from plaintiff's clients at all. It was accessible to clients "via a "right click" on any web browser." Thus, the

[371] Life Spine, Inc. v. Aegis Spine, Inc., 8 F.4th 531 (7th Cir. 2021) (applying the DTSA and the Illinois UTSA). *See also* P.H. Chen, *Trade Secret Protection on a Publicly Sold, Patented Spinal Implant Device: Life Spine, Inc. v. Aegis Spine, Inc.*, BIOTECHNOLOGY LAW REPORT, 2023, https://www.liebertpub.com/doi/abs/10.1089/blr.2023.29316.phc
[372] *Life Spine, Inc*., 8 F.4th at 535-536.
[373] *Id*. at 540-542 ("Distributors are bound by confidentiality agreements, so Aegis is left to suggest that surgeons or patients, who are not similarly bound, might reverse engineer the device. This speculative argument is hard to accept.").
[374] Card Isle Corp. v. Farid, No. 1:21-CV-1971-TWT, 2023 WL 5618246 (N.D. Ga. Aug. 30, 2023).
[375] *Id*. at * 15.

plaintiff failed to show the "code embedded in the Defendant's website was not readily ascertainable."[376]

This opinion is logically correct and difficult to disagree with. As a matter of *contract law,* parties are generally free to make these kinds of arrangements,[377] but this does not mean contracts can be used to turn a breach of contract claim into a trade secret claim. For example, a user who obtains an individual license to use ChatGPT should be liable for breach of contract, all else being equal, if they use non-public information revealed through that license to reverse engineer ChatGPT. But if anyone who has access to ChatGPT can do this at any time with ease and at little cost, it would be truly a legal fiction to call that information a trade secret. None of those users should be liable for misappropriating trade secrets, as opposed to only breach of contract. [378] In fact, under federal law and the law of most states, no one should be liable for trade secret misappropriation in that scenario—including true insiders like employees— because there is no more trade secret.

The contrary interpretation would permit trade secrecy protection for information that can cheaply and quickly be reverse engineered. As noted above, some state laws—specifically, California, Illinois, and Oregon—still protect readily ascertainable information as a trade secret, at least in scenarios where the defendant did not themselves obtain the information that way.[379] For example, if an insider like an employee gains access to ChatGPT training data through their work, they would be liable for trade secret misappropriation under California law, even if that information could *theoretically* be readily ascertained by others who do not have the same inside access.[380] But this is not the case under federal law and the law of most states. When the only thing preventing information from being deemed readily ascertainable is a EULA attached to a mass-marketed product, that information cannot be a trade secret.

---

[376] *Id*. at * 5-7. *See also Arkeyo*, 342 F. Supp. 3d at 630 (software made publicly available on internet when it was "immediately ready to install and download onto any computer," and used without modification "precisely because it was available in executable code on the zip file.")
[377] *See* Hrdy & Lemley, *supra* note 89, at 61, n. 296; Hrdy & Seaman, *supra* note 25, at 3035-3036.
[378] This is assuming that the product is available on the open market and that obtaining the product does not necessitate going through an employee or a business insider who is in a negotiated confidential relationship with the trade secret holder.
[379] *See* note 364.
[380] *See* note 364.

C. Contracts Cannot Replace "Reasonable" Secrecy Precautions

Trade secret law requires taking "reasonable" measures to maintain secrecy of any information claimed as a trade secret.[381] This is a standard, not a rule. To quote Judge Richard Posner, what constitutes "reasonable" precautions "depends on a balancing of costs and benefits that will vary from case to case and so require estimation and measurement by persons knowledgeable in the particular field of endeavor involved."[382] A trade secret owner who fails to take reasonable secrecy measures is somewhat analogous to the owner of real property who leaves it lying around, "abandoned" for anyone to find.[383]

In modern trade secret cases, meeting the reasonable secrecy measures standard often entails giving everyone who has access to the information sufficient "notice" that it is intended to be kept secret. As Deepa Varadarajan puts it, the primary policy reason for trade secret law's reasonable secrecy precautions requirement "should be to notify a relevant audience (employees and other business partners) about the existence and boundaries of claimed trade secrets and thus reduce information costs for that audience."[384]

Reasonable secrecy precautions is, by nature, difficult to satisfy after a product is sold on the open market, and the information that the company is claiming as a trade secret is fully or partially disclosed to users of the product. At one level, courts seem to understand this. In some cases involving software, courts have held that if a company sells software with features that are *plainly revealed to users*, those features cannot be trade secrets, all else being equal. For instance, in a case involving real estate software, a court found the putative trade secret holder failed to take reasonable measures to protect the "software features and functionality that [plaintiff] is claiming as its trade secret have long been available to hundreds of thousands of real estate agents."[385]

However, once again, contracts significantly enhance trade secrecy protection for publicly-distributed goods, because contracts themselves can prove companies took reasonable measures

---

[381] 18 U.S.C. § 1839(3).
[382] Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179–80 (7th Cir. 1991)
[383] *Id*. at 179.
[384] *See*, e.g., Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357, 357 (2017).
[385] Notably, the court also observed that there was no evidence a confidentiality provision informing users of their confidentiality obligations. *See* In re Formsnet LLC, Case No. CGC-21-588988, 2021 Cal. Super. LEXIS 156625 *15-18 (Sup. Ct. Cal, 2021).

to protect trade secrets.[386] In the context of software licensing, one of the most important ways a plaintiff can prove it took reasonable measures is by pointing to "the existence or absence of an express agreement restricting disclosure." [387] In practice, these agreements can themselves satisfy trade secret holders' requirement to take reasonable secrecy precautions—even if the information claimed as a trade secret is widely distributed to the general public, and even if the people entering these contracts do not consider themselves to be in a truly confidential relationship with the trade secret owner.[388] Thus, as Deepa Varadarajan puts it, "despite the important role that the [reasonable secrecy precautions] requirement plays in trade secret law, trade secret owners may elide it through strategic use of contract law."[389]

There is case law involving software licenses between businesses in which courts have held the presence of confidentiality and anti-reverse-engineering clauses, along with password protections, satisfies the licensor's requirement to take reasonable measures to protect trade secrets.[390] For example, in QSRSoft, Inc. v. Restaurant Technology, Inc., a court held a defendant liable for misappropriating trade secrets regarding the user interface and functionality of plaintiff's software, which plaintiff licensed to restaurants like McDonalds' franchisees through a password-protected system. The defendant obtained access to the software by inducing some of plaintiff's

---

[386] *See, e.g.,* AirWatch LLC v. Mobile Iron, Inc., No. 1:12-CV-3571-JEC, 2013 WL 4757491, at *3-4 (N.D. Ga. Sept. 4, 2013) (holding software licensed under a EULA could be protected as trade secret on motion to dismiss given that plaintiff alleged that it "consistently seeks to preserve its software's confidentiality by ensuring that its customers and prospective customers are subject to confidentiality obligations embodied in EULAs).

[387] Neural Magic, Inc. v. Facebook, Inc., No. CV 20-10444-DJC, 2020 WL 13819257, at *5 (D. Mass. May 29, 2020) (citing USM Corp. v. Marson Fastener Corp., 379 Mass. 90, 98 (1979) (quoting Kubik, Inc. v. Hull, 224 N.W.2d 80, 91 (Mich. App. 1974)).

[388] *But see, e.g.* Acuson Corp. v. Aloka Co., 257 Cal. Rptr. 368, 371–72 (Ct. App. 1989) (May 3,1989) ("[Confidentiality agreements] cannot prevent, the public from examining equipment that has been sold on the open market. …[S]uch agreements could not represent a reasonable effort to maintain their secrecy."). This opinion—which held goods sold on the public market cannot be trade secrets if they can be reverse engineered—was *withdrawn* by order of the court on Jun. 22, 1989.

[389] Varadarajan, *supra* note 19, at 1567.

[390] *See Altavion*, 226 Cal.App.4th at 60-62 (information is "not by necessity available to the public once the software … is placed on the market" so long as it "can only be accessed by authorized individuals by entering a password.") (citations removed); *see also, e.g.,* Kraus USA, Inc. v. Magarik, No. 17-CV-6541 (ER), 2020 WL 2415670, at *6 (S.D.N.Y. May 12, 2020) (plaintiff sufficiently protected its trade secrets because "information was maintained in [plaintiff's] computer system and … only available to [employees] with a username and password.").

customers to share their passwords, and then took screen shots.[391] Even though the screen shots revealed basic information that was plainly visible to users of the software, the court found plaintiff satisfied its duty to keep this information secret, because the software was password-protected and users were subject to license agreements limiting how they could use and share the software.[392]

This sort of case law would support that requiring end users to agree to terms of use that contain the trifecta of confidentiality clauses, no-reverse-engineering clauses, and password-protections, satisfies reasonable secrecy precautions—certainly for features that are encrypted or technologically hidden, like source code,[393] and potentially even for features that are revealed to users, like basic design and functionality.[394] This line of reasoning must have limits. If features of a product are plainly visible to users, or can easily be discerned by users with little effort, then continuing to release the product to the public under those circumstances constitutes failure to take reasonable secrecy precautions.[395]

Moreover, this calculus should be capable of change over time. Even if certain features of a product are not *currently* easy to reverse engineer, reverse engineering is likely to become easier in future; and when this occurs the legal rule needs to adjust.[396] As Elizabeth Rowe has observed, trade secrecy's reasonable measures requirement is constantly being updated in response to technological advances. New technological risks—whether it's a model extraction attack or a future advance that makes generative AI even more vulnerable to reverse engineering—should place a "higher duty of care on trade secret owners," so long as "the increased risks from

[391] QSRSoft, Inc. v. Restaurant Technology, Inc., 2006 WL 2990432, * 5-6 (N.D. Ill. 2006)
[392] *Id*. at *1, *6. *See also, e.g.,* ImageKeeper LLC v. Wright National Flood Insurance, 2020 WL 4677299, * 2-4 (D. Ct. Nevada 2020) (finding plaintiff likely took reasonable measures to protect basic functionality of software against defendant who made "clone mobile application" because plaintiff limited access only to customers who had proper login credentials and who agreed to a license agreement containing both a confidentiality agreement and an anti-reverse engineering clause).
[393] *See* note 13 *supra*.
[394] *See e.g., QSRSoft, Inc*., 2006 WL 2990432, at * 5-6; *Altavion*, 226 Cal.App.4th at 60-62 (concluding revealed software features like "design concepts" *can* be protected as trade secrets, assuming plaintiff uses nondisclosure agreements and limits access to users with passwords).
[395] The product's features have probably become readily ascertainable too. *See* cases in notes 370 and 388 *supra*.
[396] *C.f.* LaRoque, *supra*, at 438-438 (arguing it is now easier to decompile object code to discern source code); *see also* Sherkow, *supra* note 203.

technology are foreseeable."[397] If a company continues to market a generative AI product and make it widely accessible, even though the company knows, or should know, that it is now possible to easily, cheaply and quickly extract information about the product, there is a very strong argument that this company has forfeited any trade secrets it once had.

There is one final wrinkle. Recall that while the Business Terms contains a confidentiality provision for ChatGPT, the individual Terms of Use has no confidentiality provision. I think this could matter. At least for features plainly revealed to users, the absence of a confidentiality provision could create a risk to OpenAI's ability to protect trade secrets related to ChatGPT. There is case law suggesting that failing to include a confidentiality provision in software agreements forfeits trade secret protection for information—at least for features of the software that are plainly revealed to users.[398] For example, in the recent case, Turret Labs USA, Inc. v. CargoSprint, LLC, the Second Circuit dismissed a software company's trade secret claims under the DTSA and uder New York law because the plaintiff did not have "confidentiality or nondisclosure agreements in place" with users of its software. "[W]ithout confidentiality or nondisclosure agreements in this context, it is not apparent from [the agreement] that *any* user could not simply replicate the software after using it."[399] The court even suggested in *dicta* that the plaintiff's failure to employ confidentiality provisions for end users might destroy trade secrecy for back-end features accessed by a defendant who "hacked into the software to obtain unfettered access to … algorithms and other internal mechanics after getting login information from [another user.] Turret Labs has failed to plead how any of its security measures might have prevented such an unwanted intrusion." [400]

The current version of OpenAI's Term of Use for individual users does not have a confidentiality provision. It is possible a court could OpenAI has forfeited trade secrets that are plainly visible or easily accessible to ChatGPT users.[401] Although OpenAI could point to the fact

---

[397] Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17 GEO. MASON L. REV. 1, 3 (2009).

[398] *See* Broker Genius, Inc. v. Zalta, 280 F. Supp. 3d 495, 515-522 (S.D.N.Y. 2017) (denying motion for preliminary injunction based on claim for misappropriation of trade secrets because the Terms of Use "simply [did] not contain a confidentiality provision.") (citing cases).

[399] *See* Turret Labs USA, Inc. v. CargoSprint, LLC, No. 21-952, 2022 WL 701161, at *2–4 (2d Cir. Mar. 9, 2022).

[400] *Id*. at *2-4.

[401] The Business Terms provides a comparison point, showing OpenAI *did* demand confidentiality when it wanted to, but neglected to do so for individual users. *C.f. Broker Genius*, 280 F. Supp. 3d

that its Terms of Use contains other provisions, like an anti-reverse engineering clause, these clauses should not on their own suffice to generate an actual confidentiality obligation.[402] OpenAI could also point out that it requires individual users to obtain and enter a password in order to access ChatGPT.[403] However, courts will almost certainly look for express confidentiality provisions protecting the information as well.[404] Without a confidentiality provision or other signs of measures to preserve secrecy, it might be found that anything that is revealed from individuals' use of ChatGPT is not a trade secret, period.

D. The Argument for Preemption Under the DTSA

These arguments were strong prior to passage of the DTSA. But they are far stronger now. When Congress passed the DTSA in 2016, Congress deliberately included a provision clarifying "that reverse engineering and independent derivation of the trade secret do not constitute improper means."[405] This provision, codified in Title 18, Section 1839(6)(B), states that "the term 'improper means'… does not include reverse engineering, independent derivation, or any other lawful means of acquisition[.]"[406] Unlike California's trade secret statute, which the court in *Socal* (incorrectly) interpreted to encompass reverse engineering in intentional breach of a contract, due to the statute's addition of the word "alone" after reverse engineering,[407] the DTSA does not include any modifiers on the phrase "reverse engineering."[408] Reverse engineering is legal, period.

---

at 519 (observing plaintiff sometimes placed users under a duty of confidentiality but did not always do so, supporting failure to take reasonable measures).

[402] *See Broker Genius*, 280 F. Supp. 3d at 522 (rejecting argument that other provisions like anti-reverse-engineering clause make up for failure to find users to confidentiality agreements).

[403] *See Altavion*, 226 Cal.App.4th at 60-62) (suggesting in dicta that under California's UTSA a plaintiff can have a trade secret in information that "can only be accessed by authorized individuals by entering a password.") (citations omitted).

[404] *See, e.g.,* Taylor Made Express, Inc., Plaintiff, v. Brandy Kidd, et al., Defendants. Additional Party Names: Coreen Beeks, David Craig, Hurley Logistics, Inc., Laura Montanez, Top Shelf Expediting, LLC, No. 21 C 2903, 2024 WL 197231, at *5 (N.D. Ill. Jan. 18, 2024) (plaintiff did not take reasonable efforts as plaintiff did not use confidentiality agreements, even though plaintiff kept information "locked behind passwords," "providing logins only to employees and independent contractors who require it.").

[405] Defend Trade Secrets Act of 2016, S. REP. NO. 114-220, (2016), at 10 (discussing reason for including 18 U.S.C. § 1839(6)(B)(2018)).

[406] *See* 18 U.S.C. § 1839(6)(B)(2018).

[407] *See* notes 347 to 351 *supra* and accompanying text.

[408] *See* 18 U.S.C. § 1839(6)(B)(2018).

The DTSA's new reverse engineering provision gives rise to several novel preemption arguments. "Preemption" generally describes a situation in which federal law "preempts," or supersedes, a state law.[409] Preemption doctrine is typically based on the Supremacy Clause, Article VI of the Constitution, which provides that the laws of the United States "shall be the supreme Law of the Land . . . any Thing in the Constitution or Laws of any state to the Contrary notwithstanding."[410] A federal statute can preempt state law in two main ways: "express preemption," where Congress explicitly provides in a particular federal statute that state law is preempted, or implied preemption, where a court "determines that Congress implicitly intended to preempt a certain state law, or a certain field of state law, even if it did not do so expressly."[411]

As explained below, a state law that makes reverse engineering a form of trade secret misappropriation is preempted by federal law based on various implied preemption arguments, including so-called "actual conflict" preemption and "purposes and objectives" preemption.[412] Under either of these arguments, a state trade secret law prohibits an action that federal trade secret law considers to be legal reverse engineering, this generates a direct conflict between state and federal trade secret law, necessitating preemption under the Supremacy Clause.[413]

---

[409] *Federal Preemption of State Law,* 114 HARV. L. REV. 339, 339 (2000) ("[Preemption] is the doctrine by which Congress supersedes state law and establishes uniform federal regulatory schemes to ensure the smooth functioning of the national economy.").

[410] U.S. Const. Art. VI. *See also* Hillsborough Cnty., Fla. v. Automated Med. Lab'ys, Inc., 471 U.S. 707, 712–13 (1985) ("It is a familiar and well-established principle that the Supremacy Clause, U.S. Const., Art. VI, cl. 2, invalidates state laws that "interfere with, or are contrary to," federal law.") (quoting *Gibbons v. Ogden,* 9 Wheat. 1, 211, 6 L.Ed. 23 (1824) (Marshall, C.J.)).

[411] *See, e.g.,* Caleb Nelson*, Preemption*, 86 VA. L. REV. 225, 226-29 (2000) (explaining that the Supreme Court's "[preemption] taxonomy recognizes three different types of preemption: 'express' preemption, (implied) 'field' preemption, and 'conflict' preemption."); *see also* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 400 (4th Ed. 2011). For analysis of how patent preemption analysis applies to state trade secret law and state intellectual property laws in general, *see* Camilla A. Hrdy, *Getting Patent Preemption Right*, 24 J. INTELL. PROP. J. 1, 4 (2017); Camilla A. Hrdy, *State Patents as a Solution to Underinvestment in Innovation*, 62 U. KAN. L. REV. 487, 524-531 (2013) (discussing patent preemption case law as applied to a hypothetical state patent); *see also, e.g.,* Paul Heald, *Federal Intellectual Property Law and the Economics of Preemption*, 76 IOWA L. REV. 959 (1991); Douglas Lichtman, *The Economics of Innovation: Protecting Unpatentable Goods*, 81 MINN. L. REV. 693 (1997).

[412] *See* discussion *infra* at notes 418 to 427. *See also* Nelson, *supra* note 411*, at* 226-29.

[413] U.S. Const. Art. VI ("This Constitution, and the laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the authority of the United States, shall be the supreme law of the land.").

1. Express Preemption

"Express" preemption occurs when Congress indicats in the language of a statute that a certain state law is preempted. [414] There is no express preemption in the DTSA. In fact, the DTSA states, in Section 1838, that it does not generally preempt state law remedies "for the misappropriation of a trade secret[.]"[415] However, this provision does not shield a state trade secret claim that is based solely on reverse engineering, because reverse engineering is an act that the DTSA itself says is not "misappropriation of a trade secret" at all. Congress has only stated that claims for "misappropriation of trade secrets" are not preempted. [416] For other state law claims, courts should be free to engage in an implied preemption analysis.

2. Implied Preemption

There are three main types of implied preemption: "conflict preemption"—includes so-called "actual conflict" and "purposes-and-objectives" preemption—and "field preemption."[417] There is no field preemption in this situation. As just explained, Congress allows states to pass their own trade secret laws so did not stop them from occupying the field. But there is conflict preemption under both the "actual conflict" and the "purposes-and-objectives" analysis.

"Actual conflict" preemption occurs if there is an "actual conflict" between federal and state law.[418] An actual conflict can occur if it "impossible for a private party to comply with both state and federal requirements[.]'"[419] A classic example is where a state law "prevents someone from doing something that the federal government has given them a right to do."[420] This is exactly what is happening here. Federal trade secret law states that reverse engineering is a proper means of acquiring a trade secret. DTSA Section 1839(6)(B) modifies DTSA Section 1839(5), which lays

---

[414] Note, *Preemption As Purposivism's Last Refuge*, 126 Harv. L. Rev. 1056, 1057–58 (2013).
[415] 18 U.S.C. § 1838 (2016) (emphasis added).
[416] 18 U.S.C. § 1838 (2016).
[417] Note, *Preemption As Purposivism's Last Refuge*, 126 Harv. L. Rev. 1056, 1057–58 (2013).
[418] See Hrdy, *The Reemergence of State Anti-Patent Law*, *supra* note 47, at 190 (discussing different kinds of "implied 'conflict' preemption").
[419] English v. General Elec. Co., 496 U.S. 72, 79 (1990) (internal citations removed). *See also* U.S. Const. Art. VI ("This Constitution, and the laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the authority of the United States, shall be the supreme law of the land.").
[420] Hrdy, *Getting Patent Preemption Right*, *supra* note 411, at 4 (applying this concept to state laws the restrict enforcement of federal patents).

out several ways to misappropriate a trade secret by employing "improper means." [421] If an action that is alleged to be an "improper means" of acquiring a trade secret in fact constitutes reverse engineering, then there is no trade secret misappropriation. For example, if someone acquires a trade secret related to a generative AI product from someone else whom they know reverse engineered that information, then neither of those individuals is liable for trade secret misappropriation under the DTSA.[422]

If a state trade secret law provides that this act of reverse engineering is an improper means of acquiring a trade secret, there is a direct conflict between federal and state law. The state law has prevented one or more individuals from doing something that federal law has given them a right to do. The mere presence of a contract purporting to prohibit reverse engineering cannot change this rule. If a contract prohibits reverse engineering, then perhaps this contract can be enforced under state contract law; but the contract cannot be used to turn what federal law says is proper means into improper means.[423] If a state trade secret law provides that discovery of a trade secret in breach of an anti-reverse engineering clause is an improper means of acquisition, then this generates a clear conflict with federal trade secret law.[424] This is literally a situation where Congress says "you can do X; it's not trade secret misappropriation," and the state law says "you cannot do X; it is trade secret misappropriation."

This does not mean that states cannot provide for greater trade secret protections than federal law does. For example, as mentioned above, some states protect "readily ascertainable" information, even though federal law does not.[425] Some states have longer statutes of limitations than the DTSA.[426] But when it comes to the specific act of reverse engineering, Congress has

---

[421] There are three ways to misappropriate that entail improper means: (1) acquisition of a trade secret by someone who knows or should know the trade secret was acquired by improper means; (2) disclosure or use of a trade secret by someone who used improper means to acquire the trade secret; and (3) disclosure of use of a trade secret by someone who knows or has reason to know the trade secret was acquired by improper means. *See* 18 U.S.C. § 1839(5) (2018).

[422] That said, if an employee or business partner did the same thing, the employee might be liable under another theory—such as acquisition, use, or disclosure of trade secrets in violation of a duty to maintain their secrecy. *See* 18 U.S.C. § 1839(5)(B)((2018).

[423] *Accord* Chen, *supra* note 24, at 805.

[424] This is what Texas' statute provides. *See* note 318 *supra*.

[425] Cal. Civ. Code § 3426.1 (West 2023).

[426] Ohio's statute of limitations is four years. Ohio Revised Code Section 1333.66, The DTSA's is three years. 18 U.S.C. § 1836(d)(2018).

made clear that reverse engineering is not an improper means of acquiring a trade secret. If a state law makes someone liable for trade secret misappropriation for taking an action that federal law provides is not trade secret misappropriation, this state law must be preempted by federal trade secret law. There is a direct conflict between federal and state trade secret law.

The second form of implied preemption that is relevant in this context is so-called "purposes and objectives" preemption. Whereas an actual conflict occurs when it is impossible for a party to comply with both state and federal law, purposes and objectives preemption occurs when a state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[427] In this case, there is a clear conflict between a state law that holds reverse engineering is trade secret misappropriation, and the policies motivating federal trade secret law. The purpose of the DTSA was to protect "commercially valuable, proprietary information" "as a form of intellectual property" because Congress believed there was a "growing problem of trade secret theft" and that state laws lacked sufficient uniformity and jurisdictional reach to address the issue.[428] Congress sought to create a "[c]arefully balanced" new federal law in order "to ensure an effective and efficient remedy for trade secret owners whose intellectual property has been stolen."[429] Although Congress explicitly chose to so "without preempting State law," Congress did seek to "provide a single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved."[430] To retain the right balance, Congress created several constraints on trade secret liability under the DTSA, including the provision stating that reverse engineering is a proper means of acquiring trade secrets, [431] as well as other limiting provisions, including immunity for whistleblowers in certain circumstances,[432] limitations on injunctions brought against departing employees,[433] and protection for otherwise-lawful disclosures under the Freedom of Information Act.[434]

---

[427] *Id*. (quoting Wyeth v. Levine, 555 U.S. 555, 594-95 (2009)).
[428] Defend Trade Secrets Act of 2016, S. REP. NO. 114-220, (2016), at 1-2.
[429] Defend Trade Secrets Act of 2016, S. REP. NO. 114-220, (2016), at 14.
[430] Defend Trade Secrets Act of 2016, S. REP. NO. 114-220, (2016), at 14.
[431] 18 U.S.C. § 1839(6)(B)(2018).
[432] 18 U.S.C. § 1833 (2018).
[433] 18 U.S.C. § 1836(3)(A)(i)(I)-(II) (2018).
[434] 18 U.S.C. § 1838 (2018) (stating that the DTSA will not "affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).").

A state trade secret law that offers greater protection than the DTSA is not *necessarily* in conflict with the DTSA. The Supreme Court has held that states can potentially offer additional protections for intellectual property and can protect subject matter that federal intellectual property laws leave behind. For example, in Goldstein v. California, the Court upheld a state law prohibiting copying of sound recordings at a time when federal copyright law did not protect sound recordings.[435] In Kewanee v. Bicron, Court upheld a state trade secret law at a time when federal law did not protect trade secrets—even though federal patent law existed in large part to encourage disclosure of inventions, rather than retaining secrecy.[436] The Court held that trade secret law and patent law could "co-exist" with one another because they did not interfere with one another, but instead complemented one another.[437] The court noted, for example, that "[t]rade secret law encourages the development and exploitation of those items of lesser or different invention than might be accorded protection under the patent laws, but which items still have an important part to play in the technological and scientific advancement of the Nation."[438]

However, once Congress has determined to protect subject matter under a particular intellectual property regime, states cannot generally protect the same subject matter based on standards that might conflict with the federal standards or protect subject matter that Congress has indicated it "wish[es] to remain free."[439] For example, in the Supreme Court's patent preemption

---

[435] Goldstein v. California, 412 U.S. 546, 551–52, 571 (1973) (holding that under the IP Clause California could prohibit unauthorized copying of sound recordings because California was exercising a power that it "retained under the Constitution" that was not taken away by the grant of power to Congress in the IP Clause). *See also* Art. I., Sec. 8, Cl. 8. *See also* Arthur Miller, *Common Law Protection for Products of the Mind: An Idea Whose Time Has Come*, 119 Harv. L. Rev. 705, 748–49 (2006) (discussing *Goldstein*'s implications for preemption of state laws prohibiting copying of undeveloped ideas); Jeanne Fromer, *The Intellectual Property Clause's Preemptive Effect*, in INTELLECTUAL PROPERTY AND THE COMMON LAW 265 (Shyam Balganesh, ed., 2013) (discussing *Goldstein* and the Supreme Court's IP Clause preemption case law).

[436] Kewanee v. Bircron, 416 U.S. 470, 493 (1974) (holding Ohio trade secret law not preempted by federal patent law).

[437] *Id*.

[438] *Id*.

[439] *See Goldstein*, 412 U.S. at 569 (distinguishing state protection for sound recordings, which were not protected under federal copyright law at all, from state protection for articles which Congress had indicated in the Patent Act that it "wished to remain free," such as articles that were already available to the public); *see also Bonito Boats, Inc.* v. Thunder Craft Boats, Inc., 489 U.S. 141, 151 (1989) ("The offer of federal protection from competitive exploitation of intellectual property would be rendered meaningless in a world where substantially similar state law protections were readily available. To a limited extent, the federal patent laws must determine not

jurisprudence, the Court has held again and again that states cannot provide "patent-like" protection for subject matter that Congress has declined to protect under federal patent law.[440] Otherwise, inventors might choose to rely on state law instead of federal law, declining to apply for federal patents, and foregoing the investment in innovation that federal patent law seeks to encourage.[441]

In this context, Congress has determined to offer federal protection against trade secret misappropriation, but Congress has also determined that reverse engineering is *not* a form of trade secret misappropriation. Congress did not spell out its justification for explicitly legalizing reverse engineering, but it is obvious—so ingrained that Congress did not need to state it.[442] Making lawful reverse engineering the "default rule" is good public policy for all the reasons discussed above.[443] Reverse engineering enhances competition.[444] Reverse engineering advances technological development and is " 'an essential part of innovation,' likely to yield variations on the product that 'may lead to significant advances in the field.'"[445] Reverse engineering maintains balance between the various intellectual property regimes, forcing those who cannot maintain secrecy in the face of the risk of reverse engineering to disclose their innovations and rely on patent and copyright protection if they can.[446]

---

only what is protected, but also what is free for all to use."). *See also* Hrdy, *State Patents as a Solution to Underinvestment in Innovation*, *supra* note 411, at 497, note 63 (discussing this preemption case law and stating that the Patent Act apparently creates "a negative inference that any objects that do not meet the federal standards of patentability cannot be similarly protected by state laws…")

[440] Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 160–61 (1989) (holding states cannot create patent-like rights patent-like" rights that do not meet Congress's "rigorous requirements of patentability" or that represent a "significant competitor" to U.S. patent rights."). *See also* Sears, Roebuck & Co. v. Stiffel Co., 376 U.S. 225, 232 (1964) (holding state unfair competition law could not prevent copying of unpatentable pole lamp); Compco Corp. v. Day-Brite Lighting, Inc., 376 U.S. 234, 238 (1964) (ruling state unfair competition law could not prevent copying of unpatentable lighting fixture).

[441] *See* Hrdy, *State Patents as a Solution to Underinvestment in Innovation*, *supra* note 411, at 524-531.

[442] Samuelson & Scotchmer, *supra* note 10, at 1583 (observing that "[t]he legal right to reverse-engineer a trade secret is so well-established that courts and commentators have rarely perceived a need to explain the rationale for this doctrine.").

[443] *See* notes and text at 190 to 201.

[444] Samuelson & Scotchmer, *supra* note 10, at 1583.

[445] *Id*. (quoting *Bonito*, 489 U.S. at 160).

[446] *Id*. at 1583-84.

These arguments for preemption under the DTSA are particularly compelling because the Supreme Court has already made them in its patent preemption cases in the course of considering whether state intellectual property laws interfere with federal patent law. In *Kewanee*, mentioned above, the Court held that state trade secret laws are not generally preempted by federal patent law, but the Court also indicated that state laws would be preempted if they prevented reverse engineering. "A trade secret law," the court wrote, "does not offer protection against discovery by fair and honest means, such as 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."[447] The court suggested that if trade secret law *did* prevent reverse engineering, inventors might choose trade secrecy instead of patenting and disclosing their inventions through the patent system—which would generate a conflict between trade secrecy protection and the purposes and objectives of patent law.[448]

Thereafter, in *Bonito Boats v. Thunder Boats, Inc*., the Court held that a state law that prevented copying of boat hulls that were unpatentable and freely available for anyone to copy, was preempted because it might create a competitor to the federal patent system—leading inventors to rely on the less rigorous standards of state law rather than innovating in order to obtaining federal patents.[449] The court implied in *Bonito* that one reason the boat hull law

---

[447] *Kewanee*, 416 U.S. at 476.

[448] *Id.* at 489-490 ("Trade secret law provides far weaker protection in many respects than the patent law. While trade secret law does not forbid the discovery of the trade secret by fair and honest means, e.g., independent creation or reverse engineering, patent law operates 'against the world,' forbidding any use of the invention for whatever purpose for a significant length of time. … The possibility that an inventor who believes his invention meets the standards of patentability will sit back, rely on trade secret law, and after one year of use forfeit any right to patent protection, is remote indeed.") (citations removed). *See also* Sharon K. Sandeen, Kewanee *Revisited: Returning to First Principles of Intellectual Property Law To Determine the Issue of Federal Preemption,* 12 MARQ. INTELL. PROP. L. REV. 299 (2008) (suggesting that state laws can go too far and be preempted by federal patent law if they prevent reverse engineering).

[449] *Bonito Boats*, 489 U.S. at 161 ("[U]nder the Florida scheme, the would-be inventor is aware from the outset of his efforts that rights against the public are available regardless of his ability to satisfy the rigorous standards of patentability. Indeed, it appears that even the most mundane and obvious changes in the design of a boat hull will trigger the protections of the statute. …Given the substantial protection offered by the Florida scheme, we cannot dismiss as hypothetical the possibility that it will become a significant competitor to the federal patent laws, offering investors similar protection without the *quid pro quo* of substantial creative effort required by the federal statute").

conflicted with the purposes and objectives of patent law was that it prohibited reverse engineering. "In essence, the Florida law prohibits the entire public from engaging in a form of reverse engineering of a product in the public domain. This is clearly one of the rights vested in the federal patent holder, but has never been a part of state protection under the law of unfair competition or trade secrets. … Reverse engineering of chemical and mechanical articles in the public domain often leads to significant advances in technology." [450]

These cases' reasoning suggests that a state law that prevents reverse engineering would be preempted not only by federal trade secret law, but also by federal patent law. One could argue, citing to *Kewanee* and *Bonito*, that if state trade secret law prevented reverse engineering, this would turn state trade secret law into a viable competitor to the patent system.

If any of these preemption arguments are accepted, then reverse engineering would be legal under both federal and state law. The addition of a contract prohibiting reverse engineering would not alter this rule. In many circumstances, reverse engineering a publicly-distributed generative AI model—or a traditional software product for that matter—would not be trade secret misappropriation under federal or state law, regardless of the presence of a boilerplate anti-reverse-engineering clause. End users who breach an anti-reverse engineering clause can still potentially be liable for breach of contract. The court in *Code Rebel*, discussed above, recognized the possibility of contract liability based on breach of an anti-reverse engineering clause, even though there is no trade secret liability.[451]

That said, post-DTSA, one could even argue that such a contract claim is preempted by the DTSA too, given that the DTSA explicitly states that the term "improper means…does not include reverse engineering[.]"[452] As noted above, the DTSA expressly does not preempt state law remedies "for the misappropriation of a trade secret[.]"[453] But this should not affect claims for breach of contract. Courts can still engage in implied preemption analysis and find that Section

But see Hrdy, *State Patents as a Solution to Underinvestment in Innovation*, *supra* note 411, at 524-531 (critiquing this decision and arguing that states should be able to create their own patents in certain circumstances).

[450] *Bonito*, 489 U.S. at 160.

[451] *See* note 345 supra.

[452] 18 U.S.C. § 1839(6)(2016).

[453] 18 U.S.C. § 1838 (2016) (emphasis added).

1839(6)(B) preempts contract claims based on anti-reverse engineering clauses.[454] Scholar Yang Chen agrees with this analysis, concluding that "[w]hile no case currently touches on this issue, it remains possible that such anti-reverse engineering clauses may be preempted by [the DTSA.]…The DTSA expressly allows the reverse engineering of trade secrets by excluding it from improper means. In light of this language, it is questionable whether a contractual prohibition of reverse engineering can withstand …preemption[.]"[455] Courts should not blindly follow precedents set for software that were incorrect at the time and that have effectively been overruled by the DTSA in the time since. They should not be deterred from finding a better path forward.

Conclusion

Generative AI is new, but this story is an old one. Generative AI presents an extreme case of a tension that we see all the time in trade secret law cases—the tension between factual secrecy, on the one hand, and legal secrecy, on the other.[456] Trade secret holders often use a combination of secrecy and contracts to try to turn factually non-secret information into proprietary information.

One of the main messages of this article is that ChatGPT's secrets are fragile and are likely to leak out to the public eventually. Today, many features of closed-source generative AI models are secret and difficult to discern from merely using the product, but over time, these features may become vulnerable to emerging methods of reverse engineering. However, precedents involving closed-source software suggest that generative AI companies will be able to use a combination of trade secret law and contract law to obtain legal protection for underlying generative AI technology— even after reverse engineering can be accomplished with relative ease. Terms of use and end user license agreements can be used to extend protection, even after reverse engineering becomes easier. Based on past case law involving software, generative AI users who violate these terms may be liable for trade secret misappropriation as well as breach of contract. This liability could even extend to third parties who knowingly obtain secrets from licensees.

---

[454] In the past, courts have rarely preempted contract claims even when they go beyond intellectual property rights, and courts may follow the same reasoning here, for better or worse. *See* discussion in Hrdy & Seaman, *supra* note 25, at 699-706 (discussing preemption of contract claims under trade secret law, patent law, and copyright law).

[455] *Accord* Chen, *supra* note 24, at 805.

[456] *C.f.* Sandeen & Aplin, *supra*, at 1; Tschider, *supra* note 5, at 710, 715;

This trajectory is not set in stone. With software, courts let contracts write the rules of trade secrecy. But courts are not necessarily bound by precedents that were generated for a different technology. Just because some software case law took a wrong turn, these precedents should not be controlling on what is fundamentally a new technology. The stakes for innovation, competition, and transparency are too high. In fact, generative AI presents a unique opportunity for courts to revisit some of the software case law, where courts allowed trade secrecy to continue in perpetuity and allowed reverse engineering to trigger trade secret as well as contract liability.

I have identified three doctrinal levers that courts can use to ensure that generative AIs that are widely distributed to the public do not benefit from perpetual trade secrecy protection. First, reverse engineering, on its own, should never be considered a form of trade secret misappropriation. Contracts cannot be used to transform otherwise-legal reverse engineering into an improper means of acquiring information. Passage of the DTSA in 2016 makes this argument more compelling than it was in previous cases involving software, because the DTSA explicitly states that reverse engineering is not an improper means of acquiring trade secrets as a matter of federal law.[457] Second, trade secrets are supposed to end when they become readily ascertainable through proper means. If a trade secret can easily and cheaply be discerned by inspecting a publicly-distributed product, this should be deemed readily ascertainable through "proper" means. The mere presence of a mass-market, non-negotiated restriction on disclosure or reverse engineering should not, on its own, change this reality.[458] Third, trade secrets are, by statute, forfeited once the owner fails to take reasonable measures to keep the information secret. Contracts can help satisfy this requirement by creating a duty of confidentiality. But when a company continues to sell a product to the general public whose secrets are plainly visible or easily discernable from the product, it is not enough to point to the presence of a mass-market, non-negotiated confidentiality agreement.

This doctrinal approach will not ensure the end of ChatGPT's secrets today. And that is a good thing. Without some legal protection, companies might not distribute information goods at

[457] 18 U.S.C. § 1839(6)(2016). *See also* Kewanee v. Bircron, 416 U.S. 470, 476 (1974).
[458] To be clear, readily ascertainable by proper means does not include situations where obtaining access to the product requires going through an employee or a business insider who is in a negotiated confidential relationship with the trade secret holder.

all. But this doctrinal approach will make sure that, once reverse engineering is technically feasible, companies cannot maintain legal protection forever.