KEEPING CHATGPT A TRADE SECRET WHILE SELLING IT TOO

Camilla A. Hrdy[†]

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 expire 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 widespread public use.

This is what many companies did with software, and this is what some generative AI companies—including OpenAI, the developer of ChatGPT—are doing today. They are releasing their models in a closed source format that hides algorithms, code, training data, and underlying model architecture from users. And they are attaching contractual terms of use that limit users' ability to reverse engineer information about how the models work, and that prohibit using the outputs of a generative AI model to develop competing products.

Breach of these terms of use might seem like a mere contract violation. However, case law, and some state statutes, suggest otherwise. Reverse engineering in breach of contract can constitute trade secret misappropriation as well because breach of the contract transforms a lawful act of reverse engineering into an "improper means" of acquiring trade secrets. The prospect of trade secret law liability is highly significant. It means prevailing plaintiffs can

---

DOI: https://doi.org/10.15779/Z38FT8DM21

† 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, Katie Eyers, Jessica Frisina, Tait Graves, James Grimmelmann, Eric Goldman, Ellen Goodman, Paul Gugliuzza, Cynthia Ho, Thea Johnson, Lemley, Dave Levine, Jake Linford, Orly Lobel, Mike Madison, Mike Mattioli, Salil Mehra, Tim Murphy, Sarah Rajec, Sarah Ricks, Alexandra Roberts, Elizabeth Rowe, Guy Rub, Sharon Sandeen, Andres Sawicki, Jake Sherkow, Cathay Smith, Deepa Varadarajan, John Villasenor, Elenore Wade, and participants at the 2024 Rutgers Law Summer Faculty Workshop, 2024 Trade Secrets Virtual Workshop, Works in Progress in Intellectual Property (WIPIP) 2024 at Santa Clara Law, the M3 Workshop at Suffolk Law School, the Corporate Innovation and Legal Policy Workshop at University of San Diego School of Law, the Hofstra IP Colloquium at Hofstra University School of Law, the Intellectual Property Colloquium at Temple Law, and the Intellectual Property Owners Organization Trade Secret Committee. Many thanks to Devin P. Owens, J.D. Candidate at Akron Law, for his research, insights, prescience, and expertise on model extraction attacks, and many thanks to the editors at the Berkeley Technology Law Journal.

obtain trade secret law remedies, not just contract law remedies, and it means liability can extend to third parties who did not enter the contract.

Maintaining some legal protection for generative AI products is important. Otherwise, companies might not make their models available to the public at all. But trade secrecy protection should not last once reverse engineering becomes feasible and *factual secrecy* has ended. This argument is much stronger today than it was ten years ago, because the 2016 Defend Trade Secrets Act (DTSA) codifies the principle that reverse engineering is a lawful means of acquiring trade secrets as a matter of federal law. Thus, the DTSA should be interpreted to preempt state laws that say otherwise.

This approach will not eliminate trade secrecy protection for generative AI models. Companies can still rely on trade secrecy before reverse engineering becomes feasible, and they can still pursue claims against insiders, such as employees and business licensees, who have clear confidentiality obligations to the AI developer. But once a widely available AI model can be quickly and cheaply reverse engineered, companies cannot maintain trade secret protection indefinitely through contract.

TABLE OF CONTENTS

I. INTRODUCTION

Generative artificial intelligence is a species of artificial intelligence (AI). AI has been around for a long time.[1] However, generative AI has new capabilities that are extremely compelling to businesses and members of the general public. The most famous example of a generative AI is ChatGPT, a generative AI product[2] that was developed and distributed by OpenAI.[3] ChatGPT, 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, ChatGPT appears as an interactive chatbot, accessed through a smartphone application or a web browser, which can instantly spit out responses to users' prompts.[4] These responses are usually informative and

1. Artificial intelligence loosely means using computers to perform activities usually associated with human intelligence. Generative AI is a subset of AI to the extent it does that. Xavier Rodriguez, *Artificial Intelligence (AI) and the Practice of Law*, 24 SEDONA CONF. J. 783, 788–89 (2023); Ryan Abbott and Elizabeth Rothman, *Disrupting Creativity: Copyright Law in the Age of Generative Artificial Intelligence*, 75 FLA. L. REV. 1141, 1146 (2023); Gaétan de Rassenfosse, Adam B. Jaffee & Melissa Wasserman, *AI-Generated Inventions: Implications for the Patent System*, 96 S. CAL. L. REV. 1453, 1457 (2024).

2. This Article often uses the term "product" to describe generative AIs like ChatGPT, though it is meant for this term to encompass services too. *E.g.*, Andersen v. Stability AI Ltd., 700 F. Supp. 3d 853 (N.D. Cal. 2023) (describing the "Stable Diffusion" AI as a "software product").

3. OpenAI has close ties to Microsoft, which owns a very large stake in OpenAI but does not control the company. Microsoft offers its own AI, Azure OpenAI Service, based on OpenAI's technology. *Microsoft and OpenAI Extend Partnership*, OFFICIAL MICROSOFT BLOG, (Jan. 23, 2023), https://blogs.microsoft.com/blog/2023/01/23/microsoftandopenaiextendpartnership/.

4. Sources useful to understanding 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), https://www.vox.com/recode/2023/1/5/23539055/generative-ai-chatgpt-stable-diffusion-lensa-dall-e; Jacob W. S. Schneider, *Generative AI's Output: How Is It Created, and What IP Rights Should It Receive?*, HOLLAND & KNIGHT IP/DECODE BLOG (Oct. 3, 2023),

sometimes shockingly creative and insightful. They may match or exceed the quality of human-generated work.[5]

Generative AI products like ChatGPT[6] raise novel issues for trade secret law.[7] But the most practical challenge is an old one: How can "information goods" be protected under trade secret law while still generating profit from wide distribution to the general public? Generative AI, like books, music, and software,[8] is an information good. By design, information goods embed significant information about the product that is visible or potentially accessible to users through a process of "reverse engineering."[9] Companies face a unique trade secret law challenge when they distribute information

---

https://www.hklaw.com/en/insights/publications/2023/10/generative-ais-output-how-is-it-created-and-what-ip-rights; Amy Winograd, *Loose-Lipped Large Language Models Spill Your Secrets: The Privacy Implications of Large Language Models*, 36 HARV. J.L. & TECH. 615, 616–18 (2023); Maura R. Grossman, Hon. Paul W. Grimm (Ret.), Daniel G. Brown & Molly (Yiming) Xu, *The GPTJudge: Justice in a Generative AI World*, 23 DUKE L. & TECH. REV. 1, 10 (2023); Katherine Lee, A. Feder Cooper & James Grimmelmann, *Talkin' 'Bout AI Generation: Copyright and the Generative-AI Supply Chain*, J. COPYRIGHT SOC'Y (forthcoming 2025), https://ssrn.com/abstract=4523551. On AI and machine learning generally, see 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).

5. *But see, e.g.*, Jonathan H. Choi & Daniel Schwarcz, *AI Assistance in Legal Analysis: An Empirical Study*, 73 J. LEGAL EDUC. Minnesota Legal Studies Research Paper No. 21-22 (forthcoming 2025) (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).

6. There are many similar products to ChatGPT. *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 (Sept. 29, 2023), https://www.pcworld.com/article/2086819/chatgpt-alternatives.html.

7. *E.g.*, David S. Levine, *Generative Artificial Intelligence and Trade Secrecy*, 3 J. FREE SPEECH L. 559 (2023); *see also* Camilla A. Hrdy, *Trade Secrecy Meets Generative AI*, CHI.-KENT L. REV. (2025).

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

9. 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, 1579–95 (2002) (describing "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, 1908–10 (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).

goods to the public on a mass scale—as OpenAI is doing with ChatGPT. The reason is simple: Public distribution tends to destroy secrecy. Without secrecy, there can be no trade secret.[10]

However, companies overcame the public distribution challenge for software by employing a two-part solution.[11] First, 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, companies use contracts to maintain *legal secrecy*, even for features that users can potentially discern 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]

Many generative AI companies are following the same playbook that worked for software. First, they distribute generative AI models using a "closed source" structure that hides the model's inner workings from users.[16]

---

10. Camilla A. Hrdy & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV. 1, 1, 12–13 (2021).

11. *See* Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1243–44 (1995).

12. By factual secrecy, this Article means 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 infra* notes 411–416 and accompanying text.

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 accessible to users. Agency Solutions.Com, LLC v. TriZetto Grp., Inc., 819 F. Supp. 2d 1001, 1017–19 (E.D. Cal. 2011).

14. *See* Lemley, *supra* note 11, at 1243–44; *see also* Michael J. Madison, *Reconstructing the Software License*, 35 LOY. U. CHI. L.J. 275, 280–82 (2003); Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1195–1203 (2019); Jeanne C. Fromer, *Machines as the New Oompa Loompas: Trade Secrecy, the Cloud, Machine Learning, and Automation*, 94 N.Y.U. L. REV. 706, 717 (2019); *see also, e.g.*, ROGER M. MILGRIM & ERIC E. BENSEN, 1 MILGRIM ON TRADE SECRETS § 1.05 (LexisNexis 2025) (identifying case law recognizing trade secret protection for software code).

15. *See* Lemley, *supra* note 11, at 1245; Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 459 (2006); AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY (2016) (ebook); Nancy S. Kim, *Revisiting the License v. Sale Conundrum*, 54 LOY. L.A. L. REV. 99, 101 (2020); Mark A. Lemley, *The Benefit of the Bargain*, 2023 WIS. L. REV. 237, at 246, 256–58 (2023).

16. In this Article, "closed source" means generative AI models for which users are not given access to algorithms, training data, and/or underlying code. The focus here is on closed source models, but, importantly, even "open source" models do not necessarily reveal all the information needed to understand the model's functionality or how it was developed. A license may be required to access open source models too. *See* Khari Johnson, *Meta's Open Source Llama Upsets the AI Horse Race,* WIRED (July 26, 2023), https://www.wired.com/story/metas-open-source-llama-upsets-the-ai-horse-race/.

ChatGPT users, for example, generally have no idea how the underlying generative AI models work or how they reach their conclusions. Most users are not given access to the "model" at all. They interact with the user interface, which is technically a separate software system from the underlying generative AI model that generates responses to user queries.[17] From the users' perspective, ChatGPT is the ultimate "black box."[18] Second, generative AI companies utilize 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 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

17. Lee et al., *supra* note 4, at 5, 41–42 (discussing "closed source" generative AI models). *See* discussion *infra* Part II.

18. Saurabh Bagchi, *What Is an AI 'Black Box'?*, GIZMODO (May 28, 2023), https://gizmodo.com/chatgpt-app-what-is-an-ai-black-box-1850481273; *ChatGPT Is a Black Box: How AI Research Can Break It Open*, 619 NATURE, 671–72 (July 25, 2023); Daniel Hardt, *Everyone Uses ChatGPT, but It Is a Black Box*: *Here's How to Make the Most of It*, COPENHAGEN BUS. SCHOOL (Oct. 10, 2023), https://www.cbs.dk/en/cbs-agenda/areas/news/everyone-uses-chatgpt-but-it-is-a-black-box-heres-how-to-make-the-most-of-it.

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, this Article uses 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*. The Article distinguishes 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 *infra* Part III.

21. This Article uses 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. Samuelson & Scotchmer, *supra* note 9, at 1577 (defining reverse engineering broadly as "the process of extracting know-how or knowledge from a human-made artifact.").

22. *Terms of Use*, OPENAI (Dec. 11, 2024), https://openai.com/policies/terms-of-use; *see also infra* Part III.

23. *See* 18 U.S.C. § 1839(6); Kewanee Oil Co. v. Bircron Corp., 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.

Terms of Use also contain a provision that will likely be construed as a noncompete.[25] The provision prevents ChatGPT users from employing the model's "[o]utput to develop models that compete with OpenAI."[26] The enforceability of ChatGPT's noncompete provision is highly uncertain, especially in light of recent antagonism towards noncompetes on the national stage.[27] Although noncompete agreements may be enforced when entered with other businesses, courts have struck down very similar provisions, even in business-to-business agreements.[28] As I will elaborate on later, 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 in the employment context.[29]

One might assume that the consequence of breaching these provisions would be limited to breach of contract. However, some case law indicates that breaching an anti-reverse engineering clause can give rise to *both* contract and trade secret liability since 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.[30]

The prospect of trade secret liability for what should be only breach of contract is highly significant. 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 assent to the contract.[31]

PA. J. INT'L L. 783 (2022) (discussing case law regarding enforceability of anti-reverse-engineering clauses in the U.S., as well as in E.U. and in China). *But see* Samuelson & Scotchmer, *supra* note 9, 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 into by workers. Workplace noncompetes are unenforceable in some states and, in all states, are subject to "reasonableness" standards. Camilla A. Hrdy & Christopher B. Seaman, *Beyond Trade Secrecy: Confidentiality Agreements That Act Like Noncompetes*, 133 YALE L.J. 669, 673–74 (2024).

26. OPENAI, *supra* note 22 (emphasis added); *see also* discussion *infra* Part III.

27. For example, the Federal Trade Commission (FTC) announced in April 2024 that entering a noncompete with a worker is a violation of the FTC Act. *See* 16 C.F.R. § 910 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/noncompete-rule.pdf.

28. There is at least one case holding that a very similar provision was unenforceable due to its lack of a time limit. *Infra* notes 301–303.

29. *See infra* Part III.

30. *See infra* notes 370–371.

31. 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 701–02 (discussing tortious interference with contract claims brought against companies that induce others to breach confidentiality agreements).

For example, if someone reverse engineers information about ChatGPT in violation of a term of use, and then shares that information with a third party who publicly releases the information, both actors could be liable for trade secret misappropriation. A court could grant an injunction and award damages far in excess of actual losses, as well as attorney's fees. These remedies are not generally available under contract law. 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. 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 create trade secret law liability for information goods[34] that are no longer *factually* secret, there 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 detrimental to innovation and competition. It hinders others' ability to build on and improve foundational tools, harms consumers by reducing choice and raising prices, and 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

32. *See* 18 U.S.C §§ 1831–1832 (defining 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 term 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, 170–74 (2022); *see also* Van Buren v. United States, 593 U.S. 374, 394 (2021) (noting that if CFAA applied to any action done in violation of "restrictions on website providers' computers" this could "criminalize everything from embellishing an online-dating profile to using a pseudonym on Facebook.").

33. *See* Lemley, *supra* note 31, at 313, 339–40 (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 supra* note 12.

35. Lemley, *supra* note 31, at 350–51.

36. *See* Samuelson & Scotchmer, *supra* note 9, at 1583 (discussing various justifications for reverse engineering); *see also* 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 the ability to improve upon products by deriving different end products).

37. *See* Lemley, *supra* note 31, at 341–42.

secrets, patents require disclosure and their protections end 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]

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. A trade secret law claim requires proving that information is sufficiently secret, derives economic value from secrecy, and has been the subject of reasonable measures to maintain the information's secrecy.[43] 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

38. *See* 35 U.S.C. §§ 112, 154 (2018).

39. Lemley, *supra* note 31, at 341–42 (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 the 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 SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 381–405 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011) (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 disclosing algorithms used in the criminal justice system); Sander Vogt, *Show Me Your Secrets: How the Use of Trade Secrets Relates to the Demand for Transparent Artificial Intelligence – Part I*, 5 J. ROBOTICS, A.I. & L. 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*, INT'L REV. INTELL. PROP. AND COMPETITION L. (2023) (discussing tension between the EU AI disclosure obligations and trade secrets); *see also* Elizabeth A. Rowe & Nyja Prior, *Procuring Algorithmic Transparency*, 74 ALA. L. REV. 303 (2022) (discussing that the solution to lack of AI transparency in criminal justice system is negotiation with the government over appropriate disclosure terms and conditions).

42. Again, by factual secrecy, this Article means not plainly visible or readily ascertainable to users of the product because they can be easily reverse engineered. *See infra* notes 411–416 and accompanying text.

43. *See infra* notes 75–78.

trade secret. The mere presence of confidentiality agreements and anti-reverse engineering clauses cannot magically transform non-secret information into a trade secret.[44] Various doctrines support 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 because it has been rendered generally known or readily ascertainable. 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.[45]

These arguments were strong prior to the passage of a federal trade secret statute in 2016, the Defend Trade Secrets Act (DTSA).[46] And they are far stronger now. When Congress passed the DTSA in 2016, Congress explicitly included a provision, 18 U.S.C. § 1839(6)(B), which states that reverse engineering is not an "improper means" of acquiring a trade secret.[47] 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.[48] One of these preemption arguments—which I newly 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.[49] If a state trade secret law imposes liability for reverse engineering, this creates a direct conflict between state and federal law, necessitating preemption under the Supremacy Clause of the Constitution.[50]

Giving life to the DTSA's new preemption doctrine will not ensure the end of ChatGPT's trade secrets today. Companies can still rely on trade secrecy during the period before reverse engineering becomes readily achievable. Companies can still bring claims for breach of contract.[51] And companies can

44. *See infra* Part IV.

45. *See infra* Part IV.

46. *See infra* note 335.

47. *See* 18 U.S.C. § 1839(6)(B) ("[T]he term 'improper means'. . . does not include reverse engineering, independent derivation, or any other lawful means of acquisition . . . .").

48. *See* Camilla A. Hrdy, *The Reemergence of State Anti-Patent Law* 89 U. COLO. L. REV. 133, 158 (2018) ("'Preemption' generally describes a situation in which federal law 'preempts,' or supersedes, a state or local law."); *see also infra* note 462.

49. *See* discussion *infra* Section IV.D.

50. *See* discussion *infra* Section IV.D; *see also* U.S. CONST. art. VI.

51. That said, as discussed in Section IV.D., the DTSA can also be construed to preempt state contract claims that prohibit reverse engineering in contravention of 18 U.S.C.

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 II, the Article explains that many features of generative AI models are currently hidden from users and kept factually secret, despite widespread distribution to the public. These features—including algorithms, source code, training data, and various aspects of the models' overall technical architecture—will likely benefit from substantial trade secret protection.[52] However, generative AI models' trade secrets are highly vulnerable to reverse engineering through a variety of methods, such as "data scraping,"[53] "model

§ 1839(6)(B). However, the argument for preemption of contract claims is comparatively weaker than the argument for preemption of state trade secret law claims. *See infra* notes 508–524 and accompanying text.

52. *See* Sharon K. Sandeen & Tanya Aplin, *Trade Secrecy, Factual Secrecy and the Hype Surrounding AI*, *in* RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND ARTIFICIAL INTELLIGENCE 443–60 (Ryan 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 URQUHART & SULLIVAN, LLP, THE RISING IMPORTANCE OF TRADE SECRET PROTECTION FOR AI-RELATED INTELLECTUAL PROPERTY (2020), https://www.quinnemanuel.com/the-firm/publications/the-rising-importance-of-trade-secret-protection-for-ai-related-intellectual-property/ [hereinafter "QUINN"] (discussing trade secrecy for AI-related technology); Gregory Gerard Greer, *Artificial Intelligence and Trade Secret Law*, 21 UIC REV. INTELL. PROP. L. 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 (Jens Schovsbo, Timo Minssen & Thomas Riis eds., 2020) (exploring the scope of trade secret protection for AI); Sarah Speight, *Protecting Artificial Intelligence via Trade Secrets*, WORLD INTELL PROP. REV. (Sept. 1, 2023), https://www.worldipreview.com/rankings/global-trade-secrets/protecting-artificial-intelligence-via-trade-secrets (discussing trade secrecy protection for AI).

53. Michael P. Goodyear, *Circumscribing the Spider: Trademark Law and the Edge of Data Scraping*, 70 KAN. L. REV. 295, 298 (2021) ("'Scraping' consists of using a computer program to inspect, collect, and aggregate data from different webpages.").

extraction attacks,"[54] "knowledge distillation,"[55] "prompt injection attacks,"[56] and other techniques that might be used now or in the future to strategically extract information from generative AI models.[57]

Indeed, reverse engineering of generative AI models is not a hypothetical possibility. Already, several generative AI companies, including OpenAI,[58] have alleged that "bad actors" are using "illegal techniques" to "steal" trade secrets from their models in order to develop competing systems. For example, in a recent complaint, the developer of the popular medical generative AI model, OpenEvidence Inc., alleged that there was "an emerging wave of bad actors who, rather than dedicate the time and expense needed to build up unique technology[,]" were employing "bad faith, improper, and illegal techniques designed to steal others' proprietary information and code."[59] Generative AI models' vulnerability to reverse engineering will only increase over time—making it much harder, if not impossible, to maintain factual secrecy.

However, in Part III, the Article shows how companies can use contracts 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

54. *See infra* notes 233–235 and accompanying text.

55. "Knowledge distillation is a sophisticated machine learning technique that allows smaller models to learn from larger, more complex ones." Houman Asefi, *The OpenAI vs DeepSeek Knowledge Distillation Dispute: Technical and Legal Implications*, MEDIUM (Jan. 30, 2025), https://houman-asefi.medium.com/the-openai-vs-deepseek-knowledge-distillation-dispute-technical-and-legal-implications-1e69d646b928. OpenAI recently accused DeepSeek of using model distillation to train its own models based on OpenAI's technology. John Werner, *Did DeepSeek Copy Off Of OpenAI? And What Is Distillation?*, FORBES (Jan. 30, 2025), https://www.forbes.com/sites/johnwerner/2025/01/30/did-deepseek-copy-off-of-openai-and-what-is-distillation/.

56. A "prompt injection attack" uses strategic inputs disguised as legitimate prompts in order to induce a generative AI model into revealing sensitive data. Matthew Kosinski, *What is a Prompt Injection Attack?*, IBM (Mar. 26, 2024), https://www.ibm.com/think/topics/prompt-injection#:~:text=In%20this%20type%20of%20attack,is%20more%20likely%20to%20comply.

57. *See infra* Section IV.A.

58. OpenAI has accused the Chinese developer of "DeepSeek" of "inappropriately" extracting ChatGPT data, using a technique called "distillation," in order to cheaply develop a "copycat" model. *See, e.g.*, Kevin Collier & Jasmine Cui, *OpenAI Says DeepSeek May Have 'Inappropriately' Used Its Data*, NBC NEWS (Jan. 29, 2025), https://www.nbcnews.com/tech/tech-news/openai-says-deepseek-may-inapproriately-used-data-rcna189872.

59. OpenEvidence Inc. v. Pathway Med., Inc., No. 1:25-cv-10471 (D. Mass. filed Feb. 26, 2025), at 6.

of use, each of which will help OpenAI keep ChatGPT's inner workings legally protected through contract law, and potentially also trade secret law.

In Part IV, 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.[60] But I argue those cases are either wrong, easily distinguishable, or effectively overruled in light of the passage of the DTSA.[61] Under a proper interpretation of several major trade secret law doctrines—the rule that reverse engineering is not an improper means of acquiring trade secrets; the rule that trade secrets end once they become readily ascertainable; and the rule that trade secret holders must take "reasonable" secrecy precautions—trade secrecy cannot be maintained in perpetuity for information goods that are made widely available to the general public. Finally, in light of the new language in the DTSA, clarifying that reverse engineering is legal under trade secret law, a state trade secret law that makes reverse engineering misappropriation is preempted under the Supremacy Clause.

II. TURNING TO TRADE SECRECY

Generative AI like ChatGPT is created by training algorithms[62] on a large universe of data, called "training data."[63] Generative AI algorithms use this data ("the inputs") to generate new content that is at some level derived from or based on the training data ("the outputs").[64] The process of training on massive amounts of data allows the algorithms to learn and improve to the

60. *See infra* Section IV.A.

61. *See infra* Section IV.D.

62. An algorithm is a set of instructions for solving a problem or accomplishing some end. Grossman et al., *supra* note 4, at 7.

63. 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 Copyright: Ongoing Lawsuits Could Affect Everyone Who Uses Generative AI*, 381 SCIENCE 158, 159 (2023); Matthew Sag, *Copyright Safety for Generative AI*, 61 HOUS. L. REV. 295, 313–16 (2023).

64. This Article uses "inputs" to refer to 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. *Cf.* Mark A. Lemley & Bryan Casey, *Fair Learning*, 99 TEX. L. REV. 743, 777 (2021) (discussing possible ways to understand inputs and outputs in the machine learning context).

point that they can eventually generate their own content. The outputs are not, generally speaking,[65] the same as the inputs; they are newly generated.[66]

Companies spend millions of dollars developing and training generative AI models.[67] They do not do this for free. They want to make money off their massive investments.[68] Intellectual property rights—which generally confer a limited right to prevent copying and competition—will be crucial for ensuring that AI companies can profit from their investments in this emerging field.[69] However, intellectual property rights come with costs, including limiting competition, raising prices, and "controlling the use of the intellectual work in subsequent products."[70] To the extent that AI models and related inventions are treated as intellectual property, these costs inevitably lead to tensions between different interest groups, and may raise 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?[71] What if an employee of an AI

65. 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 & James Grimmelmann, *The Files Are in the Computer: Copyright, Memorization, and Generative AI*, CHI.-KENT. L. REV. (forthcoming 2025); Matthew Sag, *A Response to Lee and Grimmelmann* (Feb. 21, 2024), https://matthewsag.com/a-response-to-lee-and-grimmelmann/.

66. *See supra* note 4.

67. Thomas H. Davenport & Nitin Mittal, *How Generative AI Is Changing Creative Work*, HARV. BUS. REV. (Nov. 14, 2022), https://hbr.org/2022/11/how-generative-ai-is-changing-creative-work; *see also* Jonathan Vanian, *ChatGPT and Generative AI Are Booming, but the Costs Can Be Extraordinary*, CNBC (Mar. 13, 2023), https://www.cnbc.com/2023/03/13/chatgpt-and-generative-ai-are-booming-but-at-a-very-expensive-price.html.

68. OpenAI is in part a nonprofit, but not really. Matt Levine, *OpenAI Is a Strange Nonprofit*, BLOOMBERG (Nov. 21, 2023), https://www.bloomberg.com/opinion/articles/2023-11-21/openai-is-a-strange-nonprofit.

69. To varying degrees, intellectual property rights give a right to exclude and allow the owner to prevent others from competing with them. The government does this in order "to encourage inventors and authors to invest in the development of new ideas and works of authorship." 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, at 22 (2023).

70. *Id.* at 22 (noting that "[g]ranting inventors and authors rights to exclude others from using their inventions, discoveries, and expression limits the diffusion of those ideas and so prevents some others from benefiting from and building upon these advances, at least for the duration of intellectual property protection . . . . These rights enable those possessing intellectual property rights to charge monopoly prices or to otherwise limit competition, such as by controlling the use of the intellectual work in subsequent products.").

71. *See* 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

company wishes to leave and work for a competitor—can they share or use information they learned from their original employer?[72] What if a member of the public wants to reverse engineer a generative AI model to figure out how it works—can they do so, and under which laws might they be liable?[73] If the government wants to regulate generative AI by forcing companies to disclose information about how the models were trained, can it do so if some or all of this information is considered a trade secret that cannot be freely disclosed to the public?[74]

This Article will not address all 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 will likely be increasingly vulnerable to reverse engineering. All else being equal, reverse engineering *should* eventually destroy information's trade secret status. In Part III, I go on to show how contracts can be used to extend the life of trade secret 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 DTSA and the Uniform Trade Secrets Act (UTSA) as "information"[75] that is not "generally known" or "readily ascertainable through proper means,"[76] that derives "independent economic value" from secrecy sufficient to give the owner an actual or "potential"

---

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).

72. Hrdy & Lemley, *supra* note 10 (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 LOVE LEAKS, RAIDS, AND FREE-RIDING, 1–12 (2013) (discussing trade secret law and other legal limitations on employee mobility and knowledge sharing).

73. Samuelson & Scotchmer, *supra* note 9, 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.").

74. *See* Christopher J. Morten, *Publicizing Corporate Secrets*, 171 U. PA. L. REV. 1319, 1327 (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).

75. 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").

76. 18 U.S.C. § 1839(3) (2016); UTSA § 1.

economic advantage over others,[77] and that the putative owner has taken "reasonable measures" to keep secret.[78]

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."[79] There are a few main categories of civil trade secret defendants.[80] The most common category consists of current or former employees of the trade secret holder, as well as third parties who hire those former employees in order to obtain trade secrets.[81] The second most-common category includes 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.[82]

Finally, essentially *anyone*—both insiders and outsiders—can be liable if they use "improper means" to acquire trade secrets.[83] For example, a court recently suggested that using advanced automation techniques to "hack" into a public website to acquire trade secrets constitutes acquisition by "improper means."[84] Acquisition-by-improper-means can result in both direct and indirect liability.[85] Direct liability attaches to the person who acquires trade secrets using improper means; indirect liability attaches to third parties who

77. 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).

78. 18 U.S.C. § 1839(3)(A); UTSA § 1(4)(i).

79. 18 U.S.C. § 1839(5); UTSA § 1(2).

80. These defendants could potentially be liable for criminal trade secret theft as well, assuming they have the requisite intent. 18 U.S.C. §§ 1831–32 (1996).

81. Employees generally have a duty to maintain the secrecy of their employers' trade secrets. This duty is usually established by express confidentiality provisions in their employment agreements. 18 U.S.C. § 1839(5)(a)–(b); *see also* Hrdy & Seaman, *supra* note 25, at 682–83 (describing the duty of secrecy established through employee confidentiality agreements).

82. 18 U.S.C. § 1839(5)(a)–(b). As this Article will 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 is questionable whether they fall into this category.

83. *See* 18 U.S.C. § 1839(5)(a)–(b).

84. *See infra* notes 352–371 and accompanying text.

85. *See* ELIZABETH A. ROWE & SHARON K. SANDEEN, TRADE SECRET LAW: CASES AND MATERIALS 253–55 (3rd ed. 2021) (discussing direct and indirect pathways to misappropriation).

acquire trade secrets from that person when they know or should know the trade secrets were acquired by improper means.[86]

The easiest way to protect a generative AI model as a trade secret would be to use it only in-house.[87] However, while some businesses will surely develop generative AI tools for their own internal use,[88] 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.[89] Other companies will likely wish to distribute their AI products as widely as possible, as OpenAI has done.

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).[90] Individual end users have to sign OpenAI's mass-market terms of use, called simply "Terms of Use."[91] As this Article will discuss in depth in Part III, the Terms of Use create significant limitations on what users can do, though they come 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 use ChatGPT to make new applications and end products.[92] Enterprise licensees pay negotiated fees and agree to special terms of use called the "Business Terms," which contain various restrictions on what licensees

86. 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).

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

88. *See* Andrew McAfee, Daniel Rock & Erik Brynjolfsson, *How to Capitalize on Generative AI: A Guide to Realizing Its Benefits While Limiting Its Risks*, HARV. BUS. REV. 43, 43–48 (Nov.-Dec. 2023) (advising businesses on when and how to adopt generative AI to improve operations).

89. Peter Henderson, Xuechen Li, Dan Jurafsky, Tatsunori Hashimoto, Mark A. Lemley & Percy Liang, *Foundation Models and Fair Use*, 24 J. MACH. LEARNING RSCH. 1, 4 (2023).

90. The subscription fee is currently $20 a month. *ChatGPT Pricing*, OPENAI, https://openai.com/chatgpt/pricing/ (last visited Nov. 26, 2024).

91. *Terms of Use*, *supra* note 22.

92. *ChatGPT Enterprise*, OPENAI, https://openai.com/chatgpt/enterprise/; *see also* Sachin Bhatmuley, David Kiernan, Carl Kukkonen III, Robert Latta, Ka-on Li, Mary Alexander Meyers, Mauricio Paez, Emily Tait, Kerianne Tobitch & Undine von Diemar, *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/.

can do with OpenAI's information and a mutual confidentiality obligation.[93] In exchange, Enterprise licensees gain access to ChatGPT's application programing interface (APIs).[94] This allows licensees to integrate ChatGPT into their own products and apps, to customize OpenAI's pre-trained GPT model, and to tailor it to their own needs.[95] 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.[96] 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," powered by ChatGPT, to gain new insights on their health and receive personalized recommendations.[97]

This is all amazing news for users. But generative AI's widespread public distribution to individuals, businesses, and developers presents a challenge for AI companies that hope to rely on trade secret law to protect their information against disclosure and competitive use. Like software, generative AI is an "information good"—it embeds information about its functions and it can be replicated, such that some of the information is either plainly visible or potentially ascertainable to users.[98] Selling information goods, as Amy Kapzcynski and Talha Syed observe, is really just another way of selling *information*.[99] "One way to appropriate returns from producing information," Kapzcynski and Syed write, "is by selling the information itself"; but another

93. *Business Terms*, OPENAI, https://openai.com/policies/business-terms/ (last updated Nov. 14, 2023).

94. An application programming interface (API) allows computer programmers to use prewritten computing tasks for use in their own programs. *See* Google LLC v. Oracle Am., Inc., 593 U.S. 1, 8–10 (2021). Enterprise licensees get other benefits too. They can get early access to new versions of ChatGPT before they're available to the general public, and they get more technical support. *Introducing ChatGPT Enterprise*, OPENAI (Aug. 28, 2023), https://openai.com/blog/introducing-chatgpt-enterprise/.

95. Marty Swant, *With Developer APIs for ChatGPT and Whisper, OpenAI Is Opening the Floodgates with a Familiar Playbook*, DIGIDAY (Mar. 3, 2023), https://digiday.com/media-buying/with-developer-apis-for-chatgpt-and-whisper-openai-is-opening-the-floodgates-with-a-familiar-playbook/; Davenport & Mittal, *supra* note 67; Winograd, *supra* note 4, at 617–18; Claudia Slowik & Filip Kaiser, *How Much Does It Cost to Use GPT Models? GPT-3 Pricing Explained*, NEOTERIC BLOG (Feb. 16, 2023), https://neoteric.eu/blog/how-much-does-it-cost-to-use-gpt-models-gpt-3-pricing-explained/.

96. Steven Lerner, *"They're Not Cheap": Law Firm CIOs on Generative AI Tools*, LAW360 PULSE (Oct. 17, 2023), https://www.law360.com/pulse/articles/1733616; *see also*, *e.g.*, LAWDROID, https://lawdroid.com/.

97. Victoria Song, *Whoop Is Adding a ChatGPT-Powered "Coach"*, VERGE (Sept. 26, 2023), https://www.theverge.com/2023/9/26/23888984/whoop-coach-chatgpt-ai-fitness.

98. *See* Kapczynski & Syed, *supra* note 9, at 1908.

99. *Id.*

way is "by selling an information-embedded good."[100] Doing so profitably "typically requires exclusion of others from the information in question."[101]

How, then, can generative AI companies exclude others from copying, using, or sharing their information, after they release it in publicly distributed generative AI products? Patenting seems like a logical solution. However, as discussed directly below, companies often choose a combination of trade secrecy protection and contracts in lieu of patents for a variety of reasons.[102] This presents a challenge, because trade secrecy requires, well, secrecy. If distributing a product to the public destroys that secrecy, then there is no more protection under trade secret law.[103] The Supreme Court has made clear that selling—or licensing—a product and maintaining trade secret protection is perfectly possible so long as the information does not "lose its secret character."[104] 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."[105]

Companies might initially consider obtaining patents instead of relying purely on secrecy.[106] Trade secret law does not create exclusive rights against the world—independent development and reverse engineering are legal.[107] Patents, in contrast, give the patent owner the right to stop literally anyone from making, using, or selling their invention in the United States for a period of roughly twenty years for utility patents and fifteen years for design patents.[108] But generative AI companies will likely choose to rely heavily on

100. *Id.*

101. *Id.*

102. *See infra* note 112 and accompanying text. Companies also may not wish to rely *solely* on contracts—which only apply to parties in "privity" (those whose who actually entered the contract)—and which come with much weaker remedies; *see also* Hrdy & Seaman, *supra* note 25, at 687–88 (explaining the ways in which trade secrecy is generally stronger than contract law).

103. Hrdy & Lemley, *supra* note 10.

104. Kewanee, 416 U.S. at 484, n.13. As discussed *infra* notes 384–389 and accompanying text, the distinction between selling and licensing a product or service is not dispositive for whether trade secret rights are maintained.

105. *See* Lemley, *supra* note 31, at 313.

106. 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. PAT. & TRADEMARK OFF., PUBLIC VIEWS ON ARTIFICIAL INTELLIGENCE AND INTELLECTUAL PROPERTY POLICY (Oct. 2020); *WIPO Technology Trends 2019: Artificial Intelligence*, WORLD INTELLECTUAL PROPERTY ORGANIZATION (2019).

107. *See* 18 U.S.C. § 1839(6)(B).

108. *See* 35 U.S.C. § 154(a)(1)*; see also* 35 U.S.C. § 173 ("Patents for designs shall be granted for the term of 15 years from the date of grant.").

trade secrecy, rather than relying solely on patents. There are a variety of reasons for this, which I have discussed in detail elsewhere—not least of which is that a lot of generative AI inventions will not be patentable or will only benefit from a very narrow patent scope.[109] In the end, the companies' calculus will likely look a lot like it did for software, where companies have often opted for trade secrecy over patenting to protect hidden information like source code and algorithms.[110] 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.[111] 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 distributed.[112] In Part III, I will challenge this notion, because in fact contracts can be used to maintain legal secrecy even after factual secrecy has dissipated.[113] 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 appearance of the user interface of ChatGPT is a self-disclosing feature, for example, as are 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.[114] 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

109. *See* Hrdy, *supra* note 7.

110. *C.f.* Katyal, *supra* note 14, at 1212–16 (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* note 52, at 1 (discussing AI's amenability to trade secrecy).

111. *See* Lemley, *supra* note 31, at 313.

112. *See, e.g.*, Tabrez Y. Ebrahim, *Artificial Intelligence Inventions & Patent Disclosure*, 125 PENN ST. L. REV. 147, 183–84 (2020).

113. *Accord* Varadarajan, *supra* note 19, at 1567.

114. 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 a company to protect even plainly visible features by imposing confidentiality obligations. *See, e.g.*, *infra* notes 424–428, 442–449 and accompanying text.

market, because they are not plainly visible to users of the product and are difficult (though not impossible) to reverse engineer.[115]

Importantly, not all developers choose secrecy. Some generative AI models are fully released to the public. They are "open-source."[116] An example is Meta's Llama.[117] But many generative AI models, including ChatGPT, are "closed-source." They are only accessible to the general public through a user interface.[118] "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 components."[119] In other words, users do not actually get access to the model at all. They only have access to the software through which the model is deployed.[120]

This closed source structure makes these models particularly amenable to trade secrecy. Several features cannot be accessed by ordinary users at all, including algorithms, code, training datasets, and overall methodology. These features, each of which is discussed below, are kept as trade secrets.

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.[121] 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 survive attempts at reverse engineering.[122] According to one commentator, "[i]n today's algorithmic

115. 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, 1042–48 (2016).

116. Lee et al., *supra* note 4, at 41–42.

117. Meta released code and other details about development, including the "training recipes" which are available on Github. *See Introducing Code Llama, a State-of-the-Art Large Language Model for Coding*, META (Aug. 24, 2023), 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. *License*, META, https://ai.meta.com/llama/license/ (last updated July 18, 2023).

118. Lee et al., *supra* note 4, at 5.

119. *Id.* at 15–17.

120. *Id.* at 41–42.

121. Tschider, *supra* note 4, at 687–89. *See, e.g.*, Vogt, *supra* note 41, at 228 ("Algorithms serve as the foundational structure of almost any AI system.").

122. Tschider, *supra* note 4, at 710–11 (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 8, at 790 (same).

world, trade secrets are the best form of intellectual property protection for algorithms"; algorithms, as "mathematical instructions," are "ineligible for patent and copyright protections."[123] Therefore, "trade secret law is the only option for algorithms, and secrecy is the only way to keep others from using your created algorithms."[124] This is an over-simplification because some complex algorithms may in fact be patentable.[125] But the point is trade secrets are a comparatively effective way to protect algorithms. Even a single algorithm can be an appropriate trade secret subject matter, assuming it meets the elements. Trade secret law protects "information" writ large.[126] Unlike the patent regime, trade secret law does not require the creator of information to be a human being, which may be relevant for algorithms created by generative AI.[127]

Courts have frequently protected algorithms related to AI in the past.[128] But a few challenges may arise. One is trade secret law's "identification" requirement.[129] 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 opposing party.[130] 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 to Microsoft's motion for production.[131] The court concluded that because the plaintiff was alleging that "a particular algorithm"

123. Greer, *supra* note 52, at 263.

124. *Id.*

125. A series of complex algorithms that yield specific technological improvements, a truly novel model architecture, or the software user interface might be patentable. U.S. PAT. & TRADEMARK OFF., *supra* note 106. The patent office has issued many AI patents already. *See, e.g.*, WORLD INTELLECTUAL PROPERTY ORGANIZATION, *supra* note 106.

126. *See* 18 U.S.C. § 1839(3); UTSA, § 1.

127. *See* 18 U.S.C. § 1839(4).

128. *See, e.g.*, Glover v. Imubit, Inc., 2019 Tex. Dist. LEXIS 72440, *2 (Dist. Ct. Jud. Div. 55 2019) (finding employer would likely prevail in proving it owned trade secrets in "processes, procedures, algorithms, and technologies relating to artificial intelligence and machine learning . . . .").

129. *See* The Sedona Conference, *The Sedona Conference Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases*, 22 SEDONA CONF. J. 223 (2021).

130. *See, e.g.*, Torsh, Inc. v. Audio Enhancement, Inc., 2023 U.S. Dist. LEXIS 204359, *16 (E.D. La. 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.").

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

was a trade secret, as opposed to a general concept for an algorithm, "the algorithm itself should be disclosed."[132]

Companies naturally may not wish to disclose their algorithms. Courts can ensure secrecy for these disclosures by placing the parties under protective orders, sealing some or all of the record, or redacting portions of their orders to avoid disclosing trade secrets.[133] 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.[134]

Another potential problem, recently discussed by John Villasenor, is that *the AI itself* may have generated some of the algorithms used in generative AI.[135] "The complexity in 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 . . . ."[136] Villasenor rightly concludes that this issue is not fatal to trade secret protection. Trade secret law has *never* required the owner of the trade secret to itself have full knowledge of the secret.[137] To state a misappropriation claim, a plaintiff "must identify the trade secret in question with sufficient specificity" in order to allow the defendant to know, generally speaking, what information they are accused of misappropriating; yet, the plaintiff need not attest that they *understand* exactly what the trade secret is.[138] Indeed, this is the assumption underlying almost all employee-generated trade secrets—trade secrets are created by human employees, but are likely owned by a corporation, which may or may not know which trade secrets its

132. *RealD Spark*, 2023 U.S. Dist. LEXIS 80221, at *11.

133. *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).

134. *RealD Spark*, 2023 U.S. Dist. LEXIS 80221, at *14.

135. John Villasenor, *Artificial Intelligence, Trade Secrets, and the Challenge of Transparency*, 25 N.C. J.L. & TECH. 495, 499 (2024); *see also* Camilla Hrdy, *Beyond the AI Black 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 (explaining how AI itself may have generated some of the algorithms used in generative AI).

136. Villasenor, *supra* note 135.

137. The trade secret statutes define the "owner" of a trade secret simply as "the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed." 18 U.S.C. § 1839(4).

138. *See* WWMAP, LLC v. Birth Your Way Midwifery, 711 F. Supp. 3d 1313, 1319 (N. D. Fla. 2024).

employees have in their possession.[139] The key, rather, is that trade secret owners effectively describe these algorithms in sufficient detail 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.[140]

That said, a plaintiff who seeks to claim algorithms as its trade secrets would still need to demonstrate that the defendant 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,"[141] accused a former employee, Paladino, of misappropriating trade secrets, including "algorithms and methods for applying machine learning to large volumes of geospatial data."[142] The court denied the plaintiffs' motion for a preliminary injunction, however, because the plaintiffs did not show that Paladino had access to the algorithms and methods at issue.[143] 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.[144]

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.[145] This could be a challenge. For example, what if others outside the company would not understand or be able to benefit from the algorithm?[146] What if an algorithm has become outdated, such that any economic value it had is gone?[147] On the flip side, what if algorithms are not *yet* developed at all?[148]

139. *See* Catherine L. Fisk, *Removing the "Fuel of Interest" from the "Fire of Genius": Law and the Employee-Inventor, 1830–1930*, 65 U. CHI. L. REV. 1127, 1128 (1998).

140. Villasenor, *supra* note 135, at 516.

141. DigitalGlobe, Inc. v. Paladino, 269 F. Supp. 3d 1112, 1116–17 (D. Colo. 2017)

142. *Id.* at 1126.

143. *Id.*

144. *Id.* at 1126–27.

145. Hrdy, *supra* note 77, at 568–76.

146. Sandeen & Aplin, *supra* note 52, at 456.

147. *See* 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.").

148. Hrdy, *supra* note 77, at 602–04 (noting that courts have sometimes found early-stage prototypes that are not yet on the market lack independent economic value).

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, Inc. v. Facebook, Inc.*[149] 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 that 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 that Zlateski had developed while employed at Neural Magic.[150] 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."[151] The court therefore initially denied Neural Magic's request for preliminary injunction, due partly to Neural Magic's failure to prove that its algorithms possessed the requisite independent economic value due to secrecy.[152] That said, the case did eventually proceed, and seemed like it would go to trial.[153] The case settled in the summer of 2023.[154] Despite its inconclusive outcome, the *Neural Magic* case shows that the requirement to prove a trade secret derives economic value from secrecy might be a real hurdle for AI startups that have not yet commercialized their algorithms in any meaningful way. Simply alluding to *potential* revenues in future may not be sufficient.

149. Neural Magic, Inc. v. Facebook, Inc., 2020 WL 13819257, at *4–5 (D. Mass. May 29, 2020).

150. *Id.* at *1–3.

151. *Id.* at *4–5.

152. *Id.* at *7–9.

153. *See* Neural Magic, Inc. v. Meta Platforms, Inc., 659 F. Supp. 3d 138 (D. Mass. 2023).

154. 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/.

2. Source Code

Generative AI, like software, relies in large part on code. ChatGPT uses code in both the underlying large language model and the software system constituting the user interface. Both are closed source, and both are not released to the public.[155] 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.[156] Thus, source code is kept as a trade secret, even if the object code is not.[157]

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.[158] 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 generative AI or related software.[159] But copyright law only protects "substantially similar" iterations of the code, and it also includes a "fair use" defense.[160] Trade secret law has neither of these limitations. As Deepa Varadarajan has repeatedly emphasized, trade secret law has no "fair use" defense.[161] Trade secret law protects the information writ large, regardless of whether the defendant's end product is different from the information that

155. *See supra* note 14.

156. 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 14, at 1193–95, 1207–08; *see also, e.g.*, Fabkom, Inc. v. R.W. Smith & Assocs., Inc., 1996 WL 531873, at *3–4, 7–9 (S.D.N.Y. 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.").

157. 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, 662–64, n.8 (4th Cir. 1993).

158. *See, e.g.*, Katyal, *supra* note 14, at 1207, 1228; Lim, *supra* note 4, at 835; *see also* Computer Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 717–19 (2d Cir. 1992) (17 U.S.C. § 301 did not preempt trade secret claim).

159. *See* 17 U.S.C. § 101 (defining literary work in a way that includes computer code); *see also, e.g.*, Katyal, *supra* note 14, at 1198–1201 (discussing rise of copyright protection for code); *see also Google*, 593 U.S. (fair use for software APIs).

160. *See* 17 U.S.C. § 107.

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

the defendant obtained from the plaintiff.[162] This means that if someone uses a trade secret, such as source code, in order to make a completely new product for a totally different purpose, they might still be liable under trade secret law,[163] if not under copyright law.

An oft-cited case recognizing that trade secrecy is available for source code, along with copyright protection, is *Data General Corp. v. Grumman Systems Support Corp.* Data General sued Grumman Systems Support Corporation ("Grumman"), alleging that Grumman stole source code embedded in Data General's software. A district court, applying Massachusetts common law in 1994, upheld a jury verdict that found 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."[164]

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,[165] but Samuel J. LaRoque argues that object code can now be more readily discovered using a process called "disassembly" or "decompilation."[166] LaRoque argues this process is 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.[167] There is case law, albeit very fact-specific, supporting the view that object code can sometimes easily be decompiled to discern source code.[168]

---

162. *See, e.g.*, Fishman & Varadarajan, *supra* note 36, at 1056–57.

163. *See* Camilla A. Hrdy, *Should Dissimilar Uses of Trade Secrets Be Actionable?*, 167 U PA. L. REV. ONLINE 78, 79–80, 84–85 (2019) (arguing that using a trade secret for a new product, with a new purpose, can still threaten the secrecy of the underlying information, and so the notion that "trade secret law should imitate copyright law's willingness to permit substantially dissimilar uses of content . . . conflicts with trade secret law's fundamental purpose: to protect the integrity of secret information.").

164. Data Gen. Corp. v. Grumman Sys. Support Corp., 825 F. Supp. 340, 359 (D. Mass. 1993), *aff'd*, 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).

165. *See* Lemley, *supra* note 11, at 1244; Katyal, *supra* note 14, at 1216, 1234.

166. 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.").

167. LaRoque, *supra* note 166, at 438–39.

168. *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

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.[169] For example, in the recent case *Apex.AI, Inc. v. Langmead*, the plaintiff Apex.AI, which develops "software tools for use in autonomous 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 Apex.AI's software, source code, and other intellectual property"[170]—after he began marketing the process through his own company, allegedly "plac[ing] Apex.AI's proprietary source code" on his own platform.[171] 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 Apex.AI's source code and other asserted trade secrets pending further litigation.[172]

That said, source code trade secrets can raise procedural complexities. 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.[173] But as the case proceeds through discovery, the plaintiff will probably have to share the source code in great detail.[174] 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

---

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.").

169. *See, e.g.*, NEXT Payment Sols., Inc. v. CLEAResult Consulting, Inc., 2018 WL 3637356, at *13 (N.D. Ill. July 31, 2018) (finding plaintiff sufficiently pled its computer software was a trade secret where the software was confidential and plaintiff "derived economic value from [its software] not being generally known or accessible.").

170. Apex.AI, Inc. v. Langmead, 2023 U.S. Dist. LEXIS 82291, *1–2 (N.D. Cal. May 10, 2023).

171. *Id.* at *2.

172. *Id.* at *1, 3, 5–6 (granting motion for ex parte temporary restraining order in part and order to show cause why preliminary injunction should not issue).

173. *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.").

174. *See* Torsh, 2023 U.S. Dist. LEXIS 204359, at *11–12; *cf.* T2 Modus, LLC v. Williams-Arowolo, 2023 U.S. Dist. LEXIS 170656, *18–20 (E.D. Tex. 2023) (not requiring plaintiff to produce the source code in response to Request for Production).

line number . . .”[175] Again, these disclosures can all be done pursuant to a protective order and other precautionary measures.[176]

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, as well as information regarding which training data was used, or which training data should be used, to train a model.

> [Generative AIs] 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.[177]

Identifying, collecting, and obtaining permissions for training data “is expensive. It requires a substantial investment of multiple resources: time, data storage, and computing power.”[178] 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 formats”); and then compiling that data into “vast and carefully structured collections of related data.”[179] The process may also entail securing licenses, either to individual works or to entire datasets.[180]

Keeping training datasets secret is likely to provide developers of generative AI 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 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* the AI developer.[181] The owner of the training dataset may be a different company.[182] One or both of these entities could keep the training datasets as

175. Torsh, 2023 U.S. Dist. LEXIS 204359, at *15–16.
176. *See* RealD Spark, 2023 U.S. Dist. LEXIS 80221, at * 20.
177. Andrew Torrance & Bill Tomlinson, *Training Is Everything: Artificial Intelligence, Copyright, and “Fair Training*,” 128 DICK. L. REV. 233, 242 (2023).
178. Lee et al., *supra* note 4, at 39–40.
179. *Id.* at 5.
180. *See id.* at 38–39.
181. *See* 18 U.S.C. § 1839(4) (defining “owner” of trade secret).
182. Lee et al., *supra* note 4, at 4–5 (discussing different actors along AI supply chain).

trade secrets, so long as they take the necessary measures to preserve secrecy and the datasets do not become generally known across the industry.[183]

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."[184] It is also possible to ascertain at least some of the works that were used to train a generative AI model.[185]

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.[186] The trade secrecy rules are similar to copyright law's treatment of "compilations."[187] Courts apply divergent standards for protecting combination trade secrets, but the general rule is that the whole combination must impart an economic advantage due to its secrecy.[188] As Charles Tait Graves puts it, a party cannot claim a trade secret in a "part or fragment of information that is not, by itself, a valid trade secret[.]"[189] Instead, if the theory is that the entire "combination" of information if a trade secret, then the party must prove that the "whole," and not just the "part" is a protectable trade secret.[190] This is similar in practice to how copyright law

183. *See* Hrdy, *supra* note 77, at 579 ("Multiple firms can possess the same trade secret and use it competitively in private, so long as it is not 'generally known' to people in the industry.").

184. Sandeen & Aplin, *supra* note 52, at 453.

185. There are emerging resources that can be used to figure out whether a work was used to train an AI. *See* Andrew Wilson-Bushell, *Training Generative AI: Separating Fact from Fiction*, WORLD INTELLECTUAL PROPERTY REVIEW (Sept. 1, 2023), https://www.worldipreview.com/copyright/training-generative-ai-separating-fact-from-fiction; *see also HAVE I BEEN TRAINED?*, https://haveibeentrained.com/; *see also, e.g.*, Sag, *supra* note 63, at 326–27 (discussing use of "model extraction attacks" to ascertain training data).

186. 18 U.S.C. § 1839(3) (specifying that trade secrets can encompass information such as "compilations").

187. Copyright protects "compilations" of facts separately from the underlying facts. *See* 17 U.S.C. § 103(a); *see also infra* note 191; Lee et al., *supra* note 4, at 33–34, 52–53.

188. *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. App'x. 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); *see also* Charles Tait Graves, *The Part for the Whole in Trade Secret Law*, 33 TEX. INTELL. PROP. L.J. 197, 204–09 (2025) (discussing case law applying widely different approaches the "combination" secrets).

189. Graves, *supra* note 188, at 201.

190. *Id.* (critiquing recent cases that "failed to consider the difference between a part or fragment of information that is not, by itself, a valid trade secret, and information that is, whether as a part or as a whole, a protectable trade secret.").

treats compilations of facts: The individual facts are not protectable, but the overall arrangement and selection can be.[191]

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, "[i]f most of that data is collected from publicly visible and available sources, then that information is not secret information and cannot have value because it is secret"[192] But courts are often lenient about protecting combinations of otherwise-public information as trade secrets. For example, one appellate court recently held spreadsheets can be protected as trade secrets, even if they contain information that could be obtained from public sources.[193]

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. 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.[194] However, for combination trade secrets, protection is effectively weaker, because many courts (rightly) hold that acquiring, using, or disclosing only some of the information making up the combination is not actionable.[195] For example, imagine an employee of OpenAI left their job to go work at Google, and they used some, but not all, of the data on which ChatGPT was trained to develop a new generative AI for Google. Under a proper application of the law, the former employee would not be liable for using only part of OpenAI's training dataset, assuming that the combination

191. *See* Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345, 349 (1991); *see also, e.g.*, Thomson Reuters Enter. Ctr. GmbH v. Ross Intel. Inc., 694 F. Supp. 3d 467 (D. Del. 2023).

192. Sandeen & Aplin, *supra* note 52, at 456; *see also* Hrdy, *supra* note 77, at 598.

193. *See* Allstate Ins. Co. v. Fougere, 79 F.4th 172 (1st Cir. 2023).

194. *See infra* note 326.

195. To be clear, there is significant disagreement in the case law on this point. *Compare* Am. Airlines, Inc. v. KLM Royal Dutch Airlines, Inc., 114 F.3d 108, 110–12 (8th Cir. 1997) (defendant not 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 the 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.").

of all the training data is all that is asserted as a trade secret, and the part the employee used does not independently qualify as a trade secret.[196]

Again, it is worth highlighting the procedural complexities. Claiming that an entire training dataset is a combination trade secret may require identifying and disclosing all of the data that makes up the putative trade secret. This entails a disclosure risk. If a plaintiff claimed their entire dataset was a combination trade secret, then they might have to reveal the entire training dataset to the court and the other side. For example, in RealD Spark LLC, mentioned above, the plaintiff, RealD, alleged that the "[d]atasets to support SocialEyes' image recognition methods" were trade secrets.[197] During discovery, RealD provided a "nearly 3,000-page range" of documents to identify its training datasets.[198] 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 the court concluded that this identification was not sufficiently specific.[199] 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.[200] Again, even with a protective order in place, such specification 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.[201] How a specific generative AI was developed and trained—what Katherine Lee, A. Feder Cooper, and James Grimmelmann call the overall "technical architecture"[202]—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.

196. If the part the employee used is a trade secret in its own right, this could supply an independent basis for trade secret liability, and there would be no need to rely on a combination trade secret theory. *See generally* Tait Graves & Alexander Macgillivray, *Combination Trade Secrets and the Logic of Intellectual Property*, 20 SANTA CLARA COMPUT. & 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.").

197. RealD Spark, 2023 U.S. Dist. LEXIS 80221, at *2.

198. *Id.* at *14.

199. *Id.* at *16.

200. *Id.*

201. Sandeen & Aplin, *supra* note 52, at 453; *see also* QUINN, *supra* note 52 at 6–7.

202. Lee et al., *supra* note 4, at 4.

A model's technical architecture can have several components, depending on which form of model it is and how it was developed.[203] 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.[204] 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)."[205] 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, the knowledge that a neural network was utilized could help others build a similar or improved model. Knowing which weight parameters were used to build that network would be more valuable still.

A key challenge in these cases will be distinguishing specific details about model architecture—which may be a trade secret—from technology 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."[206] At least some of the fundamental technology is well-known in the field and unlikely to qualify as a trade secret.[207]

Several AI-related trade secret cases have been dismissed because plaintiffs provided generic descriptions of AI technology, which courts found could not possibly be "secrets" in the field. For example, in *Lamont v. Krane*, 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

203. *Id.* at 12 ("Different model architectures vary widely in size and complexity, and in turn have different capabilities for encoding relationships in the data.").

204. Tschider, *supra* note 4, at 689–90; Lee et al., *supra* note 4, at 10–11.

205. Lee et al., *supra* note 4, at 12 ("[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).").

206. Lee et al., *supra* note 4, at 24.

207. 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. *See* 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), https://www.forbes.com/sites/alexzhavoronkov/2023/01/23/can-google-challenge-openai-with-self-attention-patents/; Lee et al., *supra* note 4, at 30 (mentioning "publication of the transformer architecture in 2017").

Montreal."[208] 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 Google Ventures relied upon anything in particular that it obtained from the plaintiff, or that was not a matter of general knowledge.[209]

Companies can also own "modification" trade secrets relating to model architecture.[210] After initial development and training, generative AI models are often refined and improved. As Lee, Cooper, and Grimmelmann explain, a "pre-trained" "base model" can "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."[211] For example, third-party developers with access to a pre-trained ChatGPT model can "fine-tune" it based "on their own data, creating a custom version tailored to their application."[212] When generative AI is adopted within a business, it will likely have to be continually updated to achieve optimal performance.[213]

Any of these modifications and improvements can also be protected as trade secrets, because they likely 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 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" means extracting information from a product (or service) that is available on the open market by observing it, picking it apart, doing tests on it, or taking specific actions to learn about the product, such as decompiling the

208. Lamont v. Krane, 2019 U.S. Dist. LEXIS 81451, *3 (N.D. Cal. 2019).

209. *Id.* at *8–9; *see also* Loop AI Labs Inc. v. Gatti, 195 F. Supp. 3d 1107, 1114–15 (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).

210. *See* Metallurgical Indus. Inc. v. Fourtek, Inc., 790 F.2d 1195, 1199 (5th Cir. 1986).

211. Lee et al., *supra* note 4, at 5; *see also id.* at 42–43.

212. Rachel Lim, Michael Wu & Luke Miller, *Customizing GPT-3 for Your Application*, OPENAI (Dec. 14, 2021), https://openai.com/index/customizing-gpt-3/.

213. *See* Iavor Bojinov, *Keep Your AI Projects on Track*, HARV. BUS. REV. 53–59 (Nov.–Dec. 2023).

source code underlying software or extracting data from a generative AI model to learn how it was developed.[214]

From the perspective of trade secrecy, "reverse engineering" can be *complete*—meaning all the asserted trade secrets can easily be discerned from the product—or it can be *partial*, meaning only some of the asserted trade secrets are readily 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.[215] Likewise, for software, some information, like object code, is more easily accessible, whereas other information, like source code, can take longer and be more expensive to reverse engineer.[216]

Reverse engineering is one of the most important ways that trade secrets embedded in publicly distributed products can *end*. Trade secrets that can easily be reverse engineered from publicly available products are terminated because they no longer meet the criteria for legal protection under trade secret law.[217] Importantly, not all acts of reverse engineering threaten trade secrecy. As James Pooley has observed, companies engage in reverse engineering for all sorts of reasons, ranging from repairing a product, to achieving interoperability, to deliberately "creating a clone" for purposes of competition.[218]

---

214. Samuelson & Scotchmer, *supra* note 9, at 1577, 1607–08.

215. "Tolerances" refers to the precise measurements and other specific details needed to manufacture a product. Courts often protect tolerance data as trade secrets to the extent it cannot easily be measured and copied from the product itself. *See, e.g.*, A. H. Emery Co. v. Marcan Prod. Corp., 389 F.2d 11, 15–16 (2d. Cir. 1968).

216. *See generally* MILGRIM & BENSEN, *supra* note 14, at § 1.05 (stating that "the most valuable trade secret in modern commerce, software source code, is not lost upon marketing of software object code if the recipient is duly prohibited from disassembling and decompiling the object code to derive the underlying source code.").

217. *See* 18 U.S.C. § 1839(3) (2016); *see also* Hrdy & Lemley, *supra* note 10, at 42 ("Abandonment of a trade secret can happen when the information is no longer secret or when its former owner has ceased to take steps to preserve its secrecy."); Deepa Varadarajan, *Forfeiting IP*, 59 AM. BUS. L.J. 175, 176 (2022) ("Intellectual property (IP) owners who act (or fail to act) in certain ways can forfeit their rights. For example . . . if a trade secret owner stops guarding the confidentiality of a trade secret, the IP right ends."); *see also* Camilla A. Hrdy, *Fagundes & Perzanowski: A New Framework for Conceptualizing the End of IP Rights*, WRITTEN DESCRIPTION (Feb. 9, 2025), https://writtendescription.blogspot.com/2025/02/perzanowski-fagundes-new-framework-for.html (discussing Dave Fagundes and Aaron Perzanowski's argument that failing to maintain secrecy constitutes "ex post" "invalidation" of trade secrets and Deepa Varadarajan's argument that failing to keep information secret constitutes "forfeiture.").

218. *See* Samuelson & Scotchmer, *supra* note 9, at 1582, n.23 (citing JAMES POOLEY, TRADE SECRET LAW § 5.02 (1997)).

When reverse engineering is undertaken for the purpose of competition, this obviously poses a major business risk to the original developer. They may lose their first-mover advantage and preeminent status in the market. But this risk is believed to be beneficial for public 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 industrial context."[219] They give four reasons this type of reverse engineering is good for public policy.

First, assuming the result is more competition, then consumers benefit from more options and lower prices.[220] Second, reverse engineering can advance technological development by way of "cumulative innovation," since improvements can proceed outside the control of the original developer.[221] Third, reverse engineering maintains "balance" in intellectual property law by forcing developers of new inventions who cannot maintain trade secrets to obtain patents.[222] Finally, reverse engineering respects peoples' rights to do what they want with products they lawfully acquire.[223]

For all these reasons, Sameulson and Scotchmer argue, legal reverse engineering has historically been the default rule.[224] The major exception is where the invention is the subject of a valid patent; otherwise, reverse engineering is usually legal.[225] This default rule is integral to trade secret law. Obtaining trade secrets through reverse engineering is simply not trade secret misappropriation.[226] 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

219. Samuelson & Scotchmer, *supra* note 9, at 1582.

220. *Id.* at 1583.

221. *Id.*

222. *Id.* at 1583–84.

223. *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.").

224. *Id.* at 1582 ("Reverse engineering is generally a lawful way to acquire know-how about manufactured products.").

225. *See, e.g.*, Kewanee, 416 U.S. at 476–90 (1974) (finding that 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).

226. 18 U.S.C. § 1839 (5)–(6) (2016); *see also* UTSA, § 1, cmt.

owner is deemed to have failed to take "reasonable" secrecy precautions to protect information that is highly vulnerable to reverse engineering.[227]

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 decompilation.[228] In his recent article, Jake Sherkow similarly asserts 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."[229]

In the earlier stages of a technology's lifecycle, however, reverse engineering tends to be harder, simply because the technology is new, and even experts do not possess the know-how required to replicate it. Generative AI is still relatively new, and at present, it is unclear how vulnerable generative AI models are to reverse engineering. Scholars have opined that, in general, AI is highly conducive to trade secrecy because AI is "exceptionally difficult to reverse engineer . . . ."[230]

However, this will not be the case forever. Reverse engineering generative AI models is at present difficult, costly, and time-consuming. But it will become easier, cheaper, and quicker over time. Complete reverse engineering may be possible in the near future.[231] There are already various methods that can be used to at least *partially* reverse engineer a generative AI model. One example is the "model extraction attack."[232] In general terms, a model extraction attack relies on strategic prompting of an AI model in order to

227. 18 U.S.C. § 1839(3) (2016). *See infra* Part IV.

228. LaRoque, *supra* note 166, at 439–40 (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).

229. *See* Jacob S. Sherkow, *The Myth of DNA Trade Secrecy*, 75 U.C. L.J. 1047, 1088 (2024).

230. In fact, OpenAI itself is doing significant research on how to make "its models more explainable," and recently released a new research paper on a new technique for shedding light on some of the workings of AI models. John Hillman, *Smart Regulation: Lessons from the Artificial Intelligence Act*, 37 EMORY INT'L L. REV. 775, 789–90 (2023) ("The 'black box' nature of many AI systems makes reverse engineering nearly impossible."); *see also*, Tschider, *supra* note 4, at 687–88, 709–12 (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).

231. *See* Will Knight, *OpenAI Offers a Peek Inside the Guts of ChatGPT*, WIRED (June 6, 2024), https://www.wired.com/story/openai-offers-a-peek-inside-the-guts-of-chatgpt/.

232. I am very grateful to Akron Law student Devin P. Owns for teaching me about model extraction attacks. *See* Devin P. Owens, *Artificial Intelligence Models May Not Have Owners* (unpublished student paper) (on file with author) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5055010).

extract data from the model and use it to replicate the original model's behavior and functionality.[233] 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.[234]

Intellectual property law scholars have previously noted the possibility of strategically extracting data from AI models, but—back then—the technology was highly speculative.[235] This is no longer the case. Strategic data extraction is already happening.[236] For example, in the ongoing lawsuit between the New York Times and OpenAI, OpenAI has alleged that the New York Times used strategic prompting in order to determine which training data OpenAI used to train ChatGPT, and that the Times did so in violation of OpenAI's Terms of Use.[237] OpenAI has also accused the developers of a new competing AI model,

233. A model extraction attack typically entails using advanced AI techniques to input a massive number of queries into the target AI model, analyzing the target AI model's responses in order to learn precisely how the model was developed and trained, and using the model's responses to train a new model that mimics the original's behavior and functionality. Milad Nasr, Nicholas Carlini, Jonathan Hayase, Matthew Jagielski, A. Feder Cooper, Daphne Ippolito, 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.").

234. Florian Tramèr, Fan Zhang, Ari Juels, Michael K. Reiter & Thomas Ristenpart, *Stealing Machine Learning Models via Prediction APIs*, 25TH USENIX SECURITY SYMPOSIUM 601 (Aug. 10, 2016), https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_tramer.pdf; *see also* Winograd, *supra* note 4, at 625–26 (discussing a "training data extraction attack" whereby an "adversary" "deliberately causes a model to leak memorized information" to extract users' private information).

235. Several articles have discussed the fact that model extraction attacks could theoretically be used to reverse engineer trade secrets. *See* Arti K. Rai, Isha Sharma & Christina Silcox, *Accountability, Secrecy, and Innovation in AI-Enabled Clinical Decision Software*, 7 J.L. & BIOSCIENCES 1 (2020) (citing Tramèr et al., *supra* note 234); *see also* Fromer, *supra* note 14, at 720–24, n.109 (citing Tramèr et al., *supra* note 234).

236. For example, Matthew Sag notes that data extraction methods can be used to discern which training data was used to train an AI. Sag, *supra* note 63, at, 326–27.

237. The New York Times' investigation apparently revealed that ChatGPT was trained on copyrighted New York Times content. Indeed, the Times alleges that ChatGPT 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 also alleged that these actions were taken in violation of OpenAI's Terms of Use. *See* The New York Times Co. v. Microsoft Corp., No. 1:23-cv-11195 (SHS) (OTW), Memorandum of Law in Support of OpenAI Defendants' Motion to Dismiss, at 2 (S.D.N.Y.

called "DeepSeek," of engaging in illicit "knowledge distillation" in order to develop a "copycat" system.[238] "Knowledge distillation," like model extraction attacks, entails extracting massive amounts of data from an AI model's outputs in order to create a new model that approximates the original model's decision-making patterns.[239] OpenAI alleges that DeepSeek was built using knowledge distillation, and that this was done in violation of OpenAI's Terms of Use. DeepSeek has denied these allegations, asserting that their model was developed independently.[240]

In a very recent trade secret lawsuit—which was filed just prior to publication of this article—another generative AI company, called OpenEvidence Inc., alleged that a Canadian company, Pathway Medical Inc., used a so-called "prompt injection attack" to extract "trade secrets" from OpenEvidence's generative AI model with the goal of developing a competing system.[241] OpenEvidence (which is not affiliated with OpenAI[242]) distributes a

2024), https://fingfx.thomsonreuters.com/gfx/legaldocs/byvrkxbmgpe/OPENAI%20MICROSOFT%20NEW%20YORK%20TIMES%20mtd.pdf.

238. Mary Bennett & Rob Robinson, *OpenAI Accuses DeepSeek of Unlawful Use of AI Models, Raising Ethical and Legal Concerns*, HAYSTACKID (Feb. 3, 2025), https://www.jdsupra.com/legalnews/openai-accuses-deepseek-of-unlawful-use-2896277/; *see also* Kevin Collier & Jasmine Cui, *OpenAI Says DeepSeek May Have 'Inappropriately' Used Its Data*, NBCNEWS (Jan. 29, 2025), https://www.nbcnews.com/tech/tech-news/openai-says-deepseek-may-inapproriately-used-data-rcna189872.

239. In comparison to model extraction attacks—which seek to learn as much as possible about the original model—knowledge distillation is typically motivated by efficiency and cost reduction, rather than exact replication. That said, the difference between knowledge distillation and model extraction attacks is nuanced, and some sources depict knowledge distillation as a form of "model extraction" or "model stealing." *See* Daryna Oliynyk, Rudolf Mayer & Andreas Rauber, *I Know What You Trained Last Summer: A Survey on Stealing Machine Learning Models and Defences*, ARXIV (June 16, 2022), https://arxiv.org/abs/2206.08451; *see also, e.g.*, Amir Moslemi, Anna Briskina, Zubeka Dang & Jason Li, *A Survey on Knowledge Distillation: Recent Advancements*, 22 MACH. LEARN. WITH APPL. 100605 (2024), https://doi.org/10.1016/j.mlwa.2024.100605 (discussing utility of knowledge distillation for developing "deep learning models on resource-limited devices without compromising performance.").

240. *See, e.g.*, *OpenAI Accuses Chinese Startup DeepSeek of Unauthorized Data Use, Sparking AI Ethics Debate*, OUTPOST (Jan. 31, 2025), https://www.theoutpost.com; Houman Asefi, *The OpenAI vs DeepSeek Knowledge Distillation Dispute: Technical and Legal Implications*, MEDIUM (Jan. 30, 2025), https://houman-asefi.medium.com/the-openai-vs-deepseek-knowledge-distillation-dispute-technical-and-legal-implications-1e69d646b928; John Werner, *Did DeepSeek Copy Off of OpenAI? And What Is Distillation?*, FORBES (Jan. 30, 2025), https://www.forbes.com/sites/johnwerner/2025/01/30/did-deepseek-copy-off-of-openai-and-what-is-distillation/.

241. OpenEvidence Inc. v. Pathway Med., Inc., No. 1:25-cv-10471 (D. Mass. filed Feb. 26, 2025), at 1–2.

242. OPENEVIDENCE, https://www.openevidence.com/.

popular generative AI tool for use by medical professionals and patients.[243] Licensed medical professionals (unlike general users) can obtain *unlimited* access by providing a National Provider Identifier (NPI) and attesting to be a licensed medical professional.[244] In its lawsuit, OpenEvidence alleged that the Canadian company, Pathway Medical, Inc., somehow got access to a medical practitioner's NPI and used it to "impersonate" a licensed practitioner in order to obtain illicit access to the model.[245] Pathway then allegedly used strategic prompting (which OpenEvidence referred to as a "prompt injection attack") in order to "mislead" the AI model into revealing valuable trade secrets bearing on how the model was developed and "fine-tuned."[246]

These discovery methods are advancing rapidly. Even if it is not currently possible to *fully* "reverse engineer" a generative AI model like ChatGPT or OpenEvidence, it is possible to learn significant amounts of information about how the model was developed, trained, and implemented. These techniques will only improve over time.

The prospect of easy and cheap reverse engineering has three major implications for trade secret law. First, the person doing the reverse engineering should not themself be liable for trade secret misappropriation, assuming that this is really reverse engineering and not "improper means."[247] 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."[248] Third, if a company continues

243. Similar to ChatGPT, OpenEvidence is a "large language model" that appears to users as a "chatbot," which can be used by doctors and patients to ask questions about medical issues, including "diagnoses, treatments, medications," and "potential side effects" to medications. *Id.* at 14–15. Like ChatGPT, OpenEvidence is open to the general public for free; but general public users only get to ask two questions per week. *Id.* at 16.

244. An NPI is "a unique 10-digit identification number assigned to healthcare providers. *Id.* at 16. The Terms of Use provides that "[t]he Services are intended for physicians and other healthcare professionals. By using the Services, you represent and warrant that you have the right, authority, and capacity to agree to and abide by these Terms and that you are not prohibited from using the Services or any portion thereof." *Id.* at 16–17.

245. *Id.* at 2, 18.

246. OpenEvidence alleged that the main trade secret Pathway stole was OpenEvidence's "system prompt code." *Id.* at 20. The system prompt code refers to the instructions given to a generative AI model in order to "fine-tune" the model and guide and improve its responses to users. OpenEvidence alleged this is a tightly kept trade secret and indeed OpenEvidence's "crown jewel," the key to its economic value to users. *Id.* at 7, 10–11.

247. The person who extracts trade secrets through "reverse engineering" should not be deemed to be using "improper means" because reverse engineering is not improper means, by statute. 18 U.S.C. § 1839(6). However, some courts might perceive *any* use of new automation or AI techniques to be "improper." This possibility is discussed and critiqued in Section IV.A.

248. *See* 18 U.S.C. § 1839(3); *see also supra* note 217.

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.[249] There is significant legal and factual uncertainty surrounding all these issues.[250] But the consequence of quick, cheap, and easy reverse engineering should, as a general matter, be that trade secrecy is destroyed.

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.

III. 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 of confidentiality and placed restrictions on what users could do.[251] Some generative AI companies, including OpenAI, have pulled out the same playbook that worked for software. First, as just shown, they are keeping generative AI systems factually secret[252] by deploying them in a "closed source" format that hides back-end features from users.[253] Second, they are using contract law to obtain broader rights than trade secrecy alone would afford. In this part, I explain how Open AI uses contracts to restrict what users of ChatGPT can do with the technology.[254]

A. INDIVIDUAL TERMS OF USE VS. ENTERPRISE LICENSE BUSINESS TERMS

First, it is necessary to draw an important distinction. Two different "terms of use" apply to ChatGPT, depending on the agreement the user enters. Individual end users of ChatGPT generally "click to agree," or otherwise

249. *See id.*

250. *See* discussion *infra* Part IV.

251. *See supra* notes 11 and 15.

252. Factual secrecy means not visible to users or easy to discern through reverse engineering. *See supra* note 12.

253. *See* Lee et al., *supra* note 4, at 5, 41–42 (explaining "closed source" deployment of many generative AI models).

254. End user license agreements are usually used to govern use of software. Terms of use often govern use of websites. *See supra* note 15.

indicate their assent,[255] to "Terms of Use" when they sign up to use ChatGPT.[256] The Terms of Use are, in effect if not in name, "contracts of adhesion."[257] Contracts of adhesion are "boilerplate" contracts that are unilaterally drafted by one party that uses them in many transactions.[258] They are not negotiated; instead, the end user has no choice but to "adhere" to the terms or walk away.[259] The other party has far less knowledge, is not represented by a lawyer, and has essentially no bargaining power in the transaction.[260]

There are different terms of use—called the "Business Terms"—which apply to businesses or developers that sign up for a ChatGPT "Enterprise License," which was discussed in Part II.[261] The Enterprise License is typically the result of a negotiation between OpenAI and the business or developer seeking an Enterprise License.[262] The Enterprise License is specifically negotiated between OpenAI and another (comparatively) sophisticated entity

255. Under contract law principles, users must assent to terms of use, or they are not enforceable. A "click to agree" format is usually sufficient, though not always necessary, for proving mutual assent. *See* ERIC GOLDMAN, INTERNET LAW: CASES & MATERIALS 56–57 (2022 ed.) (providing a taxonomy of online contracts and suggesting that an online contract that satisfies the requirement of mutual assent should be referred to more generally as a "clickthrough" rather than a "clickwrap" or a "click to agree."). Courts have generally held that viewing a conspicuous hyperlink to a terms of use, and thereafter objectively manifesting assent, such as by clicking "I agree," is sufficient to satisfy mutual assent—so long as the "offeree is asked to affirmatively assent to conspicuous, hyperlinked contract terms," "has an opportunity to review the hyperlinked terms," and "affirmatively indicate[s] acceptance of them." Mohammed v. Uber Techs., Inc., 237 F. Supp. 3d 719, 731 (N.D. Ill. 2017) (citing Mohamed v. Uber Techs., Inc., 109 F.Supp.3d 1185, 1196–97 (N.D. Cal. 2015)); *see also* Meyer v. Uber Techs., Inc., 868 F.3d 66, 75 (2d Cir. 2017) ("'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.'") (quoting Sgouros v. TransUnion Corp., 817 F.3d 1029, 1033–34 (7th Cir. 2016)).

256. *See Terms of Use, supra* note 22.

257. *See* Orly Lobel, *Boilerplate Collusion: Clause Aggregation, Antitrust Law & Contract Governance*, 106 MINN. L. REV. 877, 889 (2021).

258. *Id.*

259. *Id.*

260. *Id.*

261. *See Business Terms*, *supra* note 93.

262. *See ChatGPT Enterprise*, *supra* note 92; *Introducing ChatGPT Enterprise*, *supra* note 94; Jay, OPENAI DEVELOPER FORUM (Sept. 19, 2023), 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. *See* Jay, OPENAI DEVELOPER FORUM (Dec. 5, 2023), https://community.openai.com/t/is-chatgpt-enterprise-expensive-is-there-a-minimum-budget-who-qualifies/545691.

that seeks tailored and more extensive access to both ChatGPT and to OpenAI.

The difference between these two terms of use matters for trade secret law. Courts will likely scrutinize the Terms of Use as a "mass-market" end user contract entered between "outsiders" that does *not* generate a duty of confidentiality between the parties. In contrast, courts will likely treat the Business Terms as a negotiated contract between "insiders," in which both parties have express and implied duties of confidentiality to one another.[263]

As a result, breaching the Business Terms is much more likely to give rise to trade secret liability based on a traditional theory of misappropriation, involving acquisition, use, or disclosure of trade secrets in breach of a duty to maintain their secrecy.[264] The Terms of Use for individual users, in contrast, create a much weaker foundation for a traditional trade secret law claim. This claim would instead have to rest on a theory that the user acquired trade secrets by "improper means." This theory would likely rest in part, if not entirely, on the theory that the user accessed trade secrets in breach of a specific provision in the Terms of Use, such as an anti-reverse-engineering or noncompete clause. This argument is discussed in detail in Part IV.A. In addition, due to the negotiated nature of the transaction, the Business Terms would be more likely to survive challenges based on doctrines like unconscionability.[265]

B. THE CONTRACTUAL PROVISIONS PROTECTING CHATGPT'S SECRETS

The ChatGPT terms of use contain 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.[266] As I'll discuss in more depth in Part IV, case

263. Indeed, as discussed below, the Business Terms contains a mutual confidentiality clause, whereas the Terms of Use agreement for individual users has no confidentiality clause at all. *See infra* notes 328–334 and accompanying text; *see also* Lemley, *supra* note 11, at 1239 (noting that courts tend to distinguish between "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).

264. 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 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) (defining misappropriation).

265. *See infra* note 273.

266. *See Terms of Use, supra* note 22.

law from software suggests that a 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 state 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 . . . ."[267]

Anti-reverse engineering clauses are standard in software agreements.[268] Courts and commentators diverge on whether anti-reverse engineering clauses can serve as the basis for a trade secret claim.[269] But purely as a matter of contract law, anti-reverse engineering agreements are typically enforced.[270] They can be scrutinized under the relevant jurisdiction's contract rules and can be found unenforceable under doctrines like "unconscionability."[271] 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.[272] When a term is substantively more restrictive—which an anti-reverse-engineering agreement arguably is—courts tend to require more notice

267. *See id.*; *see also Business Terms*, *supra* note 93. 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* Sean Hogle, *An Anti-Reverse Engineering Clause That Actually Works*, EPICLAW (Apr. 20, 2020), https://epic.law/an-anti-reverse-engineering-clause-that-actually-works/.

268. Madison, *supra* note 14, at 281.

269. *See, e.g.*, Lemley, *supra* note 11, at 1248–59; MENELL ET AL., *supra* note 69, at 102.

270. *See, e.g.*, Daniel Laster, *The Secret Is Out: Patent Law Preempts Mass Market License Terms Barring Reverse Engineering for Interoperability Purposes*, 58 BAYLOR L. REV. 621, 624 (2006) ("Courts increasingly are enforcing [anti-reverse engineering clauses] as a matter of contract law, notwithstanding arguments of copyright preemption."); *see also, e.g.*, Triage Logic Mgmt. & Consulting, LLC v. Innovative Triage Servs., LLC, 2020 WL 4597279, at *7–8 (N.C. Super. Aug. 11, 2020) (enforcing no-reverse engineering clause under contract law).

271. 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)." *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).

272. Murti v. Thor Motor Coach, 2023 Cal. Super. LEXIS 13443, *6 (Cal. Sup. Ct. 2023).

and signs of true bargained-for assent by users.[273] This means courts might likely look less favorably on the anti-reverse engineering clause that applies to individual ChatGPT users, as opposed to the Business Terms.

There are also potential "preemption" challenges to enforcing anti-reverse-engineering clauses through state contract law. These include preemption by patent law,[274] preemption by copyright law,[275] and trade secret law.[276] These arguments have not been very successful in the past. Courts tend to view contracts as private bargains that are not disturbed by the existence of intellectual property rights, absent some clear legislative intent.[277] 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,[278] even though reverse engineering software is in some instances "fair use" under the Copyright Act.[279]

---

273. *Id.* at *16. ("[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.").

274. *See* Laster, *supra* note 270, at 624 (arguing that anti-reverse-engineering clauses should be preempted by patent law when they take the form of a "non-negotiated mass market" license and when the reverse engineering is needed to achieve interoperability).

275. *See* Guy A. Rub, *Moving from Express Preemption to Conflict Preemption in Scrutinizing Contracts over Copyrighted Goods*, 56 AKRON L. REV. 56, 303 (2023) (discussing general trend of non-preemption though noting recent case law holding that certain contracts were expressly preempted by the Copyright Act).

276. 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."). The new federal preemption argument is discussed in Section IV.D.

277. *See* Hrdy & Seaman, *supra* note 25, at 703–06 (discussing the "pro-contract" approach in IP preemption case law).

278. *See, e.g.*, Bowers v. Baystate Techs., Inc., 320 F.3d 1317 (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 803–05, 806–09 (discussing trend of courts enforcing anti-reverse-engineering clauses).

279. 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, 843–44 (Fed. Cir. 1992). The court in Atari stated:

Given this history, courts will likely enforce the ChatGPT anti-reverse engineering clauses as a matter of contract law.[280] There is case law to support this prediction.[281] 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 in part."[282] The court found this anti-reverse engineering clause was enforceable.[283] It was neither an illegal restraint on trade akin to a noncompete agreement[284] nor preempted by copyright law.[285]

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 will be discussed in detail in Part IV, some courts have held that a 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, some state trade secret statutes explicitly allow for this interpretation.[286] 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.[287] Part IV

> 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.

280. Chen, *supra* note 24, at 805.

281. *See, e.g.*, Red.com, Inc. v. Jinni Tech Ltd., 2017 WL 4877414, 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).

282. Triage Logic, 2020 WL 4597279, at *7–8.

283. *Id.*

284. *Id.* at *41–42.

285. *Id.* (citing, e.g., SAS Ins., Inc. v. World Programming, Ltd., 874 F.3d 370, 380 (4th Cir. 2017)).

286. *See infra* Part IV.

287. *See infra* Part IV.

will 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.[288]

2. No Competition

Second, the Terms of Use contain what will likely be construed as a noncompete agreement, also called a "noncompete." The provision is not labeled as a noncompete, but it prohibits users from using ChatGPT outputs "to develop models that compete with OpenAI."[289] OpenAI is not the only AI developer deploying these clauses. Meta—which releases its Llama model in an *open-source* format—has a similar provision in its EULA.[290]

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 users from competing with OpenAI under any circumstances.[291] They simply prevent users 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 fight me, but you can still fight me with a different sword."[292]

Still, this is a restriction on competition, and likely 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.[293] California famously bans noncompetes when entered with workers.[294] On the other hand,

288. *See infra* Part IV.

289. *See Terms of Use, supra* note 22. Notably, the language in the Business Terms is more permissive. 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[.]" Enterprise licensees are also allowed to "fine tune" pre-trained GPT models on their own data. *See Business Terms*, *supra* note 93.

290. 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)." *License*, *supra* note 117; *see also supra* note 117.

291. *Cf.* Hrdy & Seaman, *supra* note 25, at 673–75 (defining noncompetes, contracts that prevent the recipient of information from competing following the exchange, and comparing a noncompete to a confidentiality agreement, which merely prevents use or disclosure of certain information).

292. There is no footnote for this. It's completely made up.

293. *See Terms of Use, supra* note 22.

294. 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. *See* CAL. BUS. & PROF. CODE § 16600 (2023); *see also* Edwards v. Arthur Andersen LLP, 44 Cal. 4th 937, 946–47 (2008).

California's ban is not typically applicable outside the employment context.[295] Instead, California courts tend to assess business-to-business noncompetes for "reasonableness," rather than treating them as per se unenforceable.[296]

That said, a court would presumably still review the OpenAI noncompete for "reasonableness" in adjudging its enforceability.[297] Under the laws of most jurisdictions, a noncompete must be "reasonable" in terms of time, geography, and scope, and be reasonably related to protecting "legitimate interests."[298]

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 are forbidden from using to compete. The Output does not have to be a trade secret or confidential information. It can be anything generated by ChatGPT.[299] 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 do not receive specific notice, let alone separate consideration, that might justify enforcing a promise to never use ChatGPT's outputs to compete with OpenAI.[300]

Most importantly, the OpenAI noncompete has no time limit. The prohibition on competition lasts forever. Some case law—and not even from

295. This could change. The California ban was just amended to be even stronger. For example, 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).

296. *See, e.g.*, Quidel Corp. v. Superior Court, 57 Cal. App. 5th 155, 166–68 (2020). Notably, the Federal Trade Commission's 2024 ban on noncompetes only applies to agreements between employers and workers. *See* 16 C.F.R. § 910 (2024).

297. *See, e.g.*, Quidel Corp. v. Superior Court, 57 Cal. App. 5th 155, 166–67 (2020) ("Noncompetition clauses have been deemed valid outside the employment arena[,]" but courts apply "a test of reasonability, contemplating whether the arrangement promoted competition."); Ixchel Pharma, LLC v. Biogen, Inc., 9 Cal. 5th 1130, 1156, 470 P.3d 571, 585–86 (2020) (interpreting Section 16600 to apply "more strictly" for "agreements not to compete after the termination of employment" and applying a "reasonableness standard" to noncompetes entered among businesses).

298. *See* RESTATEMENT (SECOND) OF CONTRACTS § 188 (AM. L. INST. 1981).

299. 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. *See Terms of Use, supra* note 22.

300. 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).

California—suggests that perpetual noncompete clauses in software agreements cannot survive a "reasonableness" standard. They are unenforceable. For example, in *Triage Logic*, a North Carolina court recently found a noncompete clause in a software license agreement to be an illegal restraint on trade and thus unenforceable under North Carolina law.[301] The clause provided that "the Licensee shall not . . . develop similar software, services or product offerings substantially similar to the System."[302] 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.[303]

Courts will be particularly skeptical of the noncompete in OpenAI's Terms of Use, which applies to individual users, rather than businesses that negotiate an enterprise license.[304] This Terms of Use is a contract of adhesion. Individual users of ChatGPT do not negotiate a contract with OpenAI; this is non-negotiated boilerplate language offered on a "take-it-or-leave-it" basis.[305] The user—who is typically less powerful and less sophisticated, and not represented by an attorney—has no choice but to adhere to its terms.[306] Courts reviewing this noncompete would ask not only whether the user had reasonable notice and an opportunity to read the contract,[307] but also whether this noncompete belies users' "reasonable expectations."[308] A California court would likely treat this clause even less favorably, because, as noted above, in

301. Triage Logic, 2020 WL 4597279, at *4.

302. *Id.*

303. 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." *Id.* at *9.

304. *See Terms of Use, supra* note 22; *see also Business Terms*, *supra* note 93.

305. *See* Danielle D'Onfro, *Contract-Wrapped Property*, 137 HARV. L. REV. 1058, 1085 (2024) ("Adhesion contracts are terms that a consumer must accept to proceed with a service or use a product. They differ from other contracts in that the consumer has no option to negotiate the terms of the agreement. The consumer can only accept or reject the contract or choose from 'a menu of choices from a single firm.').

306. *See id.*

307. *See* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 30–35 (2d Cir. 2002) (holding users not given sufficient notice of terms in online user agreement, and stating that generally there must be "[r]easonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers . . . .").

308. Courts sometimes hold that certain terms in standardized contracts are not enforceable because they contradict the user's "reasonable expectations," especially where the other party has reason to know this is the case. *See* C & J Fertilizer, Inc. v. Allied Mut. Ins. Co., 227 N.W. 2d 169 (Iowa 1975); *see also* RESTATEMENT (SECOND) OF CONTRACTS § 211(3) (AM. L. INST. 1981) ("Where the other party has reason to believe that the party manifesting such assent would not do so if he knew that the writing contained a particular term, the term is not part of the agreement.").

California, noncompete clauses are generally unenforceable, at least when entered between employers and workers.[309]

That said, it is possible courts might enforce the noncompete clause in the Business Terms, as opposed to the one that applies to individual users.[310] In general, the analysis applied to noncompetes in business-to-business arrangements is more lenient than in employee or end user cases.[311] Courts might scrutinize the Business Terms in a more nuanced way, focusing on the realities of the exchange. For example, OpenAI could argue that business users are given much broader access to ChatGPT, including access to the APIs, and that, in exchange for this enhanced access, OpenAI is asking licensees not to build competing models using their privileged access.

Importantly, even if the noncompetes are unenforceable, they can still potentially 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.[312]

3. Confidentiality

Finally, users of ChatGPT who obtain an Enterprise License are subject to a mutual confidentiality obligation. The Business Terms include 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 . . . ."[313] It obligates Recipients to "(a) only use Discloser's 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."[314] There are some exceptions for information that "(a) is or

309. *See supra* notes 294–295.

310. *See Business Terms*, *supra* note 93.

311. *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* 2 LOUIS ALTMAN & MALLA POLLACK, CALLMANN ON UNFAIR COMPETITION, TRADEMARKS AND MONOPOLIES, § 16:47 (4th ed. 2022).

312. 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)).

313. *Business Terms*, *supra* note 93.

314. *Business Terms*, *supra* note 93.

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."[315]

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.[316] Indeed, one major benefit of the Enterprise License, from the businesses' perspective, is that they can reduce the risk that their employees will use ChatGPT and give up their company's trade secrets.[317] However, the confidentiality provision in the Business Terms is written to be mutual. It protects OpenAI's trade secrets and confidential information as well.[318]

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.[319] 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.[320] 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.[321] Third, the confidentiality provision extends protection beyond trade secrets to cover a broader range of non-public

315. *Business Terms*, *supra* note 93.

316. *See Business Terms*, *supra* note 93.

317. *Introducing ChatGPT Enterprise*, *supra* note 94; *see also* Shelby Hiter, *ChatGPT Enterprise: AI for Business*, EWEEK (Sept. 6, 2023), https://www.eweek.com/artificial-intelligence/chatgpt-enterprise/.

318. 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)." *Business Terms*, *supra* note 93.

319. *See* Hrdy & Seaman, *supra* note 25, at 689.

320. 18 U.S.C. § 1839(5)(B)(ii)(II).

321. *See* Hrdy & Seaman, *supra* note 25, at 688–89.

information.[322] As shown above, the provision is drafted broadly to cover "Confidential Information"—including but not limited to trade secrets.[323]

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.[324] 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 II, some of this information may well qualify as trade secrets. If so, then an Enterprise licensee who uses or discloses this information might be liable for trade secret misappropriation in addition to breach of contract.[325]

Trade secret liability would extend not just to exact copying of OpenAI's information, but also to improvements and products "derived from" that information.[326] 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 allow 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 the Whoop example above.[327] But if the licensee acts outside of this permission, they could be liable for both breach of contract and trade secret misappropriation.

---

322. *Id.* at 689.

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

324. *Introducing ChatGPT Enterprise, supra* note 94.

325. *See* Hrdy & Seaman, *supra* note 25, at 685–93; *see also, e.g.*, Hampton Roads Connector Partners v. Land to Sand Site Servs., Inc., 2023 WL 8539536, at *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].").

326. *See, e.g.*, Gourmeta, Inc. v. Weilenmann, 1993 U.S. Dist. LEXIS 1201, *14–15 (N.D. Ill. 1993). This is different from copyright law which requires proving substantial similarity between the original product and the end product. *See, e.g.*, Mark A. Lemley, *The Fruit of the Poisonous Tree in IP Law*, 103 IOWA L. REV. 245, 267 (2017); *see also, e.g.*, Hrdy, *supra* note 163.

327. 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." *Business Terms*, *supra* note 93.

The story is different for individual users of ChatGPT. The current version of the ChatGPT "Terms of Use," which become effective December 11, 2024, do 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, only applying to OpenAI's and "third parties" information and not to users' information.[328] 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."[329] 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."[330]

The original provision faced criticism for being "unilateral" and came across as hypocritical. It seemed as if OpenAI made sure its own information was kept confidential,[331] but it did not make the same promise to users. ChatGPT was left free to absorb and train on users' informational inputs, while leaving users 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 provision."[332] 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,[333] but it contains no confidentiality clause at all.[334] As discussed in Part IV, the absence of a

328. *Terms of Use*, *supra* note 22.

329. *Terms of Use*, *supra* note 22.

330. *Terms of Use*, *supra* note 22.

331. 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 7, at 575.

332. Kate Downing, *OpenAI's Massive Data Grab*, LAW OFFICES OF KATE DOWNING (Mar. 10, 2013), https://katedowninglaw.com/2023/03/10/openais-massive-data-grab/; *see also, e.g.*, Noah, *Chat GPT Terms & Conditions Are Scary*, MEDIUM (May 11, 2023), https://medium.com/@thelightofday/chat-gpt-terms-conditions-are-scary-7a095eb38ebc (discussing concerns about users' privacy and other restrictions imposed on ChatGPT users).

333. *See Terms of Use, supra* note 22.

334. *See Terms of Use, supra* note 22.

confidentiality provision may create risks to OpenAI's ability to protect trade secrets related to ChatGPT.

IV. HOW COURTS CAN CHANGE THE STATUS QUO

Once information is no longer factually secret, it should not be legally protected as a trade secret. Yet contracts can create trade secret protection by mandating confidentiality and by prohibiting reverse engineering. Liability for breaching these contracts should generally be limited to breach-of-contract remedies. However, in software cases, courts have held that breaching a contract can sometimes constitute trade secret misappropriation as well. Courts reason that when reverse engineering is performed in breach of a contract, the breach of contract itself supplies the "improper means" required for trade secret liability—even if the underlying action would otherwise constitute legal reverse engineering.[335]

Scholars such as Pamela Samuelson have criticized this reasoning as applied to software.[336] But as discussed below, courts have permitted trade secret holders to succeed on this argument.[337] The same logic will likely apply to generative AI. Companies will argue that violating anti-reverse engineering clauses constitutes *both* breach of contract and trade secret misappropriation. This would mean that a person who extracts trade secrets from an AI model in breach of a terms of use would face liability under trade secret law as well as contract law.[338]

335. *See* 18 U.S.C. § 1839(5)(A) ("[T]he term 'misappropriation' means . . . acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means . . . "); *see also* 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 that knowingly breaching a contract that prohibits reverse engineering of software turns the act of reverse engineering into acquisition of trade secrets by improper means).

336. *See* Samuelson & Scotchmer, *supra* note 9, 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 COMMCN'S OF THE ACM 15, 15 (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.").

337. *See infra* notes 388–403 and accompanying text.

338. *See infra* notes 389–394 and accompanying text; *see also Terms of Use, supra* note 22.

This expansion of trade secret liability is concerning. It allows plaintiffs to seek civil—and potentially criminal[339]—trade secret remedies beyond contract law. Moreover, third parties who never entered a contract could still be liable if they knowingly acquire information obtained through "improper means." For example, if someone reverse engineers trade secrets in breach of a contract, and shares this information with a third party, who never signed the contract at all, a court might decide the third party knew or should have known that the information was acquired through improper means, and so the third party could also be liable.[340]

This reasoning is wrong. Courts should not accept that breach of an anti-reverse engineering clause, on its own, constitutes "improper means" of acquiring trade secrets. 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 from publicly distributed products or services.

There are several doctrinal levers through which courts can accomplish this, each of which is discussed in turn below: (A) the universal rule that reverse engineering is legal under federal and state trade secret law; (B) the nearly-universal rule that "readily-ascertainable" information is not a trade secret; and (C) the requirement that trade secret owners must demonstrate they took "reasonable" measures to protect information they claim to be trade secrets.

Finally, the DTSA, which became effective on May 11, 2016, makes all of these arguments far more compelling.[341] Unlike the UTSA, the DTSA explicitly states that "reverse engineering" is not an "improper means" of acquiring trade secrets as a matter of federal law.[342] The DTSA provides in Section 1839(6)(B) that "improper means" of acquiring a trade secret "does not include reverse engineering, independent derivation, or any other lawful means of acquisition."[343] Therefore, pursuant to the Supremacy Clause, it should no

339. Trade secret liability can even expose some defendants to criminal liability, assuming they possessed the requisite intent. This is something that contract law alone obviously does not do. 18 U.S.C §§ 1831–1832 (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* Kerr, *supra* note 32.

340. 18.U.S.C. § 1839(5). This is the fact pattern in *DVD CCA v. Bunner*, which I discuss *infra* notes 389–394; *see also supra* note 326 (explaining that trade secret liability reaches information derived from trade secrets, even if the end product is different).

341. 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, 108, n.8 (2018).

342. 18 U.S.C. § 1839(6)(B); *see also supra* notes 459–506 and accompanying text.

343. *See* 18 U.S.C. § 1839(6)(B).

longer be possible to argue under state trade secret law that reverse engineering constitutes acquisition of trade secrets through improper means.[344] Section (D) reveals that the DTSA gives rise to several novel "preemption" arguments that have yet to be raised—let alone tested—and 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

Even before the passage of the DTSA, it was well-established that "reverse engineering"—obtaining a product on the open market "by a fair and honest means" and picking that product apart to learn how it was made—is not trade secret misappropriation.[345]

However, the line between legal reverse engineering and acquisition of trade secrets by "improper means" is unclear. What counts as "improper" depends on the perceived social wrongness of the defendant's actions in the industry and context, and on the degree to which the defendant's success in accessing trade secrets was precipitated by the trade secret holder's own failure to protect against this sort of act.[346] 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 through garbage.[347] But courts have found other actions, such as picking locks to learn lock codes, to be lawful reverse engineering.[348]

---

344. U.S. CONST. art. VI.

345. *See Kewanee*, 416 U.S. at 487–93 (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. 2 (listing reverse engineering as a lawful means of acquiring trade secrets). For a survey of state trade secret laws, see Russell Beck, *50-State Noncompete Survey*, BECK REED RIDEN LLP, https://beckreedriden.com/50-state-noncompete-chart-2/ (last updated Sept. 26, 2024); *see also* Samuelson & Scotchmer, *supra* note 9, at 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.").

346. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. e (AM. L. INST. 1995).

347. *See* Victoria A. Cundiff, *Reverse Engineering the Competition*, Paper presented at Law Seminars International Program on Trade Secrets (2003) (citing, *e.g.*, E. I. DuPont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970); Tennant Co. v. Advance Mach. Co., 355 N.W.2d 720, 725 (Minn. Ct. App. 1984)).

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

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,[349] 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 company 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.[350] 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.[351]

When this legal case arises, two factors will significantly complicate courts' task in distinguishing between lawful reverse engineering and unlawful improper means.

1. Is Using Non-Human Means to Access Trade Secrets "Improper"?

First, successfully reverse engineering generative AI will *itself* likely require using AI or some form of automation that goes beyond what humans can do on their own. Courts could potentially view these enhanced techniques as "improper means," based simply on the fact that they rely on non-human means to gain access to trade secrets. If so, then otherwise-lawful 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 defendants hired a "hacker"[352] to obtain access to a database of insurance quotes "by

349. *See* text accompanying *supra* notes 233–234.

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

351. 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 (DMCA)—to the extent the person seeks access to copyrighted content. *See* Samuelson & Scotchmer, *supra* note 9, 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.

352. "Hacker" was the court's own descriptor. 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).

creating a robot" to "scrape" the plaintiff's website.[353] The lower court held defendants' actions were legal, given that the website was made "freely available to the public."[354]

The Eleventh Circuit reversed, holding the lower court failed to consider whether using a "bot" to obtain the database was "improper means."[355] 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."[356] To the contrary, the Eleventh Circuit strongly implied that the fact that defendants used *non-human means*—a "scraping attack" effectuated by 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 to extract data from a website to a flying an airplane over an unfinished chemical plant to take photographs—which the Fifth Circuit had held in a famous trade secret case was "improper means."[357] 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."[358]

The Eleventh Circuit remanded for the lower court to determine whether the "scraping attack" amounted to improper means.[359] On remand, the lower court held in favor of the plaintiff after a bench trial. The court held that the defendants acquired plaintiff's trade secrets using "improper means" by "using a robot to hack" the plaintiff's website.[360] The Eleventh Circuit affirmed.[361] One of the defendants filed a petition for certiorari to the U.S. Supreme Court; the Court is unlikely to hear the case.[362]

As it stands, the Eleventh Circuit's holding in *Compulife* might be read by future courts to suggest that using AI, automation, or any non-human means to learn trade secrets is "improper," notwithstanding the fact that reverse engineering is lawful under trade secret law. This is not the right approach.

353. Compulife Software Inc. v. Newman, 959 F.3d 1288, 1298–1300 (11th Cir. 2020).

354. *Id.* at 1312–14.

355. *Id.* at 1314.

356. *Id.*

357. *See DuPont*, 431 F.2d.

358. *Compulife*, 959 F.3d at 1314–15 (citing cases).

359. *Id.* at 1313.

360. *See* Compulife Software, Inc. v. Rutstein, No. 9:16-CV-80808, 2021 WL 3713173, at *21 (S.D. Fla. July 12, 2021), order clarified, No. 9:16-CV-80808-BER, 2021 WL 5830554 (S.D. Fla. Oct. 20, 2021).

361. *See* Compulife Software, Inc. v. Newman, 111 F.4th 1147, 1162–63 (11th Cir. 2024).

362. *See* Petition for Writ of Certiorari, Compulife Software Inc. v. Newman, No. 24-634 (U.S. Nov. 27, 2024).

There should not be a static, bright-line rule that using non-human means to extract trade secrets is unlawful. Indeed, the Eleventh Circuit itself cautioned against adopting an inflexible rule that using automated methods to discover information on the internet is always "improper" under trade secret law.[363] Instead, how courts treat such techniques in the future must depend on the facts of the case and the precise circumstances of the acquisition. Courts' positions should also be capable of change over time. If using non-human methods to extract data becomes more acceptable in the coming years, then a court should deem these methods proper reverse engineering. Past case law should not control every future technological iteration.

Still, *Compulife* demonstrates that this is a real possibility. Courts might view any attempt to reverse engineer an AI model using a model extraction attack, knowledge distillation, or another AI or computer-enhanced technique to be "improper" due to its inherent nature.

2. Is Breaching a "Terms of Use" to Access Trade Secrets "Improper"?

There is a second reason that extracting trade secrets from a publicly distributed generative AI model might be deemed trade secret misappropriation. That reason is, of course, contracts. Some courts have held that otherwise-lawful reverse engineering can be transformed into misappropriation when done in breach of a terms of use or end user license agreement (EULA). Essentially, breach of the contract itself is deemed to constitute "improper means" of acquiring trade secrets.[364]

As discussed in Part III, accessing a generative AI model like ChatGPT typically requires agreeing to various restrictions, such as "no reverse engineering" or "no competition." If a member of the public obtains a ChatGPT account and automatically extracts information about how ChatGPT was developed in order to create a competing model, this would breach ChatGPT's terms of use.[365] This hypothetical user could be held liable for breach of contract as well as trade secret misappropriation, because a court might determine that breach of the contract makes these actions—which would otherwise constitute lawful reverse engineering—"improper means" of acquiring trade secrets.

---

363. *See* Compulife Software, Inc. v. Newman, 111 F.4th 1147, 1162–63 (11th Cir. 2024) (noting that "scraping and related technologies (like crawling) may be *perfectly legitimate*[,]" though holding that in this case the defendants "did not take innocent screenshots of a publicly available site; instead, they copied the order of Compulife's copyrighted code and *used that code* to commit a scraping attack that acquired millions of variable-dependent insurance quotes.") (emphasis in original).

364. *See supra* notes 335, 389–392 and accompanying text.

365. *See Terms of Use*, *supra* note 22; *see also supra* notes 266–312 and accompanying text.

This is not a legitimate interpretation of the scope of trade secret law liability. Scholars like Pam Samuelson have observed that it would be problematic 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.[366] As Samuelson put it over twenty years ago, courts should recognize "the longstanding rule that reverse engineering 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."[367]

When Samuelson first 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.[368] Now there is. This generates a potential conflict between federal and state law regarding which types of actions to discover trade secrets qualify as lawful reverse engineering as opposed to unlawful 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.[369] Some state statutes differ, however, about whether reverse engineering *in breach of a contract* can itself constitute "improper means." Some states' statutes explicitly refer to breach of an anti-reverse-engineering clause as improper means of discovering trade secrets. Texas's 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 . . . ."[370] Other states'

366. Samuelson, *Reverse Engineering Under Siege*, *supra* note 335, 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*, LAW AND THEORY OF TRADE SECRECY (Rochelle C. Dreyfuss, Katherine J. Strandburg Eds., 2010).

367. Samuelson, *Reverse Engineering Under Siege*, *supra* note 335, at 1.

368. *See generally* Christopher Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317 (2015) (arguing against federalization of trade secret law); *but see* 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).

369. *See* 18 U.S.C. § 1839(6); *see also* citations *supra* note 345; *see also, e.g.*, Evolution, Inc. v. SunTrust Bank, 342 F. Supp. 2d 943, 962 (D. Kan. 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.").

370. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.006 (West 2023).

statutes refer to breach of duties "imposed . . . by contract [or] license" as an improper means of acquiring trade secrets.[371]

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* . . . ."[372] 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 breaches of any contractual duty, let alone a contractual duty not to reverse engineer.[373] 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.[374] That said, even if a breach of an anti-reverse engineering provision (as opposed to a breach of a confidentiality or nondisclosure provision) is not specifically delineated as improper means under these laws, the text is *not* written to be

371. 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. § 39-8-20 (2023).

372. 18 U.S.C. § 1839(6); UTSA, § 1); *see also* CAL. CIV. CODE § 3426, discussed *infra* note 374.

373. 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)).

374. 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). 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). 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* CAL. 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[.]").

exhaustive.[375] 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*.[376]

This choice is indeed what some courts have done. Both before and after the DTSA, some courts have determined that reverse engineering in breach of a license constitutes misappropriation of trade secrets.[377] Importantly, though, many of these cases often occur 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.[378] 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 that they will abstain from reverse engineering the other party's products.[379] In these situations, the reverse engineering provision is merely a 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 on the theory that the defendant acquired, used, or disclosed trade secrets in breach of a duty to maintain secrecy.[380] Courts do not strictly need to rely on the theory that breach of an anti-reverse-engineering clause, alone, constitutes acquisition through "improper means."

---

375. *See, e.g.*, DSMC, Inc. v. Convera Corp., 479 F. Supp. 2d 68, 71 (D.D.C. 2007) ("Courts have held . . . the statute does not provide an exhaustive list of what constitutes improper means. More generally, 'improper means' has been defined as those means that fall below the generally accepted standards of commercial morality and reasonable conduct."); eShares, Inc. v. Talton, No. 22-CV-10987, 2024 U.S. Dist. LEXIS 59936, at *19 (S.D.N.Y. Mar. 29, 2024) (noting that "[t]he language of [the DTSA] defines 'improper means' with terms like theft, espionage and breach of a duty to maintain secrecy[,]" and that "[a]lthough the definition is not exclusive, these terms make clear that the conduct requires a level of impropriety that merely accessing or downloading documents onto a personal device does not implicate.").

376. *See supra* notes 352–359.

377. The key line of cases is discussed in text accompanying *infra* notes 389–403.

378. *See, e.g.*, Rust-Oleum Corp. v. NIC Indus., No. 1:18-cv-01655-CL, 2023 U.S. Dist. LEXIS 190585, at *31–32 (D. Or. Oct. 23, 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., No. 04 Civ. 3531(LTS)(HBP), 2009 WL 7133660, at * 3, 20 (S.D.N.Y. Aug. 5, 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).

379. *See* discussion of this distinction in Hrdy & Seaman, *supra* note 25, at 682–83.

380. *See* 18 U.S.C. § 1839(5)(A)–(B); Hrdy & Seaman, *supra* note 25, at 686.

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."[381] When businesses or employees agree to terms of an agreement that significantly limits what they can do, this is just an ordinary contract that, all else being equal, the law should enforce.[382] But this is not what end user cases look like. In end user cases, the person doing the reverse engineering typically has no prior 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.[383] 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 clause in an end user license agreement is enforceable under contract law—which it may well be, given how contract law currently treats these provisions[384]—a breach of this provision should not give rise to trade secret law liability. Trade secret law does not stop others from reverse engineering a product that is available on the open market.[385] There is no obvious basis for distinguishing reverse engineering of a physical product, like a soft drink, from reverse engineering of a software product. "Reverse engineering of manufactured products involves manipulation of physical objects. Reverse engineering of computer software involves analysis of program texts."[386] The fact that software products—and now, generative AI

381. *See* Lemley, *supra* note 11, at 1286.

382. *Id.* at 1285.

383. *Id.* at 1286–87 (discussing the difference between negotiated contracts and "contracts of adhesion" entered with consumers); *see also* Lobel, *supra* note 257.

384. *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).

385. 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 supra* note 345.

386. *See* Samuelson & Scotchmer, *supra* note 214, at 1614, n.184. That said, Samuelson and Scotchmer note that "information-rich products of the digital economy . . . bear a higher quantum of applied know-how within the product distributed in the market[,]" in comparison to "manufactured goods," for which "much of the know-how required to make the goods

products—are "licensed" to users as "services," rather than "sold" as "goods," should not magically escape this characterization.[387]

The upshot is that someone who obtains access to a generative AI product and has no prior confidentiality obligation should 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 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.[388] 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*.[389] In *Bunner*, Jon Johansen reverse engineered putative trade secrets in violation of an anti-reverse engineering clause in an end user license agreement; then Andrew Bunner, who did not undertake an anti-reverse-engineering

---

remains within the factory when the products go to market …" *Id.* at 1579. In other words, they suggest reverse engineering "information-rich" goods like software might in some ways be *easier* without legal protection from reverse engineering.

387. This strategy has worked in copyright law, because the sale versus license distinction matters. The possessor of a copyrighted good who is an owner has more rights than a mere licensee. Courts have held that 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 the major protections for "owners," like the essential step defense and the first sale defense, don't apply. Guy Rub, *Against Copyright Customization*, 107 IOWA L. REV. 677, 685 (2022); *see also* Camilla Hrdy, *Guy Rub: Copyright or Contract?*, WRITTEN DESCRIPTION (May 17, 2021), https://writtendescription.blogspot.com/2021/05/guy-rub-copyright-or-contract.html. However, in trade secret law, there is no basis for drawing a distinction between a sale and a license. The trade secret statutes provide that reverse engineering is a proper means of obtaining trade secrets; it does not make the right to reverse engineer contingent on the status of being an owner. *See supra* note 345. 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).

388. 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, e.g.*, Chen, *supra* note 24, at 802–09; Laster, *supra* note 270, at 667–87.

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

obligation, posted the information on his website.[390] 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."[391] 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."[392] The case was appealed up to the 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 . . . ."[393] 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 an anti-reverse engineering clause in the end user license agreement.[394]

Fortunately, Judge Moreno wrote in a concurring opinion that the lower court had been incorrect to assume that reverse engineering in breach of the anti-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."[395] 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.

---

390. 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 the 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 websites, including a website maintained by Andrew Bunner. *Id.* at 871–72.

391. *Id.*

392. "[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, No. CV786804, 2000 WL 48512, at * 2 (Cal. Super. Ct. Jan. 21, 2000).

393. *See Bunner*, 31 Cal. 4th at 875.

394. *See id.*, n.5.

395. *See id.* at 901 n.5 (Moreno, J., concurring).

The second case, decided over a decade later, is *Aqua Connect, Inc. v. Code Rebel*. In *Code Rebel*, the Central District of California cited to Judge Moreno's concurrence in order to explicitly reject the argument that reverse engineering constitutes "improper means" for trade secret law purposes merely because it is done in violation of a contract.[396] The defendant, Code Rebel, allegedly 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).[397] 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. The court wrote:

> [T]he only improper means pled in the [complaint,] 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 breach does not convert reverse engineering into an "improper means" within the definition of California trade secret law.[398]

Code Rebel is a very important decision. It did the work which 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 contractual prohibition within a EULA. The court also made clear that software owners in such cases can still bring a breach of contract claim.[399] 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" or "fraudulent" violation of a EULA which "expressly prohibit[s]" reverse engineering can "constitute an improper means by which to reverse engineer" a trade secret.[400] The court conceded that California's UTSA states that "[r]everse engineering or independent derivation *alone* shall not be considered improper means."[401] But the court reasoned that the legislature's "[u]se of the word 'alone' indicates that

396. Aqua Connect, Inc. v. Code Rebel, LLC, No. CV 11-5764-RSWL (MANx), 2012 WL 469737, at *2 (C.D. Cal. Feb. 13, 2012) (citing *id.)*.

397. *Id.* at *2.

398. *Id.*

399. *Id.*

400. 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).

401. *Id.* (quoting CAL. CIV. CODE § 3426.1(a)) (italics added).

reverse engineering attended by some [other wrongful act] is improper."[402] 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."[403]

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 for purposes of trade secret law. The *Socal* court's focus on the California trade secret statute's use of the word "alone" is misguided. Federal trade secret law states that reverse engineering is a proper means of acquiring a trade secret; it makes no mention of the word "alone."[404] Even under California trade secret law, there is no basis for reading so much into the word "alone." The inclusion of the word "alone" does not mean that the reverse engineering must not have been prohibited by a contract; it means the product or service being reverse engineered must have been legally acquired on the open market.[405] 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."[406]

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 . . . ."[407] As I will explain in Section IV.D., this provision of the DTSA arguably *preempts* state laws that prohibit reverse engineering. This

402. *Id.*

403. *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.").

404. *See* 18 U.S.C. § 1839(6) (stating that "improper means" "does not include reverse engineering, independent derivation, or any other lawful means of acquisition[.]").

405. In other words, the word "alone" is simply reinforcing the well-established principle that if the product is illegally acquired and then reverse engineered, this would not be legal reverse engineering. *See* DVD Copy Control Ass'n, Inc. v. Bunner, 31 Cal. 4th 864, 901 (2003) (Moreno, J., concurring) ("Apparently the word 'alone' refers to the fact that the item reverse engineered would have to be obtained 'by a fair and honest means, such as purchase of the item on the open market for reverse engineering to be lawful.'"); *see also* UTSA § 1, cmt. ("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*[.]") (emphasis added).

406. *See* Aqua Connect, Inc. v. Code Rebel, LLC, No. CV 11-5764-RSWL (MANx), 2012 WL 469737, at *2 (C.D. Cal. Feb. 13, 2012).

407. 18 U.S.C. § 1839(6).

includes state laws that impose 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, individual users of ChatGPT—or any other information goods that are widely distributed on the open market[408]—will not be liable for trade secret misappropriation merely based on reverse engineering.[409]

B. READILY ASCERTAINABLE INFORMATION IS NOT A TRADE SECRET

There is another, potentially even more powerful doctrinal lever for finding that 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. Below, I explain how courts have erred and how they can change their approach.

Products that are distributed on the open market are often harder to protect under trade secret law. This is by design. Patents are supposed to be the main option for protecting a new product against competition.[410] Once reverse engineering a product's incorporated trade secret becomes technologically feasible, trade secret protection is 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.[411]

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.[412]

---

408. 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.

409. 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 Section IV.D., I question whether those contract claims might be preempted by the DTSA as well. *See supra* note 397.

410. *See* Lemley, *supra* note 31, at 313.

411. *See* 18 U.S.C. § 1839(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.").

412. *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").

As one court recently put it, "readily" means "in a ready manner" such as "without hesitating" or "without much difficulty."[413] 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,[414] or if it could be reverse engineered in a matter of hours, days, weeks, or potentially even months.[415] 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.[416]

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 short window of time, then this information should be deemed readily ascertainable and not protectable as a trade secret, period.[417]

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 requirement that trade secrets must not be readily ascertainable.[418] Second, even in jurisdictions that do include the not-readily-

413. Card Isle Corp. v. Farid, No. 1:21-CV-1971-TWT, 2023 WL 5618246, at *5 (N.D. Ga. Aug. 30, 2023) (citing Merriam-Webster and other case law); *see also* Sherkow, *supra* note 229, at 1066 ("While the contours of ready ascertainment are a source of significant dispute, courts have primarily focused on the effort or expense in recreating the information.").

414. *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).

415. Alpha Pro Tech, Inc. v. VWR Int'l, LLC, No. 12-1615, 2017 U.S. Dist. LEXIS 135507, at * 22 (E.D. Pa. Aug. 21, 2017) (finding 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").

416. 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 modified* (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).

417. *See* citations *supra* note 411; *see also* LaRoque, *supra* note 166, at 438–40 (arguing that in light of technological advances it is much easier to decompile object code in order to discern source code and that these "advances in reverse engineering of software make it more difficult to protect [software] trade secrets."); *see* Sherkow, *supra* note 229, at 1066 (arguing that in light of advances in DNA and genomic sequencing "it's not clear that DNA sequences are no longer 'readily ascertainable' or if they 'derive independent economic value' from their secrecy.").

418. *See* CAL. CIV. CODE §§ 3426–3426.11 (West 2023); 765 ILL. COMP. STAT. 1065/1–1065/9 (2023); OR. REV. STAT. §§ 646.461–646.475 (2023). Importantly, in California, the fact

ascertainable requirement, 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.[419] Third, most courts seem to agree that what counts as "readily" ascertainable is a question of fact,[420] 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.[421] The determinations of what is, or is not, "readily" ascertainable are so divergent that it is hard to derive bright line rules.[422]

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."[423] To the extent breach of a contractual duty, alone, is deemed an "improper" means of acquiring trade secrets, then it

---

that information is readily ascertainable by proper means in theory may be raised as an affirmative defense. Judicial Council of California Civil Jury Instructions (2023) No. 4420 ("[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]."). *But see* James Pooley, *The Messy Process of Making and Applying the Law*, IP WATCHDOG (Mar. 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 77, at 557.

419. *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*, *in* INTELLECTUAL PROPERTY AT THE EDGE: The Contested Contours of IP 271 (Rochelle Cooper Dreyfuss & Jane C. Ginsburg eds., Cambridge University Press 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).

420. *See* Life Spine Inc. v. Aegis Spine, Inc., 8 F.4th 531, 541 (7th Cir. 2021) ("[W]hether the information is public is a question of fact.").

421. *See, e.g.*, Gibraltar Lubricating Servs., Inc. v. Pinnacle Res., Inc., 486 S.W.3d 224, 226 (Ark. Ct. App. 2016) (holding jury entitled to decide plaintiff's lubricant formulas were trade secrets, 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 six hours to ascertain the ingredients' relative weights, all at a cost of $3,000 to $4,500 per lubricant.").

422. *See* Hrdy & Seaman, *supra* note 25.

423. *See* 18 U.S.C. § 1836(3); UTSA, § 1.

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 would require breaching a contractual anti-reverse engineering clause, or users would be contractually bound to keep any information they learn from the product confidential, then this information might *never* be deemed readily ascertainable through "proper" means.[424]

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' contractual promise to 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.[425] 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

424. 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." John Bean Techs. Corp. v. B GSE Grp., LLC, 480 F. Supp. 3d 1274, 1301 (D. Utah 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, No. CGC-21-588988, 2021 Cal. Super. LEXIS 156625, at *15–18 (Cal. Super. Ct. Feb. 10, 2021) (finding 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).

425. *Life Spine, Inc.*, 8 F.4th at 531 (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.*, *in* BIOTECHNOLOGY LAW REPORT (2023), https://www.liebertpub.com/doi/abs/10.1089/blr.2023.29316.phc.

such access unless they first sign confidentiality agreements."[426] 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.[427]

Fortunately, not all courts have accepted this position. For example, in a very recent decision, *Card Isle Corporation v. Edible Arrangements*, the Northern District of Georgia rightly held that the plaintiff did not own trade secrets in the computer code for integrating the plaintiff's product into a client's website, because this code was fully revealed to users.[428] The court held that 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.[429] 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 the plaintiff's clients at all. It was accessible to clients "via a 'right click' on any web browser." Thus, the plaintiff failed to show the "code embedded in the Defendant's website was not readily ascertainable."[430]

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,[431] 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

426. *Life Spine, Inc.*, 8 F.4th at 535–36.

427. *Id.* at 540–42 ("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.").

428. Card Isle Corp. v. Farid, No. 1:21-CV-1971-TWT, 2023 WL 5618246 (N.D. Ga. Aug. 30, 2023).

429. *Id.* at *15.

430. *Id.* at *5–7; *see also* Arkeyo, LLC v. Cummins Allison Corp., 342 F. Supp. 3d 622, 630 (E.D. Pa. 2017) (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").

431. *See* Hrdy & Lemley, *supra* note 103, at 61, n.296; Hrdy & Seaman, *supra* note 25, at 3035–36.

misappropriating trade secrets, as opposed to only breach of contract.[432] Under federal law and the law of most states, no one should face liability for trade secret misappropriation in this scenario—including true insiders like employees—because the information no longer qualifies as a trade secret.

The contrary interpretation would permit trade secrecy protection for information that can cheaply and quickly be reverse engineered. As mentioned earlier, some state laws—specifically, California, Illinois, and Oregon—still protect readily ascertainable information as a trade secret, at least when the defendant didn't themselves obtain the information that way.[433] For instance, if an insider like an employee gains access to ChatGPT training data through work, they would be liable for trade secret misappropriation under California law, even if others could theoretically obtain the information easily without having inside access.[434] However, this is not the case under federal law and the law of most states. When the only barrier preventing information from being deemed readily ascertainable is a EULA attached to a mass-marketed product, that information cannot be a trade secret.

C. CONTRACTS CANNOT REPLACE "REASONABLE" SECRECY PRECAUTIONS

Trade secret law requires taking "reasonable" measures to maintain the secrecy of any information that is claimed as a trade secret.[435] This is a *standard*, not a strict rule. What constitutes "reasonable" measures varies from case to case and depends on the context, the field, and the business in question.[436] As Deepa Varadarajan has observed, taking "reasonable" secrecy precautions generally requires ensuring that those who are granted access to the information are put "on notice" that it is intended to remain secret.[437]

---

432. 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.

433. *See supra* note 418.

434. *See id.*

435. *See* 18 U.S.C. § 1839(3).

436. Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179–80 (7th Cir. 1991); *see also* Varadarajan, *supra* note 217, at 222 (noting that what constitutes "reasonable" secrecy efforts is context-dependent and varies based on the size and capacity of the firm).

437. *See* Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357, 357 (2017) (asserting that the primary policy reason for trade secret law's reasonable secrecy precautions requirement is "to notify a relevant audience (employees and other business partners) about the existence and boundaries of claimed trade secrets thus reducing information costs for that audience."); *see also* Varadarajan, *supra* note 217, at 213–15 (arguing that "[f]orfeiture mechanisms" in IP law generally "serve an important signaling or notice function" and that trade secret law requires owners to "engage in ongoing reasonable secrecy efforts…to force owners to notify a relevant audience . . . about a proprietary claim.").

Satisfying the reasonable measures requirement is inherently challenging once a trade secret is revealed in product that is sold on the open market. 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 qualify as trade secrets. For instance, in a case involving real estate software, a court found the putative trade secret holder failed to take "reasonable" measures to protect software features that were visible to users, stating that the facets of the software that plaintiff was "claiming as its trade secret have long been available to hundreds of thousands of real estate agents."[438]

Nonetheless, contracts can significantly enhance trade secrecy protection for publicly distributed goods, because contracts can demonstrate that a trade secret holder sought to "preserve its software's confidentiality" by requiring customers to undertake confidentiality obligations through contract.[439] Courts have often held that trade secret holders can prove they took "reasonable" measures merely by pointing to "the existence . . . of an express agreement restricting disclosure."[440]

Some commentators have criticized the law's deferential treatment of contracts as a means to prove reasonable secrecy precautions. For example, Varadarajan observes that, "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."[441] But on the ground,

438. 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 (Cal. Super. Ct. Feb. 10, 2021).

439. *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").

440. 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. Ct. App. 1974))). *But see, e.g.*, Acuson Corp. v. Aloka Co., 257 Cal. Rptr. 368, 371–72 (Cal. Ct. App. 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 June 22, 1989.

441. Varadarajan, *supra* note 19, at 1567.

especially in software cases, courts have given significant weight to contracts as a means to prove reasonable measures.[442]

For example, in *QSRSoft, Inc. v. Restaurant Technology, Inc.*, the court held a defendant liable for misappropriating trade secrets related to the plaintiff's software user interface and functionality. The plaintiff licensed the software to restaurants like McDonalds' franchisees through a password-protected system. The defendant obtained access by inducing the plaintiff's customers to share their passwords, and then took screenshots.[443] Despite the basic nature of the information revealed in the screenshots, the court found that the plaintiff had satisfied its duty to protect the information, because the software was password-protected and because users of the software were subject to licensing agreements limiting its use and sharing.[444]

This type of case law supports the notion that requiring users to contractually agree not to discover, use, or share trade secrets—when accompanied by appropriate password protections—can satisfy the reasonable secrecy precautions requirement, potentially even for *visible* features like basic design and functionality.[445] However, this reasoning should come with limits. If a product's features are plainly visible to users, or can easily be discerned with minimal effort, continuing to release the product to the public under those circumstances should constitute a failure to take reasonable secrecy precautions.[446] As Elizabeth Rowe has observed, trade secrecy's reasonable measures requirement is constantly being updated in response to technological

442. *See* Altavion, Inc. v. Konica Minolta Sys. Lab'y, Inc., 226 Cal. App. 4th 26, 60–62 (2014) (holding that 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) (holding that 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.").

443. QSRSoft, Inc. v. Rest. Tech., Inc., No. 06 C 2734, 2006 WL 2990432, *5–6 (N.D. Ill. Oct. 19, 2006).

444. *Id.* at *1, *6; *see also, e.g.*, ImageKeeper LLC v. Wright Nat'l Flood Ins., No. 2:20-cv-01470-GMN-VCF, 2020 WL 4677299, at *2–4 (D. Nev. Aug. 12, 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).

445. *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).

446. In this scenario, the product's features should be deemed readily ascertainable too. *See supra* notes 411–417 and accompanying text.

advances that making learning secrets easier.[447] Methods for discovering the secrets behind generative AI models will continue to advance, making the models more vulnerable to reverse engineering. If a company continues to market a generative AI product and make it widely accessible despite knowing 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, to quote Varadarajan, "forfeited" the trade secrets it once had in that AI product.[448]

There is one final wrinkle. Recall that while the OpenAI Business Terms contain a confidentiality provision for ChatGPT, the individual user Terms of Use have no confidentiality provision. I think this could matter—at least for features plainly revealed to users. If OpenAI continues to distribute ChatGPT to users without requiring them to agree to any express confidentiality provision, this could eventually destroy 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.[449] For example, in *Turret Labs USA, Inc. v. CargoSprint, LLC*, the Second Circuit dismissed a software company's trade secret claims under the DTSA and under New York law because the plaintiff did not have "confidentiality or nondisclosure agreements in place" with users of its software.[450] 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."[451]

The current version of OpenAI's Terms of Use for individual users does not have a confidentiality provision. It is possible that a court could find that

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

448. *See* Varadarajan, *Forfeiting IP*, *supra* note 217, at 198 ("[A] failure to engage in ongoing reasonable secrecy efforts leads to forfeiture of the trade secret right.").

449. *See* Broker Genius, Inc. v. Zalta, 280 F. Supp. 3d 495, 515–22 (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.") (citations omitted).

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

451. *Id.* at *2–4.

OpenAI has forfeited trade secrets that are plainly visible or easily accessible to ChatGPT users.[452] Although OpenAI could point to the fact 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.[453] Separately, OpenAI could also point out that it requires individual users to obtain and enter a password in order to access ChatGPT.[454] However, courts will almost certainly look for express confidentiality provisions protecting the information as well.[455] Without a confidentiality provision or other signs of measures to preserve secrecy, courts will likely find that anything that is revealed from individuals' use of ChatGPT is not a trade secret at all.

D. THE ARGUMENT FOR PREEMPTION UNDER THE DTSA

These arguments were strong, even 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."[456] 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 . . . ."[457] 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

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

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

454. *See* Altavion, Inc. v. Konica Minolta Sys. Lab'y, Inc., 226 Cal. App. 4th 26, 60–62 (2014) (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).

455. *See, e.g.*, Taylor Made Express, Inc. v. Kidd, 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.").

456. *See* S. REP. NO. 114–220, at 10 (2016) (discussing reason for including 18 U.S.C. § 1839(6)(B)).

457. 18 U.S.C. § 1839(6)(B).

engineering,[458] the DTSA does not include any modifiers on the phrase "reverse engineering."[459] Reverse engineering is legal under trade secret law.

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.[460] 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."[461]

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."[462] There are three types of implied preemption: (1) "actual conflict" preemption, which is where there is an actual conflict between a state law and a federal law; (2) "field preemption," which is where Congress regulates so extensively that it is deemed to have occupied the field, leaving very little room for state law to operate; and (3) "purposes and objectives" preemption, which is where a state law conflicts with Congress' policy objectives in passing a federal law.[463]

458. *See supra* notes 400–404 and accompanying text.

459. *See* 18 U.S.C. § 1839(6)(B).

460. *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.").

461. 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, 22 U.S. 1, 211 (1824)).

462. *See, e.g.*, Caleb Nelson*, Preemption*, 86 VA. L. REV. 225, 226–29 (2000) (emphasis added) (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 402 (4th ed. 2011) (explaining express and implied preemption). 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, 524–31 (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).

463. *See* discussion *infra* notes 471–478; *see also* Nelson, *supra* note 462*,* at 226–29.

A state law that makes reverse engineering a form of trade secret misappropriation is preempted based on several of these theories pursuant to the Supremacy Clause.[464]

1. Express Preemption

Express preemption, again, occurs when Congress expressly indicates in the language of a statute that a certain state law is preempted.[465] 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 . . . ."[466] However, this provision does not apply to a state trade secret claim that is based solely on reverse engineering, because reverse engineering, the DTSA provides, is not "misappropriation of a trade secret" at all.[467] Congress has only stated that claims for "misappropriation of trade secrets" are not preempted.[468] For other state law claims, courts are free to engage in an implied preemption analysis.

2. Implied Preemption

As explained above, there are three types of implied preemption: "actual conflict" preemption; "field" preemption; and "purposes-and-objectives" preemption.[469] There is no field preemption in this situation.[470] As just explained, Congress allows states to pass their own trade secret laws and thus does not stop states from entering the field of trade secret law. But there is conflict preemption under both the "actual conflict" and the "purposes-and-objectives" analysis.

---

464. *See* 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.").

465. Note, *Preemption as Purposivism's Last Refuge*, 126 HARV. L. REV. 1056, 1057 (Feb. 2013).

466. 18 U.S.C. § 1838.

467. *Id.* at § 1839(6).

468. *Id.* at § 1838.

469. Technically, purposes-and-objectives preemption is treated as a form of conflict preemption. *Actual* conflict preemption occurs when a state action makes it "impossible" for party to comply with both federal and state law; purposes-and-objectives conflict preemption happens when the state law stands conflicts with the policies (the "purposes and objectives") of the federal law. *See Preemption as Purposivism's Last Refuge*, *supra* note 465, 1057.

470. Field preemption is rare. Field preemption as where it is clear Congress has chosen for a federal statutory or regulatory regime to occupy the entire field, leaving no room for state regulation). *Id.*; *see also, e.g.,* Arizona v. U.S., 567 U.S. 387 (2012) (Arizona's immigration law preempted under field preemption doctrine because federal government had enacted such comprehensive regulations in immigration that it occupied the whole field leaving little room for state action).

"Actual conflict" preemption occurs if there is an "actual conflict" between federal and state law.[471] An actual conflict can occur if it is "impossible for a private party to comply with both state and federal requirements . . . ."[472] A classic example is where a state law "prevents someone from doing something that the federal government has given them a right to do."[473]

This is exactly what is happening here. Federal trade secret law states that reverse engineering is a proper means of acquiring a trade secret and thus not misappropriation.[474] Thus, if someone acquires a trade secret through reverse engineering—or obtains a trade secret from someone else who reverse engineered the information—neither of those actors is liable for trade secret misappropriation under the DTSA.[475] If a state trade secret law provides that these acts of reverse engineering are instead "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. 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."

Of course, states can 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.[476] Some states have longer statutes of limitations than the DTSA.[477] But when it comes to the specific act of reverse engineering, Congress has made clear that reverse engineering is not an improper means of acquiring a trade secret. If a state law transforms into trade secret misappropriation an action that federal law provides is *not* trade secret misappropriation, this state law is in direct conflict with federal trade secret law.

---

471. *See* Hrdy, *supra* note 48, at 190 (discussing different kinds of "implied 'conflict' preemption").

472. English v. Gen. 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.").

473. Hrdy, *Getting Patent Preemption Right*, *supra* note 462, at 308 (applying this concept to state laws that restrict enforcement of federal patents).

474. *See* 18 U.S.C. §§ 1839(5)–(6).

475. 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 id.* § 1839(5)(B).

476. For example, California does not include the limitation that information not be readily ascertainable. *See* CAL. CIV. CODE § 3426.1 (West 2023).

477. *E.g.*, Ohio's statute of limitations is four years. OHIO REV. CODE § 1333.66. The DTSA's is three years. 18 U.S.C. § 1836(d).

The second form of implied preemption that is relevant in this context is "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."[478]

In this case, there is a 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.[479] Congress sought to create a "[c]arefully balanced" federal law in order to "provide a single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved."[480]

Although Congress chose not to broadly preempt State trade secret laws, Congress did create several explicit constraints on trade secret liability. Congress included a provision stating that "reverse engineering" is not an "improper means" of acquiring a trade secret,[481] as well as other limiting provisions, such as immunity for whistleblowers,[482] limitations on injunctions brought against departing employees,[483] and protection for otherwise-lawful disclosures under the Freedom of Information Act.[484]

Again, 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, for example, that states can sometimes protect subject matter that federal intellectual property laws leave unprotected.[485] However, once Congress has

478. Kewanee Oil Co. v. Bircron Corp., 416 U.S. 470, 479 (1974) (quoting Hines v. Davidowitz, 312 U.S. 52, 67 (1941)).

479. S. REP. NO. 114–220, at 1–2 (2016).

480. *Id.* at 14.

481. *See* 18 U.S.C. § 1839(6)(B).

482. *See id.* § 1833.

483. *See id.* § 1836(3)(A)(i)(I)–(II).

484. *See id.* § 1838 (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)").

485. 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. 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

determined to protect subject matter under a particular intellectual property regime, states cannot protect subject matter that Congress has expressly indicated it "wish[es] to remain free."[486]

When Congress passed the DTSA, Congress was operating under the assumption that trade secret law does not prohibit reverse engineering and that reverse engineering is "fair" and "lawful" method for "discovery of a trade secret[.]"[487] Unlike the UTSA, which mentioned reverse engineering as a "proper means" of acquiring trade secrets only in the Commentary,[488] Congress expressly provided that reverse engineering is not a form of trade secret misappropriation in 18 U.S.C. § 1839(6)(B).[489] Congress did not spell out its justification for clarifying that reverse engineering is a proper means of acquiring a trade secret, but that is only because the justification is so well-established that Congress did not need to state it.[490] By the year 2016, the

---

grant of power to Congress in the IP Clause); *see also* U.S. CONST. art. I, § 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).

486. *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 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 462, at 497, n.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").

487. The legislative history mentions "reverse engineering" several times as a significant limitation on trade secret rights. *See, e.g.*, S. REP. NO. 114-220, at 2–6 (2016) ("By maintaining [an invention] as a trade secret, an inventor could theoretically keep their invention secret indefinitely . . . But the downside is there is no protection if the trade secret is uncovered by others through reverse engineering . . . discovery of a trade secret by fair, lawful methods, such as reverse engineering . . . is permitted.").

488. 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[.]").

489. *See* 18 U.S.C. § 1839(6)(B).

490. Samuelson & Scotchmer, *supra* note 9, 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").

Supreme Court had already made those arguments in its patent preemption cases when considering whether state intellectual property laws interfere with federal patent law.

In the Supreme Court's patent preemption 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 by prohibiting the copying or "reverse engineering" of a product that is already available on the open market.[491] Otherwise, inventors might choose to rely on state law instead of federal law, decline to apply for federal patents, and potentially forgo the investment in innovation that federal patent law seeks to encourage.[492]

In *Kewanee v. Bicron*, the Court held that a state law that protected trade secrets, at a time when federal law did not, was *not* preempted by federal patent law—even though federal patent law exists in large part to encourage disclosure of inventions, rather than retaining secrecy.[493] However, the Court reasoned that trade secret law and patent law can generally "co-exist" because they perform complementary functions,[494] and because "[t]rade secret law provides far weaker protection in many respects than the patent law. *While trade secret law does not forbid . . . reverse engineering*, patent law operates 'against the world,' forbidding any use of the invention for whatever purpose for a significant length of time . . . ."[495] In *Kewanee*, the Court strongly indicated that a state trade secret law would *not* survive preemption if it did prohibit "reverse

491. *Bonito Boats*, 489 U.S. at 160–61 (striking down a Florida law that "prohibits the entire public from engaging in a form of reverse engineering of a product in the public domain" and holding that states cannot create "patent-like" protection for articles that do not meet Congress's "rigorous requirements of patentability"); *see also* Sears, Roebuck & Co. v. Stiffel Co., 376 U.S. 225, 232 (1964) (holding that state unfair competition law could not prevent copying of unpatentable pole lamp); *see also* Compco Corp. v. Day-Brite Lighting, Inc., 376 U.S. 234, 238 (1964) (ruling that state unfair competition law could not prevent copying of unpatentable lighting fixture).

492. *See* Hrdy, *State Patents as a Solution to Underinvestment in Innovation*, *supra* note 462, at 524–31.

493. Kewanee Oil Co. v. Bircron Corp., 416 U.S. 470, 493 (1974) (holding Ohio trade secret law not preempted by federal patent law).

494. 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." *Id.*

495. *Id.* at 489–90 (emphasis added) (citations removed); *see also id.* at 476 ("[T]rade secret law, however, does not offer protection against . . . 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.").

engineering."[496] 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.[497]

Thereafter, in *Bonito Boats, Inc. v. Thunder Boats, Inc.*, the Court held that a state law—which 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 obtain federal patents.[498] The Court implied in *Bonito* that the primary reason the boat hull law 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.[499]

Congress clearly had this Supreme Court case law in mind when it passed the DTSA and was operating under the assumption that trade secret law does not—and *cannot*—prohibit reverse engineering; otherwise, this would conflict with the policies behind U.S. patent law.[500] More broadly, Congress was clearly very familiar with the policy arguments in favor of making lawful reverse engineering the "default rule." As discussed above, reverse engineering is seen

496. *Id.* at 489–90; *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) (arguing that state laws can go too far and be preempted by federal patent law if they prevent reverse engineering).

497. *Id.* at 489–90.

498. *Bonito Boats*, 489 U.S. at 161 (reasoning that "because 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[,]" "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."). *But see* Hrdy, *State Patents as a Solution to Underinvestment in Innovation*, *supra* note 462, at 524–31 (critiquing this decision and arguing that states should be able to create their own patents in certain circumstances).

499. *Bonito Boats*, 489 U.S. at 151, 160.

500. *See, e.g.*, S. REP. NO. 114-220, at 2–6 (2016) (mentioning the fact that trade secret law does not prevent reverse engineering as a major limitation on trade secrecy protection).

as, generally, a good thing for public policy.[501] Preserving the right to engage in reverse engineering, to quote the Supreme Court in *Bonito Boats*, ensures a "backdrop of free competition"[502] and is "an essential part of innovation" that "often leads to significant advances in technology."[503] So long as reverse engineering is *not* prohibited by trade secret law, this helps maintain balance between the various intellectual property regimes, forcing inventors who cannot maintain secrecy to obtain patents and disclose their inventions through the patent system.[504] To quote the Supreme Court in *Kewanee*, so long as trade secret law permits "discovery of the trade secret by fair and honest means, *e.g.*, independent creation or reverse engineering," "[t]he 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."[505]

Based on the text of the DTSA, and based on these patent preemption precedents, a state law that classifies reverse engineering as trade secret misappropriation is preempted by both federal trade secret law and federal patent law under the Supremacy Clause, which states that "the Laws of the United States … shall be the supreme Law of the Land."[506]

If any of these preemption arguments are accepted, then reverse engineering would be a legal way to acquire trade secrets under both federal and state law. The mere existence of a contract prohibiting reverse engineering would not alter this rule. In many circumstances, reverse engineering of 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 was no trade secret liability.[507]

The arguments above did not address contract claims. However, one could argue that a state common law claim for breach of a contract that prevents reverse engineering is also preempted by the DTSA, and by federal patent

501. *See supra* notes 214–227 and accompanying text.
502. *Bonito Boats*, 489 U.S. at 151.
503. *Id.* at 160.
504. *Id.* at 1583–84.
505. *Kewanee*, 416 U.S. at 489–90 (citations removed).
506. *See* U.S. CONST. art. VI.
507. *See supra* note 397.

law,[508] given that the DTSA explicitly states that the term "improper means" "does not include reverse engineering[.]"[509] As noted above, the DTSA does not preempt state law remedies "for the misappropriation of a trade secret[.]"[510] But this should not shield claims for breach of contract. Courts can still engage in implied preemption analysis. Scholar Yang Chen, for example, asserts 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.]"[511]

The argument for implied preemption of state contract claims is similar to the argument for preemption of state trade secret claims. Congress provided in 18 U.S.C. § 1839(6)(B) that reverse engineering is not an improper means of acquiring a trade secret, so when state law generates contractual liability for doing exactly that, this conflicts with the spirit, if not the letter, of Section 1839(6)(B), and with the policies motivating it.

However, the argument for contract preemption under the DTSA is comparatively weaker for several reasons. First, Section 1839(6)(B) states that "the term 'improper means' … does not include reverse engineering[.]"[512] This provision is specifically referencing a form of trade secret law liability (acquisition of trade secrets by improper means), and is specifically referring to an act (reverse engineering) which the Supreme Court has stated in its patent preemption jurisprudence is legal under trade secret law.[513] Congress did not, in Section 1839(6)(B), say anything about whether reverse engineering can give rise to contract law liability.[514]

Second, state trade secret law itself has historically *not* preempted state contract remedies. To the contrary, The UTSA, in Section 7, states that "[t]his [Act] does not affect . . . contractual remedies, whether or not based upon misappropriation of a trade secret."[515] "Under a plain reading of this text, the

508. At least one scholar has made the argument the Supreme Court's patent preemption jurisprudence preempts state contracts that prohibit reverse engineering, at least in some circumstances. *See, e.g.*, Laster, *supra* note 270, at 650–67 (arguing that under *Kewanee* and *Bonito Boats* a "mass market" contract that prohibits reverse engineering "for interoperability purposes" is preempted by federal patent law).

509. 18 U.S.C. § 1839(6)(B).

510. *Id.* § 1838.

511. *See* Chen, *supra* note 24, at 805.

512. 18 U.S.C. § 1839(6)(B).

513. *See Bonito Boats*, 489 U.S. at 151–60 (stating that preventing reverse engineering "has never been a part of state protection under *the law of unfair competition or trade secrets*[.]") (emphasis added).

514. Section 1839(6)(B) does *not* state, for example, that "breach of contract" does not include "reverse engineering." *See* 18 U.S.C. § 1839(6)(B).

515. *See* UTSA § 7.

UTSA does not supersede 'contractual remedies' resulting from breach-of-contract claims, whether or not based on misappropriation of a trade secret."[516]

Third, courts have not been receptive to these arguments in the past. And courts may follow the same reasoning here, for better or worse. In its patent preemption jurisprudence, the Supreme Court has tended to be respectful of contracts, even when they go beyond the protection afforded by intellectual property rights, reasoning that contracts—unlike intellectual property rights—represent private bargains that are likely to enhance rather than constrain innovation.[517] Likewise, lower courts have largely declined to preempt contract claims, even when they protect subject matter that patent or copyright would law would not.[518]

Finally, the reality is that contractual remedies are far more limited than trade secret law remedies. Trade secret law permits prevailing parties to more easily obtain injunctions and to achieve greater damages awards, along with the opportunity for attorney's fees, and comes with the risk of potential criminal penalties.[519] In contrast, a defendant who is sued for breach of contract can typically choose to breach the contract and pay compensable damages without experiencing excessive penalties. This means that, when breach of contract is the only consequence, "efficient breach" remains possible.[520] Efficient breach is where a party, who is bound to a contract, chooses to breach the contract, but is able to compensate the other party, while also enhancing overall social welfare through their activities.[521] Under the *Code Rebel* approach discussed above—where knowingly violating a term of use to reverse engineering computer software is breach of contract but *not* trade secret

516. *See* Hrdy & Seaman, *supra* note 25, at 699–703 (discussing the "contract exception" to preemption under trade secret law).

517. *See, e.g.*, Aronson v. Quick Point Pencil Co. 440 U.S. 257, 266 (1979) (holding a royalty agreement was not preempted by federal patent law, even though the subject of the contract was an unpatentable invention, concluding that "[e]nforcement of these contractual obligations, freely undertaken in arm's-length negotiation . . . will 'encourage invention in areas where patent law does not reach[.]'") (citations omitted).

518. *See, e.g.*, Chen, *supra* note 24, at 802–09; Laster, *supra* note 270, at 667–87; *see also* Hrdy & Seaman, *supra* note 25, at 703–706 (discussing case law declining to preempt contract claims under patent law or copyright law) (citing, e.g., ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453–55 (7th Cir. 1996).

519. *See* Hrdy & Seaman, *supra* note 25, at 687–88.

520. *See, e.g.*, Dave Fagundes, *Efficient Copyright Infringement*, 98 IOWA L. REV. 1791, 1794 (2013) ("[C]ontract law typically limits recovery to expectation damages in cases of nonperformance in order to avoid overcompensating promisees—thereby encouraging 'efficient breach.'").

521. *See id.* at 1791 (arguing that copyright law needs a theory of "efficient infringement" because maximizing creative production requires some level of unauthorized use . . .").

misappropriation[522]—a competitor who wishes to reverse engineer a generative AI model in breach of a terms of use can do so, and pay the fine. This is, in essence, a liability rule rather than a property rule.[523]

That said, some scholars have argued recently that courts should revive copyright preemption doctrine, and use this revitalized doctrine to preempt contractual clauses that restrict reverse engineering of generative AI models or that prohibit competition with the original developer.[524] One of the main points of this Article has been courts should not blindly follow precedents set for software that were incorrect at the time and that have effectively been overruled by the DTSA since then. They should not be deterred from finding a better path forward.

V. 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 and legal secrecy.[525] 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 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

522. *See supra* notes 396–399.

523. *See* Guido Calabresi & Douglas Malamed, *Property Rules, Liability Rules and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1089 (1972) (introducing the distinction between property rules and liability rules as alternative mechanisms for protecting entitlements and structuring legal remedies). *But see* Richard A. Epstein, *A Clear View of The Cathedral: The Dominance of Property Rules*, 106 YALE L.J. 2091, 2091 (1997) (critiquing Calabresi and Melamed's framework, arguing that property rules should generally take precedence over liability rules due to their efficiency in protecting entitlements).

524. *See* Mark A. Lemley & Peter Henderson, *The Mirage of Artificial Intelligence Terms of Use Restrictions*, Princeton University Program in Law & Public Affairs Research Paper No. 2025-04, 10 Jan 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5049562 (arguing that many of the AI companies' terms of use should be preempted by copyright law and that courts may begin turning away from the no-preemption approach); *see also* Guy A. Rub, *Moving from Express Preemption to Conflict Preemption in Scrutinizing Contracts over Copyrighted Goods*, 56 AKRON L. REV. 301, 302 (2023) (discussing recent case law holding that certain contracts were expressly preempted by the Copyright Act, though noting that "only contracts between sophisticated parties were being litigated").

525. *C.f.* Sandeen & Aplin, *supra* note 52, at 443–44; Tschider, *supra* note 4, at 710, 715.

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 held 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.

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. 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 enabled reverse engineering to trigger trade secret law liability as well as contract law liability.

This Article has identified several 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 transform otherwise-legal reverse engineering into an improper means of acquiring information. Second, trade secrets end when they become "readily ascertainable" through proper means. If information can easily and cheaply be discovered by inspecting a product, then it is readily ascertainable through "proper" means and not a trade secret. The mere presence of a mass-market, non-negotiated restriction on reverse engineering cannot change this reality.[526] Third, trade secrets are, by statute, forfeited if the owner fails to take "reasonable" measures to keep the information secret. Contracts can help owners satisfy this requirement. 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.

The passage of the DTSA in 2016 makes these doctrinal arguments more compelling than they were ten years ago, because the DTSA explicitly states that reverse engineering is not an improper means of acquiring trade secrets as a matter of federal law.[527] The DTSA thus gives rise to several new arguments for preemption. The strongest argument is that a state law that turns reverse

526. 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.

527. *See* 18 U.S.C. § 1839(6); *see also* Kewanee Oil Co. v. Bircron Corp., 416 U.S. 470, 476 (1974).

engineering into trade secret misappropriation conflicts with the purposes and objectives underlying the DTSA, not to mention federal patent law.[528] Giving life to this new brand of preemption 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 all. But this doctrinal approach will ensure that, once reverse engineering is technically feasible, companies cannot maintain legal protection forever.

528. *See supra* notes 478–507 and accompanying text.