TRADE SECRETS IN THE ARTIFICIAL INTELLIGENCE ERA

John G. Sprankling*

Artificial intelligence ("AI") is the most revolutionary technology in centuries. It will have a profound impact on intellectual property law. For the first time in history, machines may equal or surpass the ability of humans to create valuable ideas—posing an unprecedented challenge to this human-centric law. Scholars have explored the effect of AI on patent law and copyright law, but have overlooked its impact on trade secret law.

This is the first Article to analyze how AI will reshape trade secret law. It explores whether AI-generated information should qualify for trade secret protection and, if so, who should own those secrets. The Article then evaluates how key doctrines that limit protection for policy reasons will be recalibrated in light of AI abilities, potentially terminating certain human-created secrets. Finally, it considers how trade secret law may mitigate dangers that AI potentially poses to humanity.

* Professor of Law, University of the Pacific, McGeorge School of Law.

I. INTRODUCTION

Artificial intelligence ("AI") presents a fundamental challenge to trade secret law, the principal doctrine that protects valuable information. Businesses in the United States own human-created trade secrets worth approximately $5 trillion,[1] ranging from the formula for Coca-Cola to the Google search algorithm, which is more than the value of their patents.[2] Yet today AI can create valuable information with little or no human input. Experts predict that advanced forms of AI will vastly exceed human abilities in the future. As Sundar Pichai, the CEO of Alphabet, observed, AI is "the most profound technology humanity is working on . . . [m]ore profound than fire, electricity, or anything that we have done in the past."[3]

On the one hand, AI offers the opportunity to vastly expand the extent of information that can help humans in the future, such as new medicines, inventions, and business strategies. It is foreseeable that the process of creating trade secrets will increasingly be dominated by AI, rather than by

1. Shira Perlmutter, *One Year On: Developments in the Protection of Trade Secrets*, U.S. PAT. & TRADEMARK OFF.: DIRECTOR'S F. BLOG (June 29, 2017, 11:51 AM), https://www.uspto.gov/subscription-center/2017/one-year-developments-protection-trade-secrets [https://perma.cc/ZBE7-Q3DH].

2. *See* Sheldon Brown, *Patent Statistics*, PATENT EXPERTS (Mar. 22, 2023) (noting that U.S. patents are worth an estimated $3 trillion), https://patentexperts.org/patent/statistics/ [https://perma.cc/8VUA-2YS7].

3. Beatrice Nolan, *Sundar Pichai Says AI Technology Could Be More Profound than Fire or Electricity*, BUS. INSIDER (Apr. 17, 2023, 6:33 AM), https://www.businessinsider.com/sundar-pichai-google-ai-bard-profound-tech-human-history-2023-4 [https://perma.cc/9BEW-5U5N]; *see also* Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023) ("Artificial intelligence (AI) holds extraordinary potential for both promise and peril.").

humans.[4] Conversely, AI threatens the existence of many trade secrets developed by humans in the past. AI inevitably will reshape the contours of trade secret law. This Article is the first academic work to analyze how that evolution will develop.

The future of trade secret law is particularly important because an invention created by AI is not patentable unless the process involved a significant contribution by a human.[5] As a result, an invention made with little or no human involvement will enter the public domain unless it qualifies for trade secret protection.[6]

Part I explains how AI challenges the policy balance that underpins trade secret law. This balance was premised on the assumptions that (1) only humans could create valuable information and (2) they require a legal incentive to do so. But advanced AI systems can already generate trade secrets with little or no human involvement; and these systems are not motivated by legal incentives.

Part II analyzes the promise of AI-created trade secrets. It explores the extent to which AI can develop valuable information and analyzes whether it should be protected by trade secret law. This Part then addresses the key issue of who should be recognized as the owner of an AI-created trade secret. The issue of ownership rights to AI-created inventions and artistic works has generated controversies in patent law and copyright law,[7] but the issue has not yet arisen in trade secret law.[8]

Part III evaluates the threat that AI poses to human-created trade secrets. For example, a core concept in trade secret law is that protection for a secret ends when the information becomes "readily ascertainable." The ability of AI to synthesize, process, and utilize data means that certain existing secrets which were once difficult to ascertain—such as customer lists—may now be readily ascertainable by AI, and thus lose protection. However, it is not clear if AI may be legally used to obtain a trade secret that already exists; this

4. As Tim Dornis explains, "we are on the threshold of an age of *substitution* of human creativity by artificial creativity." Tim W. Dornis, *Artificial Creativity: Emergent Works and the Void in Current Copyright Doctrine*, 22 YALE J.L. & TECH. 1, 5 (2020) (emphasis in original).

5. *See* Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. 10043, 10046 (Feb. 13, 2024).

6. *See infra* text accompanying notes 105-111.

7. *See infra* text accompanying notes 96-116.

8. For example, despite its broad title, Gregory Gerard Greer, *Artificial Intelligence and Trade Secret Law*, 21 UIC REV. INTELL. PROP. L. 252, 263 (2022), only addresses the issue of whether AI algorithms should be protected as trade secrets. Similarly, David S. Levine, *Generative Artificial Intelligence and Trade Secrecy*, 3 J. FREE SPEECH L. 559, 562 (2023), only considers free speech issues.

method might be viewed as "improper means," subjecting human controllers to liability for misappropriation.[9]

Finally, Part IV considers how trade secret law might mitigate the threat that AI potentially poses to humans. The algorithms that underlie AI programs—and much of the information they generate—will be protected by trade secret law. But under narrow circumstances, an employee, attorney, or other knowledgeable person should be entitled to disclose a trade secret to protect human health and safety in the event this becomes necessary in the future.

II. REBALANCING TRADE SECRET LAW

A. A Human-Centric Doctrine

Trade secret law strikes a balance between incentivizing humans to develop valuable information and limiting the protection accorded to owners of that information.[10] The field is dominated by two statutes: the Uniform Trade Secrets Act ("UTSA"),[11] which has been adopted by almost all states,[12] and the federal Economic Espionage Act, as amended by the Defend Trade Secrets Act ("DTSA").[13] Because the DTSA was based on the UTSA, the substantive provisions of these statutes are almost identical. Under both statutes, a trade secret is (1) information, (2) which has "economic value, actual or potential," (3) which is not "generally known" or "ascertainable by proper means" by others who can obtain economic value from it, and (4) is the subject of "reasonable" efforts to maintain its secrecy.[14]

9. *See generally* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 318–19 (2008) (discussing judicial approaches to determining whether improper means were utilized to obtain a trade secret).

10. *See infra* text accompanying notes 17-25.

11. The most recent version of the Uniform Trade Secrets Act was adopted in 1985. UNIF. TRADE SECRETS ACT (UNIF. L. COMM'N 1985) [hereinafter "UTSA"]. Prior to enactment of the UTSA, trade secret law was poorly developed, often leading to confusion. *See* Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CALIF. L. REV. 1, 15 (2017).

12. Every state has adopted the UTSA except for New York. 1 PETER S. MENELL ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE: 2023, at 45 (2023).

13. Economic Espionage Act of 1996, Pub. L. No. 104-294, § 101(a), 110 Stat. 3488, 3488-3513 (1996) *amended by* Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376, 376-86 (2016) (current version at 18 U.S.C. §§ 1831-1839) (the current version of 18 U.S.C. §§ 1831-1839 will be referred to as the "DTSA").

14. UTSA, *supra* note 11, § 1(4); 18 U.S.C. § 1839(3).

The term "trade secret" is a historic misnomer because today it encompasses information which is not used in a trade or business.[15] Accordingly, the term includes virtually any type of valuable information, including algorithms, business methods, compilations, cost data, customer lists, designs, drawings, financial statements, formulas, inventions, marketing strategies, patterns, price data, product specifications, production processes, recipes, religious materials, research findings, sales data, social media contacts, and software.[16]

Patent law and trade secret law are close cousins because both protect valuable information to serve the policy goal of promoting innovation for the public good. As the Supreme Court observed in *Kewanee Oil Co. v. Bicron Corp*., "[t]rade secret law will encourage invention in areas where patent law does not reach."[17] Yet in operation, these doctrines utilize quite different approaches. While the threshold for issuance of a patent is high[18] and the term is only twenty years,[19] patent protection is strong—the patentee has a monopoly on the invention for the patent term, patent infringement is a strict liability offense, and there are few defenses to enforcement of a valid patent.[20]

In contrast, the threshold for creating a trade secret is low,[21] and the resulting protection is correspondingly fragile, for policy reasons. For example, anyone can reverse engineer[22] or independently develop[23] a trade

15. Historically, trade secret law only protected certain valuable information used in a trade or business. *See* RESTATEMENT OF TORTS § 757 cmt. b (AM. L. INST. 1939). The UTSA and DTSA removed this limitation, but the doctrine was not renamed to reflect the change. UTSA, *supra* note 11, § 1 cmt. (noting that the broader definition of "trade secret" in the Act "extends protection to a plaintiff who has not yet had an opportunity or acquired the means to put a trade secret to use"); *see also* 18 U.S.C. § 1839(3) (similarly not imposing a "use" requirement for trade secret protection to accrue).

16. *See* 18 U.S.C. § 1839(3); see *also Trade Secrets*, WIPO, https://www.wipo.int/tradesecrets/en/ [https://perma.cc/VCZ9-AWTA].

17. 416 U.S. 470, 485 (1974); *see* Lemley, *supra* note 9, at 330–31 (discussing *Kewanee Oil* and the policy bases for protecting trade secrets); *see also* Menell, *supra* note 11, at 8–9 (observing that "trade secret law [was] built on two core principles: maintaining commercial morality (preventing commercial espionage) and promoting technological innovation"). Despite dicta indicating otherwise in *Kewanee Oil*, in some situations today an invention could be protected by either patent law or trade secret law, giving the inventor a choice between the two regimes. But if an otherwise-patentable invention is created by AI without a substantial contribution by a human, it cannot be patented. *See* Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. 10043, 10046 (Feb. 13, 2024). This leaves trade secret law as the only other potential source of protection. *See infra* text accompanying notes 105-113.

18. *See* 35 U.S.C. §§ 101-103, 112.

19. *Id.* § 154(a)(2).

20. *Id.* § 271(a); *see also* MENELL ET AL., *supra* note 12, at 419–48 (discussing defenses to patent infringement).

21. *See infra* text accompanying notes 22-25.

22. UTSA, *supra* note 11, § 1 cmt.; 18 U.S.C. § 1839(6)(B).

23. UTSA, *supra* note 11, § 1 cmt.; 18 U.S.C. § 1839(6)(B).

secret already owned by another, and thus functionally become a co-owner of the secret. Moreover, a trade secret ends when it becomes generally known to, or readily ascertainable by, other people, or when the owner fails to take reasonable precautions to protect it.[24] In these situations, the original owner loses its monopoly on the secret.[25] The limiting doctrines are essential for the trade secret balance because they allow others to use the information, thereby benefiting the public.

B. The Rise of AI

The rise of AI endangers the trade secret balance in two ways. First, AI can create valuable new information without a legal incentive to do so.[26] Over time, this may reduce the motivation for humans to create such information. Second, because AI will be more adept than humans in discovering existing trade secrets, the limiting doctrines that curtail protection will weigh more heavily in the balance.[27]

In simple terms, AI can be defined as a machine "that can perform tasks that require human-level intelligence."[28] The debut of ChatGPT-3.5 on November 30, 2022, transformed AI from an esoteric concept to an everyday reality.[29] It became the first generative AI system freely available for public use, and competing systems soon followed.[30] In essence, generative AI is a type of machine learning technology capable of producing new and original content based on massive amounts of training data, in response to natural language "prompts" by a human operator. It differs fundamentally from traditional AI systems, which are trained to perform specific tasks based on limited data sets.[31] Rather, it is a general-purpose system designed to mimic

24. *See* UTSA, *supra* note 11, § 1(4); 18 U.S.C. § 1839(3).

25. Accordingly, a trade secret might conceivably last forever unless one of these limiting doctrines applies.

26. *See infra* text accompanying notes 52-77.

27. *See infra* text accompanying notes 167-231.

28. HENRY A. KISSINGER ET AL., THE AGE OF AI: AND OUR HUMAN FUTURE 14 (2021); *see also* NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES 11 (2014) ("Artificial intelligence already outperforms human intelligence in many domains.").

29. "GPT" is shorthand for "generative pretrained transformer," which describes its neural network system. Greg Pavlik, *What Is Generative AI? How Does It Work?*, ORACLE (Sept. 15, 2023), https://www.oracle.com/artificial-intelligence/generative-ai/what-is-generative-ai/ [https://perma.cc/V9R9-ZNG7].

30. Alex Hughes, ChatGPT*: Everything You Need to Know About OpenAI's GPT-4 Tool*, BBC SCI. FOCUS (Sept. 25, 2023, 12:13 PM), https://www.sciencefocus.com/future-technology/gpt-3 [https://perma.cc/TTQ6-WD9H]; Kaushik Pal, *What Are the Best ChatGPT Alternatives? 12 ChatGPT Rivals*, TECHNOPEDIA (May 1, 2024), https://www.techopedia.com/who-are-the-competitors-of-chatgpt [https://perma.cc/BP3F-HSRW].

31. *See id.* Information developed by these systems with extensive human assistance can be described as "AI-assisted" rather than "AI-generated."

human creativity in a broad range of areas, which far surpasses the ability of prior systems.

The development of a generative AI system begins with building an artificial brain—a neural network consisting of software with interconnected artificial neurons arranged in deep layers.[32] The network typically consists of three sections: one set of layers for receiving input data; a second and deeper set for processing the information; and a third set for generating output.[33] The most prevalent system uses an adversarial network consisting of two parts, one producing information and the other determining its accuracy.[34]

A generative AI system is trained on huge and diverse data sets. For example, ChatGPT-3.5 was initially trained on 570 gigabytes of data taken from internet sites, books, and other sources.[35] The system is then prompted to make predictions on that data repeatedly, potentially over one trillion times, while receiving feedback each time to refine its accuracy.[36] Eventually, humans evaluate the quality of the output and provide guidance on improvement, which is then incorporated into the system.[37] Ultimately, the system has the ability to discover patterns and relationships that humans cannot perceive.[38]

Yet the exact manner in which these systems function is unknown. As a former chief technology officer of multiple AI startups explains: "[w]e don't know how they do the actual creative task because what goes on inside the

---

32. *See* ALGER FRALEY, THE ARTIFICIAL INTELLIGENCE AND GENERATIVE AI BIBLE 30–31 (2023); *see also* TOM TAULLI, ARTIFICIAL INTELLIGENCE BASICS: A NON-TECHNICAL INTRODUCTION 72–73 (1st ed. 2019).

33. DAVID M. PATEL, ARTIFICIAL INTELLIGENCE & GENERATIVE AI FOR BEGINNERS 36–37 (2023).

34. *See* FRALEY, *supra* note 32, at 48; TAULLI, *supra* note 32, at 78.

35. Hughes, *supra* note 30. As two authorities summarized, data is vitally important for generative AI: "Today, data is no longer merely a record of a past event, but also a kind of energy source for the creation and improvement of intelligent behavior and the nascent capability of AI to reason." Jared Cohen & George Lee, *The Generative World Order: AI, Geopolitics, and Power*, GOLDMAN SACHS (Dec. 14, 2023), https://www.goldmansachs.com/intelligence/pages/the-generative-world-order-ai-geopolitics-and-power.html [https://perma.cc/L3WU-8XGJ]. A number of corporations have sued AI companies, arguing that the use of their copyrighted works for AI training purposes constitutes infringement. *See, e.g.*, Brody Ford & Brad Stone, *Time Owner Benioff Says AI Companies 'Stole' Training Data*, BLOOMBERG LAW (Jan. 16, 2024, 12:57 PM), https://news.bloomberglaw.com/artificial-intelligence/time-owner-benioff-says-ai-companies-stole-training-data [https://perma.cc/299L-SHH4]; Isaiah Poritz, *OpenAI Faces Existential Threat in New York Times Copyright Suit*, BLOOMBERG LAW (Dec. 29, 2023, 12:47 PM), https://news.bloomberglaw.com/ip-law/openai-faces-existential-threat-in-new-york-times-copyright-suit [https://perma.cc/F34T-9PKX].

36. *See* Pavlik, *supra* note 29. Neural networks "learn from experience, finding natural ways of generalizing from examples and finding hidden statistical patterns in their input." BOSTROM, *supra* note 28, at 8.

37. Pavlik, *supra* note 29.

38. Taulli, *supra* note 32, at 89.

neural network layers is way too complex for us to decipher, at least today."[39] Some researchers assert that ChatGPT-4, the more powerful successor to ChatGPT-3.5, has "built up an internal model of how the world works, just as a human brain might, and it uses that model to reason through the questions put to it."[40]

The capacity of AI to create valuable information is increasing exponentially, while human abilities remain constant.[41] Ultimately, AI abilities will vastly exceed what humans can do.[42] As a result, we must reconsider how the trade secret balance should be struck for this new era.

III. THE PROMISE OF AI-GENERATED TRADE SECRETS

A. AI Creation of Trade Secrets

1. From Tool to Creator

Advanced AI systems can generate a wide range of new information that qualifies for protection as trade secrets, with varying levels of human involvement. Early forms of AI were viewed as tools for humans to use, like a microscope or a computer.[43] But today there is a broad consensus that modern systems are qualitatively different from such tools.[44] The stunning success of the ChatGPT series, in particular, demonstrates that generative AI

39. PAVLIK, *supra* note 29 (quoting Dean Thompson, a "former chief technology officer of multiple AI startups").

40. *Id.*

41. Scientist Douglas Hofstadter "points out[] [that] these artificial brains are not constrained by the factors that limit human brains—like having to fit inside a skull. And[] . . . they are improving at an astounding rate, while human intelligence isn't." David Brooks, *Human Beings Are Soon Going to Be Eclipsed*, N.Y. TIMES (July 13, 2023), https://www.nytimes.com/2023/07/13/opinion/ai-chatgpt-consciousness-hofstadter.html [https://perma.cc/LLM3-ZQZ4].

42. *See* BOSTROM, *supra* note 28, at 22. The founders of OpenAI stated the following: "it's conceivable that within the next ten years, AI systems will exceed expert [human] skill level in most domains . . . ." *What Would Humans Do in a World of Super-AI?,* THE ECONOMIST (May 23, 2023), https://www.economist.com/finance-and-economics/2023/05/23/what-would-humans-do-in-a-world-of-super-ai [https://perma.cc/N7CQ-C885].

43. The Patent and Trademark Office ("PTO") categorizes AI systems as "tools" even if they were "instrumental in the creation of [an] invention." *See* Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. 10043, 10046 (Feb. 13, 2024).

44. *See* Mike Brooks, *How AIs Are Artificial Life: Conversations Between Dr. Mike Brooks and ChatGPT 4.0 in March 2023 About Whether AIs Are Artificial Life*, DR. MIKE BROOKS (Mar. 25, 2023), https://www.drmikebrooks.com/how-ais-are-artificial-life/ [https://perma.cc/PFG9-KE44].

has remarkable potential to create new knowledge.[45] In certain areas, AI capabilities already match what humans can do;[46] and the rapid evolution of AI technology suggests that it will exceed human performance in the future.[47]

The discussion below explains how AI can create (1) information with independent economic value that (2) is not generally known or readily ascertainable.[48] The final requirement for trade secret protection—taking reasonable precautions to maintain secrecy—can be satisfied by a variety of methods used to safeguard valuable information in digital form.[49]

AI systems have already produced information that meets the criteria for trade secret protection. The quality and quantity of this information will grow over time as these systems become more sophisticated. Yet it seems likely that many system users have not considered whether such information qualifies for legal protection. To date, no one has filed a lawsuit for misappropriation of an AI-generated trade secret.

2. Information with "Independent Economic Value"

The economic value test is relatively easy to meet. As the Restatement (Third) of Unfair Competition explains, the information must provide an "advantage" over others "that is more than trivial."[50] In *U.S. West Communication, Inc. v. Office of Consumer Advocate*, the Iowa Supreme Court offered a more functional definition: information "that would be useful to a competitor and require cost, time and effort to duplicate."[51]

Traditional AI systems were developed to perform a particular function using a specialized database, and they have been able to create valuable

45. *See* Madhan Jeyaraman et al., *ChatGPT in Action: Harnessing Artificial Intelligence Potential and Addressing Ethical Challenges in Medicine, Education, and Scientific Research*, 13 WORLD J. METHODOLOGY 170, 171 (2023).

46. Nicola Jones, *AI Now Beats Humans at Basic Tasks – New Benchmarks Are Needed, Says Major Report*, NATURE (Apr. 15, 2024), https://www.nature.com/articles/d41586-024-01087-4 [https://perma.cc/FE6U-9Y5S].

47. *See* Janna Anderson & Lee Rainie, *Artificial Intelligence and the Future of Humans*, PEW RSCH. CTR. (Dec. 10, 2018), https://www.pewresearch.org/internet/2018/12/10/artificial-intelligence-and-the-future-of-humans/ [https://perma.cc/S5P7-EUCW] (explaining that many experts believe AI will exceed human intelligence and capabilities in various complex tasks).

48. *See infra* Sections II.A.2-3.

49. These could include data encryption, security protocols for system access, employee nondisclosure agreements, and various physical security methods. *See* JOHN G. SPRANKLING & THOMAS G. SPRANKLING, UNDERSTANDING TRADE SECRET LAW 46 (2020); discussion *infra* Section III.C.

50. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. e (AM. L. INST. 1995).

51. 498 N.W.2d 711, 714 (Iowa 1993).

information for some time.[52] This category of information can be described as "AI-assisted," rather than "AI-generated."[53] For example, one AI strength is the ability to predict future events, such as weather forecasts. The Pangu-Weather AI system can predict weather "thousands of times faster and cheaper" than traditional approaches with the same degree of accuracy.[54] While such information is not patentable, it easily qualifies for trade secret protection.

Another AI-assisted capability is searching through huge accumulations of data to discover new medicines. MIT scientists have used AI to survey 61,000 molecules in order to discover a new antibiotic—halicin.[55] The program "detected new molecular qualities—relationships between aspects of their structure and their antibiotic capacity that humans had neither perceived nor defined."[56] It would have been "prohibitively expensive" for humans to conduct such research.[57] Similarly, scientists at Google DeepMind developed a system that uses "existing libraries of chemical structures to predict new ones."[58] Previously, only 48,000 types of crystals were known; but the system predicted 2.2 million new ones, many of which have now been synthesized.[59] Some of these new crystals could facilitate superconductivity, while others

52. *See* Orly Lobel, *The Law of AI for Good*, 75 FLA. L. REV. 1073, 1093–1107 (2023) (describing how AI can generate valuable information for environmental and climate protection, food scarcity and poverty alleviation, health and medicine, accommodations for disabilities, education, agency compliance, and law enforcement).

53. *See* JOSEF DREXL ET AL., MAX PLANCK INST. FOR INNOVATION AND COMPETITION, COMMENTS ON THE DRAFT ISSUES PAPER OF THE WORLD INTELLECTUAL PROPERTY ORGANIZATION ON INTELLECTUAL PROPERTY POLICY & ARTIFICIAL INTELLIGENCE 2 (2020), https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/2020-02-11_WIPO_AI_Draft_Issue_Paper__Comments_Max_Planck.pdf [https://perma.cc/XJ33-3SBE].

54. *How Scientists Are Using Artificial Intelligence*, THE ECONOMIST (Sept. 13, 2023), https://www.economist.com/science-and-technology/2023/09/13/how-scientists-are-using-artificial-intelligence [https://perma.cc/62UK-AWE7].

55. KISSINGER, *supra* note 28, at 9.

56. *Id*. at 11.

57. *Id*. at 10. Knowing what not to do in research can also be valuable information. As a comment to the UTSA explains, the Act protects "information that has commercial value from a negative viewpoint, for example the results of lengthy and expensive research which proves that a certain process will *not* work could be of great value to a competitor." UTSA, *supra* note 11, § 1 cmt. (emphasis in original). For instance, a Microsoft team used AI to screen 32.6 million potential materials for new batteries, including some not existing in nature, in only eighty hours, a process that previously "would have taken 20 years." Mark Johnson, *New Battery Material That Uses Less Lithium Found in AI-Powered Search*, WASH. POST (Jan. 9, 2024, 1:09 PM), https://www.washingtonpost.com/science/2024/01/09/microsoft-ai-battery-lithium/ [https://perma.cc/H24H-F2GM]. The search produced a list of the 120-130 strongest candidates, which will be studied in detail, thereby saving money and time. *Id*.

58. *A Google AI Has Discovered 2.2m Materials Unknown to Science*, THE ECONOMIST (Nov. 29, 2023), https://www.economist.com/science-and-technology/2023/11/29/a-google-ai-has-discovered-22m-materials-unknown-to-science [https://perma.cc/5BNU-AXMJ].

59. *Id.*

might serve as lithium ion conductors for batteries—both examples of potential economic value. But none of the crystals are patentable.[60]

Generative AI expands the complexity and range of information that can qualify for trade secret protection with little or no human input. It can write computer code, compile customer lists, develop marketing approaches, and create recipes—all of which have potential economic value.[61] But it can also develop information that is significantly more valuable.

For example, generative AI is already "transforming nearly all aspects of the pharmaceutical industry."[62] It is predicted to save $60 billion or more each year by speeding up the identification of materials for potential new drugs, the process for developing them, and other steps.[63] It can also detect various health conditions, including skin cancer, lung cancer, bone fractures, and Alzheimer's disease.[64] An AI physician's assistant can "give status updates, recommend care options, and answer doctors' questions."[65] Moreover, advanced AI can analyze various types of data to predict the outbreak of infectious diseases by locating abnormal patterns, thus alerting medical professionals to the likelihood that outbreaks will occur.[66]

Another strength of generative AI is creating innovative business strategies. For example, it might "assist an organization's strategy formation by responding to prompts requesting alternative ideas and scenarios from the

60. Physical phenomena cannot be patented. For example, as the Supreme Court noted in *Diamond v. Chakrabarty*, "a new mineral discovered in the earth . . . is not patentable subject matter." 447 U.S. 303, 309 (1980).

61. *See generally* SOC'Y OF HUM. RES. MGMT. & BURNING GLASS INST., GENERATIVE ARTIFICIAL INTELLIGENCE AND THE WORKFORCE 15, https://www.shrm.org/topics-tools/topics/artificial-intelligence-in-the-workplace#sortCriteria=relevancy%2C%40ytlikecount%20descending&f-topicfiltertag=Artificial%20Intelligence [https://perma.cc/5MEA-BPGR] (discussing the roles generative AI plays in different occupational sectors); Kweilin Ellingrud et al., *Generative AI and the Future of Work in America*, MCKINSEY GLOBAL INS. (July 26, 2023), https://www.mckinsey.com/mgi/our-research/generative-ai-and-the-future-of-work-in-america [https://perma.cc/Y2FY-6XAE].

62. BHAVIK SHAH ET AL., MCKINSEY & CO., GENERATIVE AI IN THE PHARMACEUTICAL INDUSTRY: MOVING FROM HYPE TO REALITY (2024), https://www.mckinsey.com/industries/life-sciences/our-insights/generative-ai-in-the-pharmaceutical-industry-moving-from-hype-to-reality [https://perma.cc/CG2K-FY37].

63. *See id.*

64. Nadeida Alkhaldi, *5 Ways to Use Generative AI in Healthcare*, ITREX BLOG (Sept. 6, 2023), https://itrexgroup.com/blog/top-generative-ai-in-healthcare-use-cases/ [https://perma.cc/PL96-2QAD]. *See generally* Fazal Khan, *Regulating the Revolution: A Legal Road Map for Optimizing AI in Healthcare*, 25 MINN. J.L. SCI. & TECH. 49, 55–57 (2023) (discussing how AI can be used in healthcare systems).

65. Alkhaldi*, supra* note 64.

66. *See* Jagreet Kaul Gill, *Generative AI in Healthcare System and its Uses*: *Complete Guide*, XENONSTACK BLOG (Dec. 13, 2023), https://www.xenonstack.com/blog/generative-ai-healthcare-system [https://perma.cc/FKS3-4GLW].

managers of a business in the midst of an industry disruption."[67] Or it could help a company by creating new products.[68] The Coca-Cola Company used generative AI to develop a new Coke flavor by collecting data from existing customers and analyzing what novel combination of ingredients would appeal to them.[69]

Generative AI can also reduce the time and expense required to build homes and other structures.[70] It automates the process of designing new structures, taking into account criteria such as cost, energy conservation, and structural integrity.[71] It can also develop detailed plans for each phase of the construction process and monitor the quality of ongoing work.[72]

Finally, advanced AI systems may be able to create patentable inventions.[73] For example, Stephen Thaler asserts that his system, "Device for the Autonomous Bootstrapping of Unified Science" ("DABUS"), created two patentable inventions—a "Neural Flame" and a "Fractal Container"—by itself.[74] He states that the container was "entirely the creation of an A.I. system without human control" which "had no training in computer design, and . . . was not asked to make one."[75] The container uses "fractal geometry to improve heat transfer, a kind of anti-Thermos."[76] Such inventions, if kept

67. Pavlik, *supra* note 29.

68. *See How Generative AI Is Reshaping Product Development*, SALSIFY (Oct. 31, 2023), https://www.salsify.com/blog/generative-ai-reshaping-product-development [https://perma.cc/57V2-EXNR]; *see also Generative AI: What Is It, Tools Models, Applications, and Use Cases*, GARTNER, https://www.gartner.com/en/topics/generative-ai [https://perma.cc/N4UU-TCX2] ("In the manufacturing, automotive, aerospace and defense industries, generative design can create designs optimized to meet specific goals and constraints, such as performance, materials and manufacturing methods. This accelerates the design process by producing an array of potential solutions for engineers to explore.").

69. SALSIFY, *How Generative AI Is Reshaping Product Development*, *supra* note 68.

70. *See* Patrick Murphy, *The Role of Generative AI in Reducing the Time and Cost of Building Design and Construction*, MAKET, https://www.maket.ai/post/the-role-of-generative-ai-in-reducing-the-time-and-cost-of-building-design-and-construction [https://perma.cc/DQ6V-SMFG].

71. *Id.*

72. *Id.*

73. *See* Ryan Abbott, *I Think, Therefore I Invent: Creative Computers and the Future of Patent Law*, 57 B.C. L. REV. 1079, 1083–91 (2016) (discussing cases where machines have autonomously created patentable creations); *see also* Trevor F. Ward, *DABUS, An Artificial Intelligence Machine, Invented Something New and Useful, But the USPTO Is Not Buying It,* 75 ME. L. REV. 71, 79–82 (2023) (describing scenarios where AI has created inventions).

74. Thaler v. Vidal, 43 F.4th 1207, 1209 (Fed. Cir. 2022), *cert. denied*, 143 S. Ct. 1783 (2023).

75. Steve Lohr, *Can A.I. Invent?*, N.Y. TIMES (July 15, 2023), https://www.nytimes.com/2023/07/15/technology/ai-inventor-patents.html [https://perma.cc/A8GS-C2SQ].

76. *Id.*

secret, would certainly have enough potential value to qualify for trade secret protection.[77]

3. Information that Is Not "Generally Known" or "Readily Ascertainable"

To qualify for trade secret protection, information must derive value "from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use."[78] Under this approach, the relevant group is people who can obtain value from the information—most commonly competitors—rather than the public at large. The rationale for this requirement is straightforward: the purpose of trade secret protection is to encourage innovation.[79] There is no reason to provide legal protection for information that is known or easily knowable. The "generally known" prong of this requirement is straightforward, as it concerns what people actually know. But the scope of the "readily ascertainable" prong is less clear today since it will presumably encompass what AI could discover. If an AI system generates valuable information, would it be "readily ascertainable" by other AI systems and hence not a trade secret?

Neither the UTSA nor the DTSA defines the term "readily ascertainable."[80] The UTSA offers the unhelpful comment that "[i]nformation is readily ascertainable if it is available in trade journals, reference books, or published materials."[81] Most courts seem to agree that the question turns on the "degree of time, effort, and expense required of a defendant to acquire or reproduce the alleged trade secret information."[82] For example, in *DVD Copy Control Association, Inc. v. Bunner*, a California appellate court noted that even placing a trade secret on the internet would not make it readily ascertainable if the posting was "sufficiently obscure or transient or otherwise

77. In the long run, advanced AI could vastly exceed human abilities to create new inventions. "[P]ick any task, like designing a new advanced airplane or weapon system, and superintelligent AI could do this in about a second." Tamlyn Hunt, *Here's Why AI May Be Extremely Dangerous–Whether It's Conscious or Not*, SCI. AM. (May 25, 2023), https://www.scientificamerican.com/article/heres-why-ai-may-be-extremely-dangerous-whether-its-conscious-or-not/ [https://perma.cc/UGG9-BGQ6].

78. UTSA, *supra* note 11, § 1(4)(i); 18 U.S.C. § 1839(3)(B).

79. *See* JOHN R. THOMAS, CONG. RSCH. SERV., R41391, THE ROLE OF TRADE SECRETS IN INNOVATION POLICY (Jan. 15, 2014), https://sgp.fas.org/crs/secrecy/R41391.pdf [https://perma.cc/HL6T-HP79].

80. *See* 18 U.S.C. § 1839(3)(B); UTSA, *supra* note 11, § 1 cmt. (providing examples of situations where information is readily ascertainable).

81. UTSA, *supra* note 11, § 1 cmt.

82. *See, e.g.*, Amoco Prod. Co. v. Laird, 662 N.E.2d 912, 918 (Ind. 1993).

limited so that it does not become generally known to . . . persons to whom the information would have some economic value."[83]

As these authorities reflect, the parameters of the "readily ascertainable" test are based on human abilities.[84] For example, a human could be expected to read articles in relevant trade journals, but not to undertake an exhaustive internet search. Yet it seems inevitable that in the future the scope of readily ascertainable information will be based on the capacity of AI, not humans.[85] An AI program with full access to the internet would be much more effective than a human in discovering a trade secret with minimal time or effort.[86]

The Restatement (Third) of Unfair Competition notes that "the theoretical possibility of reconstructing the secret from published materials containing scattered references to portions of the information" does not make a trade secret readily ascertainable.[87] This principle makes sense based on human abilities; a person would have to devote substantial time, expense, and effort to piece together the information that constitutes the secret. In contrast, if an AI system can piece together enough references in published sources to create new and valuable information, another AI system might be able to discover the same secret.

Consider customer lists. In *Fireworks Spectacular, Inc. v. Premier Pyrotechnics, Inc*., the court concluded that the identities of possible customers for fireworks were not readily ascertainable, noting that the plaintiffs obtained them through efforts that included "hundreds of hours of 'cold-calling.'"[88] Today it seems probable that AI could quickly create a new customer list for a product or service without hours of phone calls. But a similar AI system with the same training, database, and other characteristics could presumably create the same list if given the same prompt.[89] Thus, if the readily ascertainable standard is based on AI ability, the list is not a trade

83. 10 Cal. Rptr. 3d 185, 192–93 (Cal. App. 2004). *See generally* 1 ROGER M. MILGRIM & ERIC E. BENSON, MILGRIM ON TRADE SECRETS § 1.07A[3] (2024) (discussing judicial interpretations of "readily ascertainable").

84. *See* 1 MILGRIM & BENSON, *supra* note 83, § 1.07A[3]; *see also Amoco Prod. Co*., 622 N.E.2d at 918.

85. There is no reason to protect information which is readily ascertainable by an AI system, even if it would not be readily ascertainable to a human. Any human could simply use an AI system to learn the information.

86. *Cf.* Ryan Abbott, *Everything Is Obvious*, 66 UCLA L. REV. 2, 22–37 (2019) (arguing that ultimately "inventive machines" should become the standard for assessing nonobviousness in patent law, rather than the current standard of a human who is skilled in the particular art).

87. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (AM. L. INST. 1995).

88. 147 F. Supp. 2d 1057, 1066 (D. Kan. 2001).

89. Still, modern AI systems can differ widely from each other in many respects, including hardware, algorithms, network design, software, training data, and training methods. *See supra* text accompanying notes 28-40. It may be difficult to know whether the information is readily ascertainable without exhaustive inquiry.

secret.[90] For the same reason, a wide range of information that could traditionally qualify for trade secret protection—such as certain business methods, cost data, and price data—may not be protected in the AI era, based on the circumstances of the particular case.

The shift to an AI-based test for readily ascertainable information could create difficult proof problems. Suppose A uses an AI system to develop valuable information. If A later sues B for misappropriation, A would have to prove that the information qualifies for trade secret protection; as part of this burden, A must establish that the information is not readily ascertainable by others.[91] Traditionally, the plaintiff could satisfy this burden through evidence showing that it took substantial time and expense to develop the information, and, accordingly prove that duplicating the information would be equally difficult.[92] But if the plaintiff used AI to generate the trade secret, it must show that another person would have difficulty using AI to learn the same information.

Many AI systems are proprietary and hence not available for use by others; the defendant's inability to access the particular system that created the information would be helpful evidence.[93] But, even so, the plaintiff may have to demonstrate that no publicly available system would be able to generate the same information with a similar prompt, which may be a difficult burden. If the plaintiff used a public system in obtaining the information, it could attempt to show that a particularly complex prompt was necessary.[94]

---

90. Alternatively, suppose an AI system develops a trade secret which is not reasonably ascertainable, but a second AI system later discovers the same information through its independent effort. In this scenario, the trade secret still exists.

91. *See* UTSA, *supra* note 11, § 1(4)(i); 18 U.S.C. § 1839(3)(B).

92. *See, e.g.*, *Fireworks Spectacular*, 147 F. Supp. 2d at 1066.

93. Some modern AI systems are open to the public, typically on a fee basis. Google, OpenAI, Amazon, IBM and others have United States-based systems that can be accessed by the public. *See supra* text accompanying notes 29-30. Systems are also emerging in Abu Dhabi, Britain, China, France, Germany, India, Saudi Arabia and other countries. *See Welcome to the Era of AI Nationalism*, THE ECONOMIST (Jan. 1, 2024), https://www.economist.com/business/2024/01/01/welcome-to-the-era-of-ai-nationalism [https://perma.cc/KP4J-GRQF].

94. Guidance from the PTO on what constitutes a "significant contribution" by a human to an AI-assisted invention may be useful here by analogy. *See* Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. 10043, 10047–48 (Feb. 13, 2024). For example, the PTO concludes that a nineteen-word prompt which directs an AI system to create a "transaxle for a model car" would not be a sufficient human contribution to justify a patent. *See* EXAMPLE 1: TRANSAXLE FOR REMOTE CONTROL CAR, U.S. PAT. AND TRADEMARK OFF., https://www.uspto.gov/sites/default/files/documents/ai-inventorship-guidance-mechanical.pdf [https://perma.cc/8XQ4-ULVJ]. Simlarly, a very short prompt will almost certainly obtain information that is readily ascertainable and thus is not a trade secret. On the other hand, even a prompt that falls short of constituting a significant human contribution for purposes of patentability may generate information that is not readily ascertainable, which can be protected as a trade secret.

For example, ChatGPT-4 can accept a prompt of up to 25,000 words.[95] It is highly unlikely that anyone would later duplicate such a detailed prompt.

B. Protection for AI-Generated Trade Secrets?

1. Patent and Copyright Models

Should an invention or other work created by AI qualify for intellectual property protection? The issue has sparked widespread debate in the realms of patent law and copyright law.[96] In contrast, the question of whether valuable information generated by AI should be protected by trade secret law has been ignored.

The Patent Act and the Copyright Act are based on the Intellectual Property Clause of the Constitution, which authorizes Congress to secure "to authors and inventors the exclusive right to their respective writings and discoveries" in order to serve an expressly utilitarian purpose: "[t]o promote the progress of science and useful arts."[97] In the era when the Constitution was adopted, of course, only humans had the capacity to create inventions or works of authorship and, accordingly, the Framers intended the Clause to incentivize human creativity.

Under current law, inventions and works of authorship generated solely by AI do not qualify for patent or copyright protection.[98] This conclusion is

95. Hughes, *supra* note 30.

96. The issue has surfaced in the patent and copyright contexts because both require some form of administrative approval which requires that the creator be identified. A patent arises only when it is issued by the PTO. *See About Us*, U.S. PAT. & TRADEMARK OFF., https://www.uspto.gov/about-us [https://perma.cc/6UCE-5WJQ]. While a copyright exists without government action, it can only be enforced in litigation if it is registered with the Copyright Office. 17 U.S.C. § 411(a). But a trade secret arises without any government action. As a result, the question of whether AI-created information qualifies for protection will probably arise in future litigation—a defendant in a misappropriation action might contend that the information is not a trade secret because a non-human created it.

97. U.S. CONST. art. I, § 8, cl. 8. Patent law and trade secret law both protect the content of ideas; in contrast, copyright law only protects the manner in which ideas are expressed. 17 U.S.C. § 102(b) ("In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery . . . .").

98. *But see* Tim W. Dornis, *Artificial Intelligence and Innovation: The End of Patent Law as We Know It*, 23 YALE J.L. & TECH. 97, 114 (2020) (arguing that AI-generated inventions should be patentable); Haochen Sun, *Artificial Intelligence Inventions*, 50 FLA. ST. U. L. REV. 61, 78 (2022) (same).

primarily based on textual analysis of the relevant federal statutes, without consideration of policy issues.[99]

The landmark decision in *Thaler v. Vidal* held that DABUS, plaintiff Stephen Thaler's AI-system, could not qualify as an inventor on patent applications.[100] Because the text of the Patent Act provides that an inventor is an "individual"[101]—which the Supreme Court has defined as "a human being"[102]—the Federal Circuit concluded that only a human could be an "inventor" under the Act.[103] This is consistent with the traditional rule that a corporation or other legal entity cannot be an inventor under the Act.[104]

In February 2024, the Patent and Trademark Office ("PTO") supplemented *Thaler* by issuing its Inventorship Guidance for AI-Assisted Inventions.[105] The Guidance provides that an AI-assisted invention is patentable if a human made a "significant contribution" to the invention[106] by analogy to the rules for joint inventors set forth in *Pannu v. Iolab Corp*.;[107]

---

99. *See, e.g.*, Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. at 10046–47 (reaching the conclusion, relying primarily on statutory interpretation, that a human must significantly contribute to an invention by AI for it to be patentable); *see also* Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence, 88 Fed. Reg. 16190, 16191 (Mar. 16, 2023) (to be codified at 37 C.F.R. pt. 202); Thaler v. Vidal, 43 F.4th 1207, 1209 (Fed. Cir. 2022), *cert. denied*, 143 S. Ct. 1783 (2023) (concluding that the Patent Act requires an "inventor" to be a natural person).

100. 43 F.4th at 1213.Thaler was later asked why he did not list himself as the inventor, and his response was reported as follows:

> For one thing, Thaler said, he worried that the patents might be unenforceable if they did not list the name of the real inventor. But more importantly, he thought that writing in his own name would have been dishonest—even criminal—if DABUS conceived of the ideas spontaneously, as he maintains. He is stirred by the notion that AIs might achieve equal rights. "I'm a machine," he said. "It's a machine."

Tomas Weber, *The Inventor Who Fell in Love with His Machine*, THE ECONOMIST (Apr. 4, 2023), https://www.economist.com/1843/2023/04/04/the-inventor-who-fell-in-love-with-his-ai [https://perma.cc/9AUL-2228].

101. 35 U.S.C. §§ 100(f)-(g), 115.

102. Mohamad v. Palestinian Auth., 566 U.S. 449, 454 (2012).

103. *Thaler,* 43 F.4th at 1212. The court ignored Thaler's policy arguments on the issue, observing that they "are speculative and lack a basis in the text of the Patent Act and in the record." *Id.* at 1213. However, the court noted that it was "not confronted . . . with the question of whether inventions made by human beings with the *assistance* of AI are eligible for patent protection." *Id*. (emphasis in original).

104. *See* Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. at 10046 n.13.

105. *Id.* at 10043.

106. *Id.* at 10048. The PTO Guidance notes that merely presenting a problem to an AI system might be insufficient but provides that "a significant contribution could be shown by the way the person constructs the prompt in view of a specific problem to elicit a particular solution from the AI system." *Id*. Similarly, "a person who takes the output of an AI system and makes a significant contribution to the output to create an invention may be a proper inventor." *Id.*

107. 155 F.3d 1344, 1351 (Fed. Cir. 1998).

this will be decided on a case-by-case basis.[108] Under the PTO approach, an AI system is viewed as a "tool,"[109] even if it was "instrumental in the creation of the invention."[110] The Guidance stresses that "[t]he patent system is designed to encourage *human* ingenuity."[111] Thus, an invention generated by AI with little or no human involvement cannot be patented.

Moreover, because the PTO will assess the patentability of an AI-assisted work on a "case-by-case basis,"[112] an inventor who is uncertain about how the PTO will decide might opt for trade secret protection instead, if it is available. Otherwise, she runs the risk that (1) publication of the patent application will bar trade secret protection because the information is now generally known and (2) the PTO will later deny the application.[113]

Similarly, the Copyright Office takes the position that under the Copyright Act only a work of authorship created by a human qualifies for copyright registration.[114] Its 2023 Copyright Registration Guidance states that copyright "can protect only material that is the product of human creativity" because "the term 'author' . . . in both the Constitution and the Copyright Act . . . excludes non-humans."[115] The question is whether the work "is basically one of human authorship, with the [AI system] merely being an assisting instrument, or whether the traditional elements of authorship in the work . . . were actually conceived and executed not by man but by a machine."[116]

108. "When applying the *Pannu* factors to determine whether natural persons significantly contributed to an AI-assisted invention, one must remember this determination is made on a claim-by-claim and case-by-case basis, and each instance must turn on its own facts." Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. at 10048.

109. *See id.* at 10046.

110. *Id.*

111. *Id.* (emphasis added).

112. *Id.* at 10048.

113. Most patent applications are published eighteen months after they are filed. MENELL, *supra* note 12, at 76. But it typically takes approximately three years for the PTO to decide whether the patent should issue. *See id.*

114. However, the Copyright Act provides that the copyright in a human-created "work made for hire" can initially vest in a corporation or other entity under some circumstances. 17 U.S.C. § 201(b).

115. Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence, 88 Fed. Reg. 16190, 16191 (Mar. 16, 2023) (to be codified at 37 C.F.R. pt. 202).

116. *Id*. at 16192. For example, the Guidance notes that where "AI technology receives solely a prompt from a human and produces complex written, visual, or musical works in response, the 'traditional elements of authorship' are determined and executed by the technology—not the human user." *Id*.

2. Proposed Approach for Trade Secrets

AI-generated information should be protected as trade secrets. Trade secret law differs from the patent and copyright regimes in two key aspects. First, the UTSA and DTSA do not expressly limit protection to human creations,[117] unlike the Patent Act and the Copyright Act.[118] Second, the trade secret statutes are not constrained by the human-incentive policy that underlies the Intellectual Property Clause; the UTSA is embodied in state law, while the DTSA is authorized under the Interstate Commerce Clause.[119]

An enforceable trade secret arises without any government approval or registration—unlike a patent or copyright.[120] Nothing in the text of the UTSA or DTSA restricts the identity of the actor who may permissibly develop a trade secret.[121] As a result, there is no statutory basis for concluding that an AI-generated secret would not qualify for protection.

From a policy perspective, it makes sense to protect AI-generated trade secrets. The main policy underlying trade secret protection is to encourage innovation for the benefit of society in general.[122] People are incentivized to develop trade secrets, at least in part, because the law enables them to reap economic benefits from the exclusive right to use the information.[123] Admittedly, an AI system that develops trade secrets with little or no human involvement would not need a legal incentive to do so. But trade secret protection will incentivize humans to facilitate the development and use of such valuable information. First, it will encourage businesses and entrepreneurs to invest in advancing AI technology. Second, it would incentivize them to use and operate AI systems to develop trade secrets. Finally, it will lead them to invest in the commercial use of such secrets. While AI may generate trade secrets, society will not benefit from them unless humans facilitate their use.

---

117. *See* UTSA, *supra* note 11, § 1; 18 U.S.C. § 1839.

118. *See supra* notes 98-111, 114-116 and accompanying text.

119. *See* 18 U.S.C. § 1832(a) (making theft of a trade secret illegal when the secret is "related to a product or service used in or intended for use in interstate or foreign commerce"); 18 U.S.C. § 1836(b)(1) (creating a civil cause of action for trade secret misappropriation when the secret is "related to a product or service used in, or intended for use in, interstate or foreign commerce"); *see also* U.S. CONST. art. I, § 8, cl. 2 ("The Congress shall have power . . . [t]o regulate commerce with foreign nations, and among the several states, and with the Indian tribes. . . ."). *See generally* UTSA, *supra* note 11, at Pref. Note (stressing the need for states to adopt the Act to bring more uniformity to state trade secret law).

120. *See* TLS Mgmt. & Mktg. Servs., LLC v. Rodríguez-Toledo, 966 F.3d 46, 51–52 (1st Cir. 2020).

121. *See* UTSA, *supra* note 11; 18 U.S.C. § 1839.

122. *See supra* note 17 and accompanying text.

123. *See Trade Secrets / Regulatory Data Protection*, U.S. PAT. & TRADEMARK OFF., https://www.uspto.gov/ip-policy/trade-secret-policy [https://perma.cc/K2U7-5S2S].

It might be argued that society would benefit if AI-generated trade secrets fell into the public domain, so that anyone could use them freely.[124] But it seems unlikely that an AI system would be programmed to publicize valuable information. Nor would the humans associated with the system have any incentive to do so. Even if the information were somehow disclosed to the public, the lack of legal protection might discourage anyone from making the investments necessary to utilize it.[125]

The protection of AI-generated secrets will probably tend to favor large entities who can afford to invest in AI technology, and thus gain a competitive advantage over smaller rivals.[126] Before the AI era, larger companies were typically better able to finance expensive human-conducted research. Yet technology might level the playing field to some extent. It is possible that smaller firms may be able to deploy innovative AI technology to discover new information without the need to pay teams of human researchers.

The policy option of denying protection to AI-generated secrets would be unworkable. Unlike patents and copyrights, a trade secret is enforceable without any form of government approval or registration;[127] thus, there is no administrative forum that has the capacity to determine the origin of the secret.[128] Further, there is no objective method for an official to determine whether a trade secret was created by a human or by AI. A secret is simply information, without any reliable lineage. If the law only protected human-created secrets, humans with access to AI-generated secrets could easily misrepresent their origin.[129]

---

124. *Cf.* Haochen Sun, *Redesigning Copyright Protection in the Era of Artificial Intelligence*, 107 IOWA L. REV. 1213, 1249–51 (2022) (arguing that works of authorship generated by AI should enter the public domain rather than receive copyright protection).

125. However, it is possible that at some point in the future an advanced AI system might be entirely autonomous, operating without any human control or involvement. In that situation, the argument that AI-generated trade secrets should enter the public domain has greater force, though it is not clear how humans could obtain access to such secrets or even know that they exist.

126. The development of advanced AI models is extremely expensive; the hardware alone may cost $100 million. Pavlik, *supra* note 29.

127. *See supra* note 120 and accompanying text.

128. For the same reason, the option of recognizing AI-generated trade secrets but affording them less protection than human-created secrets (e.g., employing a more rigorous standard or limiting protection to a fixed period) is not practicable.

129. This concern also potentially applies to AI-assisted patents and copyrights. The PTO "presumes" that the human inventor listed on the patent application for an AI-assisted invention is "the actual inventor," but advises that the patent examiner "should carefully evaluate the facts from the file record or other extrinsic evidence when making determinations on inventorship." Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. 10043, 10048 (Feb. 13, 2024). The Copyright Office similarly relies on information presented by the applicant. Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence, 88 Fed. Reg. 16190, 16193 (Mar. 16, 2023) (to be codified at 37 C.F.R. pt. 202).

Much of the controversy surrounding the status of AI-generated patents and copyrights stems from exclusivity. In general, the person who creates a patented invention or original artistic work receives a legal monopoly which allows her to exclude others from using it for a particular period of time.[130] In authorizing patents for AI-assisted inventions, for example, the PTO focused on the exclusivity concern; it stressed the importance that the patent system strike "the right balance between protecting and incentivizing AI-assisted inventions and not hindering future human innovation by locking up innovation created without human ingenuity."[131]

In contrast, many people can own and utilize the same trade secret. Extending protection to an AI-generated secret does not preclude humans from discovering the information through independent creation, reverse engineering, or other proper means.[132] Nor does it "hinder future innovation by locking up innovation created without human ingenuity."[133] Anyone who legally learns the information is free to use it. Thus, the central policy concern for prohibiting patents and copyrights on AI-generated material does not apply to trade secrets.

C. Ownership of AI-Generated Trade Secrets

1. Ownership by AI?

Could an AI system own a trade secret it created? It is clear that such a system could not own a patent or a copyright.[134] Trade secret law would probably lead to the same conclusion.

The statutory regimes for ownership of patents and copyrights are straightforward. In general, a human who creates a patentable invention or a copyrightable work owns the property, based on a statute or contract.[135] Under the Patent Act, a patent is awarded to the first inventor to file a patent application; and "inventor" is defined to be an "individual," that is, a human.[136] But most inventions are created by employees in the course of their employment.[137] At common law, title to such an invention vested in the

130. *See supra* notes 18-20 and accompanying text.
131. Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. at 10047.
132. *See infra* text accompanying notes 201-202.
133. Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. at 10047.
134. *See infra* notes 135-141 and accompanying text.
135. *See* 35 U.S.C. § 261; 17 U.S.C. § 201(a).
136. 35 U.S.C. §§ 100(f), 115(a); *see supra* text accompanying notes 97-104.
137. Ingersoll-Rand Co. v. Ciavatta, 542 A.2d 879, 886 (N.J. 1988) (noting that "80% to 90% of all inventions in the United States are made by employed inventors").

employer when the employee was hired to invent;[138] today employees in many companies are required to sign assignment agreements by which they transfer any ownership rights to the employer.[139] Similarly, as a general rule the Copyright Act specifies that ownership of a copyright usually vests in the human author;[140] however, under some circumstances the Act provides that the copyright is owned by an employer or someone who commissions a particular "work made for hire."[141] There is no serious argument that an AI system could ever be the owner of a patent or copyright, even if it created the underlying work or invention.

In contrast, the law governing ownership of trade secrets is underdeveloped, in part due to historic disagreement about the theoretical basis for legal protection.[142] The doctrine was originally based on tort theory; under this view it functioned to deter wrongful conduct and thus ensure commercial morality, not to protect property rights.[143] But the adoption of the UTSA by state legislatures signaled a shift toward the property approach, in part because comments refer to an "owner" of the trade secret.[144] In contrast, the DTSA explicitly endorses the property approach.[145]

In general, ownership of a trade secret is obtained by (1) creating information that meets the statutory criteria for protection or (2) acquiring an existing secret by proper means.[146] The UTSA contemplates that a trade secret

---

138. *See* MENELL, *supra* note 12, at 120 (explaining that inventions made by employees who were "hired to invent" belonged to the employer at common law).

139. *Id.* at 121.

140. 17 U.S.C. § 201(a).

141. *Id.* § 201(b).

142. *See* MILGRIM, *supra* note 83, § 2.01; *see also* Lemley, *supra* note 9, at 324–26 (discussing different theories for trade secret protection).

143. *See* RESTATEMENT OF TORTS § 757 cmt. a (AM. L. INST. 1939) ("The suggestion that one has a right to exclude others from the use of his trade secret because he has a right of property in the idea has been frequently advanced and rejected. The theory that has prevailed is that the protection is *afforded only by a general duty of good faith* and that the liability rests upon a breach of this duty. . . ."") (emphasis added); *see also infra* notes 210-212 and accompanying text. Even the modern Restatement (Third) of Unfair Competition avoids classifying a trade secret as "property," referring to it only as an "intangible trade value." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 (AM. L. INST. 1995).

144. UTSA, *supra* note 11, §§ 1 cmt., 2 cmt.; *see also id.* § 1(2)(i) (referring to "acquisition of a trade secret *of another* [person] by a person . . . .") (emphasis added).

145. *See* 18 U.S.C. § 1839(4) (defining the "owner" of a trade secret).

146. *See* DTM Rsch., LLC v. AT&T Corp., 245 F.3d 327, 331 (4th Cir. 2001) (holding that a plaintiff in a trade secret misappropriation case "must show either that it developed the trade secret at issue or otherwise is in lawful possession of it"); *see also* SPRANKLING ET AL., *supra* note 49, at 16 ("Most commonly, a person obtains ownership of a trade secret by creating it."); UTSA, *supra* note 11, § 1 cmt. (noting that an existing trade secret can be legally obtained by another who uses "proper means" to do so).

will be owned by a "person."[147] In turn, "person" is broadly defined to mean "a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity."[148] Similarly, the DTSA defines the "owner" of a trade secret as "the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed."[149] Arguably, an AI system might be viewed as an "entity" under these definitions.

Nothing in the text of the UTSA or DTSA specifies that the creator of a trade secret must be a human.[150] Yet as a policy matter it cannot be seriously argued that an AI system could own a trade secret.[151] Such a system is not a legal entity that has the power to own, use, or transfer property. It would be unable to use a trade secret in a productive manner or license it for use by others.[152] It could not take the precautions needed to maintain the secrecy of the information. Nor would it have standing to sue if the secret were misappropriated.[153] Thus, the information would be legally protected, but humans would receive no benefit from it—contrary to the innovation policy that underlies trade secret law.[154] Finally, if an AI invention causes any form of legally-recognized harm, it is important that a human or other recognized legal actor be available to bear responsibility for the loss.[155]

---

147. *See* UTSA, *supra* note 11, § 1(2)(i) (defining "misappropriation" to include the "acquisition of a trade secret of *another* [*person*] by a person . . .") (emphasis added); *id.* § 1(4)(i) (defining "trade secret" as, *inter alia*, information which "derives independent economic value[] . . . from not being . . . readily ascertainable by proper means by, *other persons* who can obtain economic value from its disclosure or use") (emphasis added).

148. *Id.* § 1(3).

149. 18 U.S.C § 1839(4).

150. Both statutes were adopted long before advanced AI systems were developed. *See supra* text accompanying notes 11-14.

151. *See generally* Nadia Banteka, *Artificially Intelligent Persons*, 58 HOUS. L. REV. 537 (2021) (arguing that AI systems should not have legal personhood).

152. It is possible, of course, that at some point in the distant future a fully autonomous AI entity might be deemed sufficiently human-like to obtain the legal rights of a human.

153. *See generally* Robayet Syed, *So Sue Me: Who Should be Held Liable When AI Makes Mistakes?*, MONASH UNIV.: LENS (Mar. 29, 2023), https://lens.monash.edu/@politics-society/2023/03/29/1385545/so-sue-me-wholl-be-held-liable-when-ai-makes-mistakes [https://perma.cc/JHU8-3NKL] (discussing the complexities that arise when attempting to hold an AI system and its human creators legally accountable).

154. *See* THOMAS, *supra* note 79, at 2–4.

155. Notably, although Stephen Thaler sought to have his DABUS system listed on patents as the inventor, he conceded in a petition filed with the PTO that current law holds an AI system could not own property. *In re* Application No. 16/524,350, 2020 Dec. Comm'r Pat. 2 n.2, https://www.uspto.gov/sites/default/files/documents/16524350_22apr2020.pdf [https://perma.cc/JJ49-SPPK].

2. Ownership by Humans

Since an AI system cannot own a trade secret it created, the next question is who would own it. Based on the analysis above, the owner must be an actor with the ability to control and utilize the secret, presumably either a human or a human-owned entity such as a corporation or partnership.

Suppose corporation C owns and controls a proprietary AI system, which is used only by its officers and employees. In this situation, it makes sense to vest ownership of the resulting trade secrets in the corporation. The corporation owned the system, and its employees controlled the system to generate the information.[156] The copyright concept of "work made for hire" is a helpful model here.[157] While ownership of a copyright normally vests in the human who creates the work of authorship, under this doctrine title to a work created by an employee vests in the employer.[158]

The issue is more complex where one actor owns the AI system but permits another to use it, resulting in discovery of the secret. In this situation, the question of ownership could be resolved by licensing terms. D, the system owner, could license its use to E, the operator, on condition either that D own any resulting trade secrets or that ownership is divided between them. But such a license term may not be viable in the marketplace for AI services. AI users can choose among a variety of different publicly available systems,[159] and it seems likely that a broader array of systems will be accessible in the future.[160] An AI system owner that demanded an ownership interest in user-produced trade secrets would be at a competitive disadvantage. Moreover, as a practical matter, it would be difficult—but not impossible—for an AI system owner to determine if a user had created a trade secret by using its system.

Absent a contract solution, one approach could be to recognize the system owner and the system user as joint owners of the trade secret, by analogy to patent and copyright law. Two or more people can be recognized as joint inventors through working together on a problem even if their contributions

156. For example, Thaler asserted that he owned the inventions DABUS created because he owned and used the system. Corrected Opening Brief for Plaintiff-Appellant Stephen Thaler at 26–27, Thaler v. Hirshfeld, 558 F. Supp. 3d 238 (E.D. Va. 2021) (No. 2021-2347) (asserting that "as the developer, user, and owner of DABUS," Thaler "is entitled to own DABUS' output" and accordingly "owned the Neural Flame and Fractal Container as trade secrets prior to publication of the [patent] applications").

157. 17 U.S.C. § 201(b).

158. *Id.*

159. *See supra* note 30 and accompanying text.

160. *See* ION STOICA ET AL., A BERKELEY VIEW OF SYSTEMS CHALLENGES FOR AI § 3 (2017).

to developing the invention are quite different.[161] Copyright law similarly recognizes joint authorship under some circumstances.[162] But joint creation of a trade secret is rare. Joint ownership typically arises when one person develops the secret, and another person then reverse engineers or independently invents the same secret.[163] In this situation, the parties are not working together to solve a problem or create a new work, unlike the patent and copyright contexts—indeed, they have no prior relationship at all.[164]

In the AI context, it might be argued that the system owner has contributed by providing the platform, while the user has contributed by using the system to discover the secret. But in this situation, the owner and user are most likely not working together to solve the same problem, unlike the collective efforts that can lead to joint ownership of a patent or copyright. In the case of a major publicly accessible AI system like ChatGPT-4.0, it would be highly unlikely that the owner was even aware that a particular user was operating the system, much less that the user had developed a trade secret. Under these circumstances, there is no practical reason to give the system owner any rights in the secret. Indeed, its failure to impose a license term mandating a share of any trade secret discovery should be viewed as a de facto rejection of the joint ownership approach.

The trade secret goal of encouraging innovation for the benefit of the public is best served by vesting ownership in the system user, who is in the optimal position to license or otherwise use the secret.[165] Under the joint ownership approach, there would always be a chance that the system owner might later demand to share in the resulting profits, which could undercut the user's incentive to exploit the information. Thus, where the system owner's only contribution is to allow use of its publicly available system, ownership of a resulting trade secret should vest in the user.[166] On the other hand, the

---

161. 35 U.S.C. § 116; Burroughs Wellcome Co. v. Barr Labs., Inc., 40 F.3d 1223, 1227 (Fed. Cir. 1994) ("People may be joint inventors even though they do not physically work on the invention together or at the same time, and even though each does not make the same type or amount of contribution.").

162. 17 U.S.C. § 201(a).

163. *See* Don Wiesner & Anita Cava, *Stealing Trade Secrets Ethically*, 47 MD. L. REV 1076, 1119–25 (1989) (discussing situations where a trade secret claimant loses her right to recovery due to independent discovery or reverse engineering).

164. *See, e.g.*, *id*. at 1121 ("For example, a clever detective in a chemist's garment can expose a soft drink formula.").

165. *Cf.* Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. 10043, 10047 (Feb. 13, 2024) (providing that an AI-assisted invention created with a substantial contribution from the system user may qualify for a patent).

166. This approach has been adopted for AI-assisted patents. The PTO Guidance provides that "a person simply owning or overseeing an AI system that is used in the creation of an invention, without providing a similar contribution to the conception of the invention, does not

joint ownership may be appropriate where the system owner has contributed significantly more than merely allowing the use of its system.

IV. THE AI THREAT TO HUMAN-CREATED TRADE SECRETS

A. Three Challenges

The doctrines that limit the scope of trade secret protection are an integral part of the policy balance. Without them, protection could potentially last forever; competitors and other market participants would be perpetually unable to use the information. On the other hand, if these doctrines are too powerful, they may reduce the incentive to create such information in the first place.

The scope of these limiting doctrines is based on human ability. Trade secret protection ends if the secret becomes "readily ascertainable" to a human[167] or the owner fails to take "reasonable precautions" to prevent a human from discovering it.[168] The owner's exclusive right to use the information terminates when a human uses "proper means" to discover the information.[169] However, it seems likely that these doctrines will be retooled over time to reflect the enhanced ability of AI to discover information. This will pose three challenges to human-created trade secrets which exist today or will arise in the future.

First, defining "readily ascertainable" information by AI standards means that some human-created secrets will not qualify for protection. Second, the threshold for "reasonable precautions" to preserve secrecy will presumably be raised, thereby requiring owners of these secrets to adopt new protective measures. Third, the law will probably permit AI systems to acquire human-created secrets, despite the principle that secrets cannot be obtained by "improper means." In this situation, trade secret "trolls"[170] may pose a new danger.

B. Redefining the "Readily Ascertainable" Standard

When a trade secret becomes readily ascertainable, legal protection ends and the information enters the public domain, where it can be freely used by

---

make that person an inventor." *Id*. at 10049; *cf.* Ward, *supra* note 73, at 95 ("Because users of AI . . . are the actors most likely to ultimately benefit from the monopoly rights of a patent, they should be the default patent owners.").

167. *See supra* note 24 and accompanying text.

168. *Id*.

169. *See supra* note 146 and accompanying text.

170. *Cf.* David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L. REV. ONLINE 230, 234 (2015).

anyone.[171] The rationale for this outcome is straightforward: there is no reason to protect information which is easily knowable.[172] Although this doctrine was based on whether the information would be readily ascertainable by humans, it seems probable in the future it will be expanded to encompass AI ability as well.[173]

The transition to an AI-based test for "readily ascertainable" information will imperil existing trade secrets created by humans.[174] Because an AI system can, in some instances, easily discover information which would be unascertainable for a human, some human-created trade secrets will be terminated in the AI era.[175] For example, it seems likely that various types of business trade secrets, such as certain customer lists, price data, and business methods, might be readily ascertainable by AI.[176] Similarly, the ability of AI systems to write computer code may cause some existing code to lose protection.[177]

Consider the Coca-Cola formula, one of the most famous trade secrets.[178] The company website states that the cola contains these ingredients: "carbonated water, sugar, caramel colour, phosphoric acid, caffeine, natural flavours."[179] Aside from relative proportions in the recipe, the mystery ingredient is "natural flavours."[180] Even before the AI era, researchers were able to identify various aroma compounds in Coca-Cola and other colas.[181]

---

171. *See* Ryan Lambrecht, *Trade Secrets and the Internet: What Remedies Exist for Disclosure in the Information Age?*, 18 REV. LITIG. 317, 318 (1999).

172. *See supra* notes 78-79 and accompanying text. It might be argued that existing human-created trade secrets should be shielded against any change in the reasonably ascertainable standard, either generally or for a particular period. But the owner of such a secret has presumably already profited from its prior use; has a de facto lead time advantage in retaining the secret until a judicial decree resulting in termination of the secret; and can continue to use the secret in the future.

173. *See supra* notes 84-86 and accompanying text.

174. *See supra* notes 88-92 and accompanying text.

175. *See supra* notes 55-60, 84-86 and accompanying text.

176. *See, e.g.*, Thomas G. Sprankling, *Two Upcoming Shakeups in Trade Secret Law*, DAILY J., Dec. 8, 2023, at 5 ("While a human might not be able to easily sift through all available data about large tech company X or law firm Y to discern their client base, AI could—given the right prompts—potentially do so in seconds.").

177. *See, e.g.*, *supra* note 61 and accompanying text.

178. *See* Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co., 107 F.R.D. 288, 289 (D. Del. 1985) ("The complete formula for Coca-Cola is one of the best-kept trade secrets in the world.").

179. *What are the ingredients of Coca-Cola Classic?*, COCA-COLA CO., https://www.coca-cola.com/ph/en/about-us/faq/what-are-the-ingredients-of-coca-cola-classic [https://perma.cc/JT5T-NYTV].

180. *Id.*

181. *See, e.g.*, Yaowapa Lorjaroenphon & Keith R. Cadwaller, *Characterization of Typical Potent Odorants in Cola-Flavored Carbonated Beverages by Aroma Extract Dilution Analysis*,

Vanilla, cinnamon, nutmeg, other spices, and essential oils appear to be the other key ingredients.[182] Even if it is impossible for a human to duplicate the formula, an advanced AI program might well be able to do so with ease. As a result, the formula would lose all protection.

As a practical matter, however, a determination that a particular secret is "readily ascertainable" can only be obtained by a judicial decree.[183] For example, suppose trade secret owner F sues G for misappropriation; G would prove that the secret was readily ascertainable by an AI system; and the court would rule for G, thereby ending the secret.[184] Yet many trade secrets that become readily ascertainable in the AI era—and thus are terminated—will survive de facto because they have not been tested in litigation.

C. Requiring Enhanced Precautions to Maintain Secrecy

A second challenge to human-created trade secrets is that owners may fail to take the enhanced "reasonable" efforts to maintain secrecy that are necessary in the AI era.[185] Although both the UTSA and the DTSA require such precautions, the policy basis for this element is elusive.[186] Arguably, it (1) provides evidence that a valuable secret exists; (2) gives notice of the secret to competitors which discourages misappropriation; and (3) facilitates entry of the secret into the public domain where the owner no longer cares to protect it.[187]

Neither statute provides clear guidance about what "reasonable" efforts means.[188] The UTSA provides that the owner's efforts must be "reasonable under the circumstances"[189] while a comment notes that "extreme and unduly expensive procedures" are not required.[190] The Restatement (Third) of Unfair

---

63 J. AGRIC. & FOOD CHEM. 769 (2014) (describing a study aimed to determine odorants in the top three brands of cola-flavored carbonated beverages using "aroma extract dilution analysis").

182. WILLIAM POUNDSTONE, BIG SECRETS 38 (1983).

183. *See* Sarkes Tarzian, Inc. v. Audio Devices, Inc., 166 F. Supp. 250, 263 (S.D. Cal. 1958).

184. *See supra* text accompanying notes 91-92.

185. *See* UTSA, *supra* note 11, § 1(4)(ii); 18 U.S.C § 1839(3)(A).

186. *See* Lemley, *supra* note 9, at 349 ("Reasonable efforts to protect secrecy . . . probably don't make sense as a separate requirement.").

187. *See id.* at 346–47, 349; *see also* SHARON K. SANDEEN & ELIZABETH A. ROWE, TRADE SECRET LAW IN A NUTSHELL 93–94 (West Acad. 2d ed. 2018) (stating that the purposes are "to require trade secret owners to identify their putative trade secrets and put others on notice of the existence of their property rights before an act of trade secret misappropriation occurs"); SPRANKLING ET AL., *supra* note 49, at 189 (suggesting that the element helps to rebut any claim that the owner acquiesced in use of the secret by others).

188. The DTSA uses the term "reasonable measures." 18 U.S.C. § 1839(3)(A).

189. UTSA, *supra* note 11, § 1(4)(ii).

190. *Id*. § 1 cmt.

Competition helpfully observes that factors to be considered include "the foreseeability of the conduct through which the secret was acquired and the availability and cost of effective precautions against such an acquisition, evaluated in light of the economic value of the trade secret."[191] In practice, courts assess reasonableness on a case-by-case basis.[192]

The advent of AI requires that owners of human-created trade secrets take enhanced precautions to protect their information. In the past, the reasonableness of precautionary measures was based on conduct that could reasonably be expected from humans.[193] Today it is foreseeable that an AI system could be used to acquire a trade secret. Given its remarkable capacity to quickly piece together disparate clues in vast amounts of data, AI will often be more effective in obtaining existing secrets than a human would be, either as a tool directed by humans[194] or potentially with little human involvement.[195] Thus, the reasonableness of precautionary measures will necessarily be measured by what AI can do. This is a significant change because unlike patents and copyrights—which continue to exist even after they are available to the public—a secret loses legal protection if the precautions against disclosure are insufficient.[196]

It is possible that some trade secrets have already terminated because their owners did not take reasonable measures to maintain secrecy in light of the threat from AI technology. One main source of the data used to train generative AI systems is information available on the internet.[197] For example, ChatGPT-3.5 was trained on 300 billion words taken from "books, web texts, Wikipedia articles and other pieces of writing on the internet."[198] Thus, modern systems have long possessed data from which trade secrets could

191. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. c (AM. L. INST. 1995).

192. *See, e.g.*, Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991) (noting that reasonableness "depends on a balancing of costs and benefits that will vary from case to case").

193. *See* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 249 (1988) (discussing precautionary measures required by courts, which may include "disclosing the secret only under a confidentiality agreement and on a need-to-know basis, constructing fences or walls to block public view, using passwords, and restricting employee access to sensitive areas[,]" which are all certainly human activities).

194. *Cf.* Compulife Software Inc. v. Newman, 959 F.3d 1288, 1299 (11th Cir. 2020) (describing how a hacker used a bot to scrape trade secret data from owner's website).

195. *See supra* note 42 and accompanying text.

196. *See* Sharon K. Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, 19 VA. J.L. & TECH. 1, 13–16 (2014) (discussing various types of disclosure that may cause a secret to lose protection).

197. *See supra* note 35 and accompanying text.

198. Hughes, *supra* note 30.

probably be extracted. However, such secrets will continue to exist de facto until they are successfully challenged in litigation.[199]

In the future, trade secret owners should keep pace with evolving AI technology by taking greater precautions to avoid the loss of secrecy, including (1) conditioning website access by requiring a license agreement that the visitor will not utilize its data in connection with any AI system;[200] (2) using stronger methods to encrypt data; (3) avoiding digitization of data wherever possible; (4) restricting employee use of publicly available AI systems, particularly where there is a risk that prompts may inadvertently disclose sensitive data; (5) requiring password access and dual-factor identification for access to sensitive information; (6) mandating confidentiality requirements for employees, suppliers, and others; and (7) taking greater care that emails, purchase orders, sales documents, published articles, trade show events, and other information platforms do not imperil secrets.

D. Permitting AI Systems to Obtain Human-Created Trade Secrets

1. The "Improper Means" Muddle

A third challenge to human-created trade secrets is the risk that they will be obtained by AI systems without the consent of the secret owners. Anyone who acquires a trade secret by "proper means" is entitled to use it freely, just like the original owner.[201] Thus, if H owns a trade secret, J can acquire the same secret by proper means, such as independently inventing it, reverse engineering a product that embodies the secret, or reading about the secret in an article.[202] In this situation, H and J are effectively co-owners of the secret; each has rights to use, transfer, or disclose it without the consent of the

199. The determination that a trade secret has ended because the owner failed to take reasonable precautions can only be made by a judicial decree. Absent such a decree, a secret which is invalid will continue to exist de facto. *See supra* note 183 and accompanying text.

200. *E.g.*, UAB "Planner5D" v. Facebook, Inc., No. 19-CV-03132, 2019 WL 6219223, at *11 (N.D. Cal. Nov. 21, 2019) (rejecting the claim that the defendants used improper means to obtain trade secret information from plaintiff's website because, *inter alia*, plaintiff "does not allege how the Terms of Service [for its website] created a duty of confidentiality to maintain secrecy"); Broker Genius, Inc. v. Zalta, 280 F. Supp. 3d 495, 521–22 (S.D.N.Y. 2017) (denying preliminary injunction against trade secret misappropriation where the terms of service of plaintiff's website did not contain a confidentiality provision).

201. The UTSA and DTSA impose liability only for "misappropriation" of a trade secret—the acquisition, disclosure, or use of a trade secret that was acquired by "improper means." UTSA, *supra* note 11, § 1(2); 18 U.S.C. § 1839(5).

202. UTSA, *supra* note 11, § 1 cmt. (listing sample methods of "proper means"); 18 U.S.C. § 1839(6)(B) (stating that "other lawful means of acquisition" are allowed).

other.[203] On the other hand, if J obtains H's secret by "improper means" such as theft or bribery, J is liable for misappropriation of the secret. Suppose that J uses a generative AI system to obtain H's trade secret. Should this be viewed as an acquisition by "proper means" or "improper means"?[204]

Although "improper means" is a central concept in trade secret law, there is no comprehensive definition of the term. Instead, authorities seek to explain its meaning through examples. The UTSA provides that the term "*includes* theft, bribery, misrepresentation, breach or inducement of breach of a duty to maintain secrecy, or espionage through electronic or other means."[205] The DTSA definition of the term is identical.[206] Similarly, the Restatement (Third) of Unfair Competition section 43 explains that improper means "*include* theft, fraud, unauthorized interception of communications, inducement or knowing participation in a breach of confidence, and other means either wrongful in themselves or wrongful under the circumstances of the case."[207] The point is that even lawful acts—which are not wrongful per se—may be viewed as improper means in particular situations.

The landmark decision holding that a lawful method constituted "improper means" is *E.I. duPont deNemours & Co. v. Christopher*.[208] In 1969, the defendants took aerial photographs of a new DuPont factory under construction, which apparently revealed "a highly secret but unpatented process for producing methanol."[209] Relying on a comment in the First Restatement of Torts stating that "[i]n general . . . [improper means] are means which fall below the generally accepted standards of commercial morality and reasonable conduct,"[210] the Fifth Circuit concluded that the defendants had used improper means: "[t]o require DuPont to put a roof over the unfinished plant to guard its secret would impose an enormous expense to prevent nothing more than a school boy's trick."[211] The court asserted that "free wheeling industrial competition must not force us into accepting the law of

---

203. As a practical matter, J's co-ownership may reduce or eliminate the value of the secret to H—for example, if J discloses it to the public. Alternatively, J might demand a payment in return for keeping the information secret. *See infra* text accompanying notes 232-247.

204. Alternatively, suppose an AI system improperly obtains H's secret without any human involvement. Is there a legal actor who would be liable for misappropriation? While this question has not yet arisen, it could conceivably surface in the future. *Cf.* Mihailis E. Diamantis, *Vicarious Liability for AI*, 99 IND. L.J. 317 (2023) (discussing vicarious liability as a vehicle for holding humans accountable for harms AI inflicts).

205. UTSA, *supra* note 11, § 1(1) (emphasis added).

206. 18 U.S.C. § 1839(6)(A).

207. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (AM. L. INST. 1995) (emphasis added).

208. 431 F.2d 1012 (5th Cir. 1970).

209. *Id.* at 1013.

210. *Id*. at 1016 (citing RESTATEMENT OF TORTS § 757, cmt. f (AM. L. INST. 1939)).

211. *Id.*

the jungle as the standard of morality expected in our commercial relations."[212]

The *Christopher* logic is questionable, at best. The airplane was hardly novel technology, and aerial photography was common.[213] The defendants could have taken photos of the construction from an adjacent building without becoming liable. The key to *Christopher* may be the court's focus on the cost of taking precautions to guard against aerial photography: "[o]ur tolerance of the espionage game must cease when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened."[214] Thus, the court suggested that otherwise lawful means may be improper if it would be too expensive for a trade secret owner to guard against them.[215]

Today the concept of "improper means" can only be described as a muddle. A person who uses a lawful method to obtain a trade secret may be liable for misappropriation of the secret, even though he acted in good faith.[216] Despite attempts to derive a test from *Christopher* and other decisions, there is no accepted definition of the term.

2. AI as Improper Means?

No court has considered whether using AI to obtain a trade secret would be improper means. But the Eleventh Circuit decision in *Compulife Software Inc. v. Newman* tends to support this view.[217] There, Compulife compiled an electronic database of rates charged by life insurance companies using public information and sold access to the database to insurance agents.[218] It also developed a publicly available website where people could obtain free insurance quotes, based on the information in the database.[219] Defendants, who were competitors in the same business, hired a hacker to "scrape" data from Compulife's website using a bot.[220] It took the bot only four days to obtain "all premium estimates for every possible combination of demographic

212. *Id.*

213. *See* Olivia B. Waxman, *Aerial Photography Has Changed the World. Drones Are Just the Latest Example*, TIME (May 30, 2018, 4:12 PM), https://time.com/5281295/aerial-photography-history-drones/ [https://perma.cc/4HJC-ZLWX].

214. *Christopher*, 431 F.2d at 1016.

215. *Id.*

216. *Cf. id.* (holding that defendants improperly discovered trade secrets by taking aerial photos of plaintiff's manufacturing plant even though defendants did not breach a confidential relationship or engage in illegal conduct).

217. 959 F.3d 1288 (11th Cir. 2020). For an analysis of *Compulife*, see generally Geoffrey Xiao, Note, *Data Misappropriation: A Trade Secret Cause of Action for Data Scraping and a New Paradigm for Database Protection*, 24 COLUM. SCI. & TECH. L. REV. 125 (2022).

218. *Compulife*, 959 F.3d at 1296.

219. *Id.* at 1297.

220. *Id.* at 1299.

data within . . . two zip codes, totaling more than 43 million quotes," although this work "would have required thousands of man-hours if performed by humans."[221] The defendants then used this information to create a partial copy of Compulife's database.[222] The trial court found that the database was a trade secret, but that the defendants had not used improper methods to obtain it because the website was accessible to the public.[223] The Eleventh Circuit reversed:

> Although Compulife has plainly given the world implicit permission to access as many quotes as is *humanly* possible, a robot can collect more quotes than any human practically could. So, while manually accessing quotes from Compulife's database is unlikely ever to constitute improper means, using a bot to collect an otherwise infeasible amount of data may well be—in the same way that using aerial photography may be improper when a secret is exposed to view from above.[224]

The court did not determine whether the means were improper; it merely held that "the simple fact that the quotes taken were publicly available does not *automatically* resolve the question . . . ."[225]

Compulife involved an intentional effort by competitor K to effectively steal a trade secret from competitor L where all the relevant information was on L's website. In this context, the historic concern for protecting commercial morality—however it may be defined—is real.[226] Yet Compulife could have easily conditioned access to its website on an agreement to license terms that prohibited data scraping, which it failed to do.[227] Had it done so, the defendants' acquisition of data in violation of license terms would clearly have been improper means. Installation of a roof over the construction site in *Christopher* was arguably too expensive, but Compulife failed to erect a cost-effective computerized "fence."

In contrast, the use of AI to obtain trade secrets arises in quite a different setting. An AI system has access to literally billions of bits of information

---

221. *Id.* at 1300.

222. *Id.* at 1299.

223. *Id*. at 1312. The case was governed by the UTSA definition of "improper means," which Florida had adopted. *See id.* at 1311.

224. *Id*. at 1314 (citing *Christopher*, 431 F.2d at 1013) (emphasis in original).

225. *Id*. at 1315 (emphasis in original). On remand, the district court found that defendants had used improper means to obtain the information, in part because of "persistent efforts to sabotage Compulife by luring away its customers . . . ." Compulife Software, Inc. v. Rutstein, No. 9:16-CV-80808, 2021 WL 3713173, at *21 (S.D. Fla. July 12, 2021), *aff'd sub nom*. Compulife Software, Inc. v. Newman, 111 F.4th 1147 (11th Cir. 2024).

226. *See supra* note 143 and accompanying text.

227. *See* Xiao, *supra* note 217, at 132.

from a multitude of different sources.[228] Its database was created, presumably in most cases, without violating any license constraints—and without any intent to obtain a specific trade secret. Moreover, where the system is subsequently given a prompt to solve a particular problem, it seems likely that the program will utilize facts from a variety of different sources to piece together someone else's trade secret, rather than simply copy a competitor's website. Any concern for commercial morality is greatly attenuated in this context.

The scope of improper methods should logically evolve as technology advances. It seems probable that *Christopher* would be decided differently today. Satellites routinely take aerial photographs of the entire land surface of the United States, and the public can readily access those images through services such as Google Earth.[229] In the same manner, the development of advanced AI systems and their widespread use by the public has established a new technological baseline for assessing the propriety of particular means. Thus, courts will presumably conclude that the use of AI technology to learn trade secrets does not constitute improper means.

Finally, the notion that lawful acts can be viewed as improper means is probably obsolete. It reflects the traditional policy goal of safeguarding commercial morality.[230] But that goal has largely been eclipsed by the modern view that the purpose of trade secret law is to promote innovation.[231] Under this view, there is no justification for concluding that lawful acts are improper means.

3. Trade Secret "Trolls"

In recent decades, patent law has grappled with the problem of the nonpracticing entity or "patent troll."[232] Traditionally, a patentee used the invention in the production of goods or services. But as Justice Kennedy explained in *eBay, Inc. v. MercExchange*, "[a]n industry has developed in which firms use patents not as a basis for producing or selling goods but, instead, primarily for obtaining licensing fees."[233] A nonpracticing entity has sometimes been able to coerce a substantial payment from a company that

228. Abid Haleem et al., *Artificial Intelligence (AI) Applications for Marketing: A Literature-Based Study*, 3 INT'L J. INTELLIGENT NETWORKS 119, 120 (2022).

229. *See* Michael F. Goodchild et al., *Next-generation Digital Earth*, 109 PROC. NAT'L ACAD. SCIS. 11088, 11088 (2012).

230. *See supra* notes 143, 208-212 and accompanying text.

231. *See supra* notes 17, 144-145 and accompanying text; *see also* Menell, *supra* note 11, at 14–15 (discussing "commercial morality" and "encouraging research and development" as guiding principles in trade secret law).

232. *See* Sun*, supra* note 98, at 111–14 (discussing AI and patent trolls).

233. 547 U.S. 388, 396 (2006) (Kennedy, J., concurring).

produces goods by threatening to obtain an injunction that will shut down its business—often based on an overbroad patent that relates only to a small portion of the particular company's product, thereby curbing innovation.[234]

To date, this problem has not arisen in the trade secret setting because: (1) such secrets are generally held by individuals and entities that use them to produce goods or services; and (2) while a patent gives the patentee the exclusive right to the invention, a trade secret may be owned by multiple parties and thus any owner may use it freely.[235] But assuming that AI is viewed as proper means to obtain a trade secret, the nonpracticing entity problem from patent law could arise in a different context—a threat to publicly disclose the secret unless the entity is paid.

For example, the Coca-Cola Company has presumably invested millions of dollars in producing and promoting its famous drink. Suppose M uses an AI-system to ascertain the cola formula through proper means. At this point, the formula is jointly owned by the company, which produces the product, and M, who does not. While both are entitled to use the information, M has no meaningful ability to do so. He might attempt to license the formula to other soft drink companies, but this might well be impractical. For instance, competitors might suspect that M obtained the formula by improper means and fear becoming liable for misappropriation themselves.[236]

In this situation—somewhat like a patent troll—M could threaten to end the secret by making it public unless he is paid a large sum. Current trade secret law does not address this situation.[237] As a general rule, where multiple parties own the same secret, any one of them is entitled to disclose it, thus terminating the secret for all owners.[238] Of course, such intentional disclosure is rare because each co-owner either uses the secret or plans to do so, and thus has an interest in maintaining its existence. But M could credibly threaten to disclose the secret because he loses nothing by doing so.

---

234. Michael J. Meurer et al., *The Private and Social Costs of Patent Trolls: Do Nonpracticing Entities Benefit Society by Facilitating Markets for Technology?*, REGULATION, Winter 2011-2012, at 26 ("[T]hese lawsuits substantially reduce [technology companies'] incentives to innovate."); WILLIAM J. WATKINS, JR. ET AL., PATENT TROLLS: PREDATORY LITIGATION AND THE SMOTHERING OF INNOVATION 1 (2014).

235. *See supra* text accompanying note 132.

236. A person who uses a trade secret of another and "had reason to know that his knowledge of the trade secret was . . . derived from or through a person who had used improper means to acquire it" is liable for misappropriation. UTSA, *supra* note 11, § 1(2)(ii)(B)(I).

237. *See, e.g.*, Zurich Amer. Life Ins. Co. v. Nagel, 538 F. Supp. 3d 396, 405 (S.D.N.Y. 2021) (observing that the DTSA is not designed to "prohibit extortion").

238. *See, e.g.*, Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) (noting that the disclosure of a trade secret "to others who are under no obligation to protect the confidentiality of the information" terminates the secret).

In many states, M might be liable for blackmail or extortion if Coca-Cola made the demanded payment.[239] While some jurisdictions still use the term "blackmail," the Model Penal Code has renamed the offence "theft by extortion;" its section 223.4, which many states have adopted,[240] provides that a person is guilty of this offense "if he purposely obtains property of another by threatening to: . . . inflict any other harm that would not benefit the actor."[241] Here, M obtained money from Coca-Cola by threatening to disclose the formula, and this harm to the secret would not benefit M; accordingly, M would be liable for extortion.[242]

M's de facto co-ownership of the secret should not make a difference in this situation.[243] Under Model Penal Code section 223.4, it is irrelevant. This is consistent with the theory underlying the criminalization of blackmail—the blackmailer is liable for his threat to disclose a secret, even if he may lawfully reveal the secret.[244] Moreover, it makes no policy sense to allow a co-owner like M to demand payment in this situation. The reason that trade secret law recognizes rights in a person like M who legitimately discovers another's secret is to permit M to utilize the information in a socially-beneficial manner, normally by using the secret to produce goods or services, not to provide ammunition for extortion.[245]

On the other hand, there is no consensus on whether M's conduct constitutes blackmail or extortion. A number of states would conclude that it does not.[246] The same result follows under federal law. The key statute is 18 U.S.C. § 1951(a), which imposes liability for extortion that affects interstate commerce; but the offense requires "wrongful use of actual or threatened

---

239. As a general matter, "[t]he terms blackmail and extortion are often used interchangeably." James Lindgren, *Unraveling the Paradox of Blackmail*, 84 COLUM. L. REV. 670, 673 (1984). The Model Penal Code abandoned the term "blackmail" and instead classified most traditional blackmail situations as "extortion." *See id.* at 679.

240. *See, e.g.*, ALASKA STAT. ANN. § 11.41.520 (West 2024).

241. MODEL PENAL CODE § 223.4(7) (AM. L. INST. 1980).

242. *Cf.* People v. Chew, No. B173861, 2005 WL 1332208, at *4 (Cal. Ct. App. June 7, 2005) (affirming conviction for attempted extortion where defendant threatened to disclose his employer's confidential information, including trade secrets, unless he was paid $39,000).

243. The phrase "which would not benefit the actor" in section 223.4 of the Model Penal Code was intended to "preclude a theft prosecution where the purpose of the threat is to secure economic benefit—the obtaining of property—for which the actor might have some claim." MODEL PENAL CODE § 223.4 cmt. k. In the situation discussed in the text, M has no legitimate claim to the money demanded from Coca-Cola.

244. Sidney W. DeLong, *Blackmailers, Bribe Takers, and the Second Paradox*, 141 U. PA. L. REV. 1663, 1663 (1993) ("The criminalization of blackmail has been considered paradoxical because it would make unlawful a threat to do something the threatener has a legal right to do.").

245. It might be argued, of course, that disclosure would benefit the public by allowing anyone to use the information.

246. *See, e.g.*, IOWA CODE § 711.4 (2021); KY. REV. STAT. ANN. § 514.080 (West 2021).

force, violence, or fear, or under color of official right,"[247] which is not present on these facts.

It is too early to know whether trade secret trolls will arise in the future. But as the AI era unfolds, there is certainly a risk that the problem will surface. It would be helpful to amend the UTSA and DTSA to deal with this danger.

V. TRADE SECRET LAW AND THE AI THREAT TO HUMANS

A. An Existential Threat?

The Center for AI Safety has issued an open letter asserting that "[m]itigating the risk of extinction from A.I. should be a global priority alongside other societal-scale risks, such as pandemics and nuclear war."[248] U.N. Secretary-General António Guterres similarly warned that "scientists and experts have called on the world to act, declaring AI an existential threat to humanity on a par with the risk of nuclear war."[249]

The potential dangers from a patented invention can be assessed because the quid pro quo for a patent is public disclosure.[250] For example, Dr. Ananda Chakrabarty's pioneering effort to secure a patent on a genetically-engineered micro-organism sparked widespread publicity.[251] In the ensuing litigation, Nobel laureates and other scientists argued that "genetic research may pose a serious threat to the human race."[252] Although the patent was eventually approved, the Environmental Protection Agency was alerted to this risk and later adopted rules to govern these organisms.[253]

---

247. 18 U.S.C. § 1951(b)(2).

248. Kevin Roose, *A.I. Poses 'Risk of Extinction*,' *Tech Leaders Warn*, N.Y. TIMES, May 30, 2023, at A1. As one scholar notes, if AI systems develop superintelligence in the future "the outcome could easily be one in which humanity quickly becomes extinct." BOSTROM, *supra* note 28, at 116. *See generally id*. at 153 (discussing this scenario); JAMES BARRAT, OUR FINAL INVENTION: ARTIFICIAL INTELLIGENCE AND THE END OF THE HUMAN ERA (2015). President Biden also recognized that AI may pose a threat to national security. Exec. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023).

249. U.N. Secretary General, Secretary-General's Opening Remarks at Press Briefing on Policy Brief on Information Integrity on Digital Platforms (June 12, 2023), https://www.un.org/sg/en/content/sg/speeches/2023-06-12/secretary-generals-opening-remarks-press-briefing-policy-brief-information-integrity-digital-platforms [https://perma.cc/7K47-69Y3]. In one survey, 36% of AI experts expressed concern that the technology might produce a "nuclear-level catastrophe." Hunt, supra note 77.

250. Peter Lee, *New and Heightened Public–Private Quid Pro Quos: Leveraging Public Support to Enhance Private Technical Disclosure, in* INTELLECTUAL PROPERTY, COVID-19, AND THE NEXT PANDEMIC: DIAGNOSING PROBLEMS, DEVELOPING CURES 2 (Madhavi Sunder & Haochen Sun eds., forthcoming 2024) (on file with author).

251. *See generally* Diamond v. Chakrabarty, 447 U.S. 303 (1980).

252. *Id*. at 316.

253. *See* 40 C.F.R. §§ 725.1-725.984 (2024).

In contrast, it may be difficult or impossible for officials or the public in general to become aware of a potential AI threat. The algorithms that form the heart of AI systems are protected by trade secret law,[254] because they are abstract ideas which cannot be patented.[255] Similarly, most of the information generated by these systems will not meet the rigorous standards for patentability, but may qualify for trade secret protection. While patent law emphasizes disclosure, trade secret law by definition requires secrecy.[256] As the First Circuit explained in *TLS Management & Marketing Service v. Rodríguez-Toledo*: "[t]here is no requirement of registration and, by definition, there is no public knowledge of the trade secret in advance of litigation."[257] Unless litigation arises, a trade secret does not undergo scrutiny by anyone other than its owner.[258]

For example, suppose AI is used to create a biological weapon that could harm human health. This weapon—and the knowledge that it exists—might well qualify for protection as trade secrets. The information has potential economic value because, for instance, the AI system operator could invest in medical and pharmaceutical companies that would obtain business if such a weapon was used; such information would not be generally known or readily ascertainable; and it certainly would be kept secret. Alternatively, suppose that employees at an AI company became convinced that an advanced AI program itself posed a serious risk to humanity. The algorithms which comprise the program would be protected as trade secrets. In either situation, disclosure of the trade secret would constitute a misappropriation of the secret, subjecting the whistleblower to civil and criminal liability[259]—absent a special exception.

B. A Partial Solution: Disclosure to Government Officials

Under limited circumstances, a person accused of misappropriating a trade secret by disclosure may assert a common law privilege as a defense. As the Restatement (Third) of Unfair Competition explains, a "privilege is likely to be recognized . . . in connection with the disclosure of information that is relevant to public health or safety, or to the commission of a crime or tort, or

254. Greer, *supra* note 8, at 262.

255. An "abstract idea" is not patentable. *Diamond*, 447 U.S. at 309.

256. *See* Greer, *supra* note 8, at 258.

257. 966 F.3d 46, 51–52 (1st Cir. 2020).

258. *Cf.* Charlotte A. Tschider, *Beyond the "Black Box,"* 98 DENV. L. REV. 683, 688 (2021) (arguing that use of trade secret law to protect AI algorithms frustrates the policy goal of ensuring transparency in automated decision-making).

259. For example, 18 U.S.C. § 1836(b) creates civil liability for misappropriation, while 18 U.S.C. §§ 1831 and 1832 impose criminal liability.

to other matters of substantial public concern."[260] Whether the privilege arises turns on factors such as the nature of the information, the reason for disclosure, and the method by which the person obtained the secret.[261] But this formulation "offers little clarity or assurance to prospective whistleblowers" because the defense "turns on a case-by-case balancing of potentially subjective factors."[262]

In addition, the DTSA expressly provides whistleblower immunity for those who disclose trade secrets to government officials "solely for the purpose of reporting or investigating a suspected violation of law."[263] In this situation, the whistleblower "shall not be held criminally or civilly liable under any Federal or State trade secret law" for disclosure of the secret.[264]

Yet neither of these approaches is sufficient to deal with the nature and magnitude of the AI threat. In some situations, it will be difficult to know whether the disclosure of a particular secret will be covered by the "murky" common law privilege;[265] by definition, this determination can only be made by a judge after the disclosure occurs. Moreover, the DTSA whistleblower immunity provision applies only where there is a suspected violation of law.[266] Because there is no comprehensive regulation of AI today,[267] it is not clear whether a whistleblower could reasonably believe that a violation of law has occurred.

It seems likely that comprehensive federal legislation will regulate AI systems in the near future. For example, the "Blueprint for an AI Bill of Rights" issued by President Biden acknowledges that the public should be "protected from unsafe . . . [AI] systems."[268] It indicates that such systems should be subject to "ongoing monitoring [to] demonstrate they are safe" so

260. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c. (AM. L. INST. 1995).

261. *Id.* For an example of the unpredictable application of the common law privilege, see Cafasso v. Gen. Dynamics C4 Sys., Inc., 637 F.3d 1047, 1062 (9th Cir. 2011) (rejecting whistleblower's claim that the privilege shielded her from liability for removing files from her employer in order to report its illegal activity); *see also* Menell, *supra* note 11, at 32–34 (discussing Cafasso's plight).

262. Menell, *supra* note 11, at 30.

263. 18 U.S.C. § 1833(b)(1)(A).

264. *Id.* § 1833(b)(1).

265. Menell, *supra* note 11, at 30 (noting that the scope of the privilege is "murky").

266. 18 U.S.C. § 1833(b)(1)(A).

267. *See* Victor Li, *What Could AI Regulation in the US Look Like?*, AM. BAR ASS'N (June 14, 2023), https://www.americanbar.org/groups/journal/podcast/what-could-ai-regulation-in-the-us-look-like/ [https://perma.cc/5SLJ-XAM4].

268. OFF. OF SCI. & TECH. POL'Y, WHITE HOUSE, BLUEPRINT FOR AN AI BILL OF RIGHTS: MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE 5 (2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/#safe [https://perma.cc/2KEQ-HX7G].

that "unsafe outcomes" can be mitigated.[269] This can only be accomplished through legislation.[270] The monitoring contemplated by the Blueprint will be a more effective technique if the privilege to disclose trade secrets is clarified, so that employees and other insiders are willing to inform officials about specific AI risks.

Accordingly, any future federal statute regulating AI should expand the existing DTSA whistleblower protection by including a provision that grants broad immunity to any person who confidentially discloses an AI-related trade secret to a designated government official if that person has reason to believe that the secret poses a significant risk to public health or safety.[271]

VI. CONCLUSION

The AI revolution will transform trade secret law. With the ability to match and eventually exceed human reasoning abilities, advanced AI systems will create new forms of valuable information, serving the policy goal of creating innovations that benefit the public. The criteria for creating and maintaining trade secrets will shift over time from human-centric benchmarks toward new standards that reflect the capabilities of these systems. As a result, certain human-created secrets will be imperiled. Ultimately, less information may ultimately qualify for trade secret protection, but that information will be

---

269. *Id.* The Blueprint further provides that "[i]ndependent evaluators . . . should be given access to the [AI] system" to evaluate its safety, "in a manner consistent with . . . privacy, security, law, or regulation (including, e.g., intellectual property law) in order to perform such evaluations." *Id*. at 20.

270. In October 2023, President Biden issued an executive order that calls on federal agencies to, *inter alia*:

> Establish guidelines and best practices, with the aim of promoting consensus industry standards, for developing and deploying safe, secure, and trustworthy AI systems, including: . . . launching an initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities through which AI could cause harm. . . .

Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023). While this effort to encourage "consensus industry standards" is laudable, such standards would be nonbinding, and thus unlikely to be effective.

271. In the long run, it is not clear how helpful this approach will be. At some point, there may be little or no human involvement with fully autonomous AI systems. As one commentator predicts:

> Any defenses or protections we try to build . . . will be anticipated and neutralized with ease by the AI once it reaches superintelligence status. . . . We won't be able to control them because anything we think of, they will have already thought of, a million times faster than us.

Hunt, *supra* note 77.

more valuable than today's secrets. In this sense, trade secret law will move closer to patent law.

The debates about the impact of AI on patent law and copyright law may eventually be resolved by federal legislation that supersedes the guidance issued by the PTO and the Copyright Office. In turn, the UTSA and DTSA should be amended to establish standards for adjudicating AI-related trade secret disputes. At a minimum, these amendments should provide that AI-generated secrets qualify for legal protection, develop an ownership regime for these secrets, clarify how the "reasonably ascertainable" test applies in the AI era, affirm that use of AI to obtain a trade secret is not "improper means," penalize trade secret trolls, and strengthen protection for whistleblowers who warn of AI dangers.

But legislation always lags behind technology. Courts will probably have to grapple with the impact of AI on trade secret law well before the UTSA and DTSA are amended. In the interim, this Article and future works by other scholars will hopefully provide useful guidance for judges, policymakers, attorneys, and the broader public on how to rebalance trade secret law for the AI era.