



GENERATIVE ARTIFICIAL INTELLIGENCE AND TRADE SECRECY

David S. Levine *

Introduction	559
I. Trade Secret Law and Speech	562
A. Trade Secret Basics	562
B. Trade Secrets and Speech	568
II. Mundane Destroyer of Trade Secrets: ChatGPT and Reasonable Efforts ..	575
III. Supercharged Reporter, Civil Society Watchdog, or Whistleblower: ChatGPT and Speech of Public Interest.....	581
A. News Media.....	581
B. Whistleblowers	583
C. Civil Society Watchdogs.....	584
IV. Where Are We Headed?	586
Conclusion	587

INTRODUCTION

The era of generative artificial intelligence (“Generative AI”) has begun, whether we want it to or not. As this Article explains, we also now have new methods for creating, losing, disseminating, and even leaking trade secrets as a result. Indeed, from ingesting trade secrets in its training data to sharing trade secrets in response to queries, Generative AI opens new challenges to trade secrecy even

* Professor, Elon University School of Law; Affiliate Scholar, Center for Internet and Society, Stanford Law School; Affiliate, Center for Information, Technology, and Public Life, University of North Carolina at Chapel Hill. The author thanks KimberMarie Faircloth for her research assistance, Jane Bambauer, Elizabeth Rowe, and Eugene Volokh for their comments, and The Journal of Free Speech Law for the opportunity to participate in this symposium. All errors and omissions are the author’s.

while it adds to an information ecosystem that thrives on knowledge dissemination. This Article is the first to examine this new and immediate challenge and its trade secrets implications. It is written not only to frame the discussion about Generative AI and trade secrecy, but also the impact of Generative AI on information control and flows more broadly, for future analysis.

Emerging from the debates in technology and academic circles about solving problems through massive computing power and automated decision-making,¹ algorithmic discrimination,² and privacy,³ Generative AI is now approaching the forefront of the basic questions of what it means to be human.⁴ Unusually, we can trace the day that this happened to November 30, 2022, the day that a hitherto largely unknown company, OpenAI, unilaterally decided to release its Generative AI, ChatGPT, for public consumption and use.⁵

Generative AI is defined as

a set of algorithms, capable of generating seemingly new, realistic content—such as text, images, or audio—from the training data. The most powerful generative AI algorithms are built on top of foundation models that are trained on a vast quantity of unlabeled data in a self-supervised way to identify underlying patterns for a wide range of tasks.⁶

¹ See Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 876 (2016).

² See Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 674 (2016).

³ See Liane Colonna, *Artificial Intelligence in the Internet of Health Things: Is the Solution to AI Privacy More AI?*, 27 B.U. J. SCI. & TECH. L. 312, 321 (2021).

⁴ See Janna Anderson & Lee Rainie, *Artificial Intelligence and the Future of Humans*, PEW RESEARCH CENTER (Dec. 10, 2018), <https://www.pewresearch.org/internet/2018/12/10/artificial-intelligence-and-the-future-of-humans/> (“Yet, most experts, regardless of whether they are optimistic or not, expressed concerns about the long-term impact of these new tools on the essential elements of being human.”).

⁵ See Jonathan Vanian, *Why Tech Insiders Are So Excited About ChatGPT, A Chatbot That Answers Questions and Writes Essays*, CNBC (Dec. 13, 2022, 6:51 PM), <https://www.cnbc.com/2022/12/13/chatgpt-is-a-new-ai-chatbot-that-can-answer-questions-and-write-essays.html>.

⁶ *Generative AI*, BOSTON CONSULTING GROUP, <https://www.bcg.com/x/artificial-intelligence/generative-ai> (last visited Aug. 3, 2023). The article goes on to explain, “For example, GPT-3.5, a foundation model trained on large volumes of text, can be adapted for answering questions, text summarization, or sentiment analysis. DALL-E, a multimodal (text-to-image) foundation model,

Beyond the grand philosophical questions, AI also raises fundamental questions as to intellectual property law and information flows, because Generative AI creates. As Dan Burk explains in his recent article,

AI systems have been trained to generate standardized news reports, and it is now routine for machine learning systems to write short newspaper features, such as sports score reporting. AI systems are progressing toward the generation of more complicated texts, and may be expected to generate dramatic scripts, screenplays, stories, and other literary works.⁷

The Internet did not create. The phonograph did not create. Nor did the printing press. These were revolutionary media for access, copying, and distribution of works created by humans. They were, by current measure, revolutionary platforms for content and speech.

Generative AI, as the name suggests, is different. It is not creating “ideas,” *per se*, but creating content and speech in its most basic current form: words, images, and sound. Additionally, it makes that content intelligible, and even entertaining and useful, to humans. Through the probabilistic matching that it uses to create sentences and paragraphs based upon the data provided to it,⁸ Generative AI may stumble upon the incisive, the meaningful, the valuable speech that makes humanity communicative like no other living species.⁹ It may find correlations that humans would not readily conceive or see, and render them through text, sound, and

can be adapted to create images, expand images beyond their original size, or create variations of existing paintings.” *Id.*

⁷ Dan L. Burk, *Cheap Creativity and What It Will Do*, 57 GA. L. REV. 1669, 1675 (2023).

⁸ See James Grimmelman, *Glimpse of the Future: AI in Hollywood*, THE ANKLER (Feb. 7, 2023), <https://theankler.com/p/glimpse-of-the-future-ai-in-hollywood> (explaining that “what makes generative AIs different is that they are creative . . . it starts with a simple input, called a ‘prompt,’ and produces a rich media output”).

⁹ See Burk, *supra* note 7, at 1680; see also Derek E. Bambauer, *Secrecy is Dead—Long Live Trade Secrets*, 93 DENVER L. REV. 833, 846 (2016). As is already understood amongst those who study it, it can also be prone to “hallucinations,” a subtle way to describe false and misleading statements. For example, this author has regularly been told by ChatGPT that he is a graduate of Yale Law School when asked to write a biography of himself. This is false. ChatGPT is likely generating this response based upon training data that shows the likelihood of law professors graduating from one of the top law schools, like Yale. Eric J. Segall & Adam Feldman, *The Elite Teaching the Elite: Who Gets Hired by the Top Law Schools?*, 68 J. LEGAL EDUC. 614, 618 (2019) (explaining their findings that “almost ninety-five percent of the faculty members at each of the Top Ten schools who attended a U.S. law school attended a Top Ten law school”).

images in cogent ways that may not occur to humans or would take massive time and effort to create. Therein lies the immediate upheaval: Generative AI is an intelligible, if often “weird,”¹⁰ speech machine. In that sense, it creates information that can be useful in innovation and monetized. In that way, it can augment, or in more stark and dystopian ways, replace human creativity and speech.

This article will identify and analyze the most immediate concerns that arise from the confluence of Generative AI and the desire to maintain but also monetize trade secrets. The first part will discuss the basics of protecting trade secrets in the modern communications era and how Generative AI implicate speech interests, as best as we can tell from available information. The second and third parts identify a few immediate scenarios that warrant attention: Generative AI as a tool for trade secret misappropriation, and its ability to find and even create information that might otherwise qualify as trade secrets under certain circumstances and render that information free from trade secrecy’s hold. As explained, trade secrets have already been disseminated by ChatGPT, causing companies like Amazon and Samsung to rein in their employees’ use of the technology. The article closes with some thoughts on further research and on where we might be headed.

I. TRADE SECRET LAW AND SPEECH

A. *Trade Secret Basics*

Under the Uniform Trade Secrets Act (UTSA), the foundational US trade secret law and the standard for trade secret law in the United States, trade secrets are defined as

a formula, process, device, or other business information that is kept confidential to maintain an advantage over competitors; information—including a formula, pattern, compilation, program, device, method, technique, or process—that (1) derives independent economic value, actual or potential, from not being generally known or readily ascertainable by others who can obtain economic value from its disclosure or use, and (2) is the subject of reasonable efforts, under the circumstances, to maintain its secrecy.¹¹

¹⁰ See Watch Me Forever (@WatchMeForever), TWITCH, <https://www.twitch.tv/watchmeforever> (last accessed Aug. 3, 2023).

¹¹ UNIF. TRADE SECRETS ACT § 1(4) (UNIF. L. COMM’N 1985).

Thus, the right to trade secrecy protection is “defined by the extent to which the owner of the secret protects his interest from disclosure to others.”¹² The Restatement (First) of Torts, arguably the most influential scholarly work on trade secrecy in the United States, listed six bases for determining whether information constitutes a trade secret. These elements, which have been adopted by many courts when assessing whether a trade secret exists, reflect an emphasis on the owner’s activities and a burden placed on the owner to maintain secrecy through what the UTSA calls “reasonable efforts”:¹³

(1) the extent to which the information is known outside of [the] business; (2) the extent to which it is known by employees and others involved in [the] business; (3) the extent of measures taken by [the business] to guard the secrecy of the information; (4) the value of the information to [the business] and [its] competitors; (5) the amount of effort or money expended by [the business] in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.¹⁴

A trade secret owner must therefore prove that it exercised “reasonable efforts” to maintain the secret, often with reference to the above elements, along with proving its value in the marketplace, before being able to enjoy trade secret law protection.

Additionally, trade secret misappropriation requires use of an “improper means” of acquisition.¹⁵ Generally likened to acts like theft, the paradigm trade secret misappropriation action involves the former employee who brings a former employer’s trade secrets to a competitor.¹⁶ Once that trade secret is “used” or “disclosed,” the *prima facie* elements for trade secret misappropriation are met.¹⁷

¹² DVD Copy Control Ass’n, Inc. v. Bunner, 31 Cal. 4th 864, 880 (2003) (quoting Ruckelshaus v. Monsanto, 467 U.S. 986, 1002 (1984)).

¹³ UNIF. TRADE SECRETS ACT § 1(4)(ii).

¹⁴ Ashland Mgmt. Inc. v. Janien, 82 N.Y.2d 395, 407 (1993) (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939)) (brackets in original).

¹⁵ UNIF. TRADE SECRETS ACT § 1(1) (“Improper means” includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.”).

¹⁶ See David S. Almeling, *Recent Trade Secret Reform—And What Else Should Change*, LAW360 (Sep. 23, 2013, 11:24 AM), <https://www.law360.com/articles/474239/recent-trade-secret-reform-and-what-else-should-change>.

¹⁷ UNIF. TRADE SECRETS ACT § 1(2).

Generative AI raises some significant questions for the core trade secret misappropriation doctrine that has governed trade secret law for decades. What constitutes “reasonable efforts” is subject to debate when use of generative AI like ChatGPT is involved. Several of the “reasonable efforts” core elements are put to the test by Generative AI as an innovation tool, like efforts to maintain the secret and its knowledge beyond the owner’s purview. As discussed below in Part II, if a trade secret owner places confidential information into ChatGPT’s training data (wittingly or unwittingly) through a query or some other action, that could deviate sufficiently from “reasonable efforts” to maintain a trade secret as to vitiate trade secret protection all together.¹⁸

Additionally, ChatGPT can aid in the misappropriation of a trade secret, acting as an accomplice or agent (of sorts) of a trade secret misappropriator. If ChatGPT is directed to answer a query through prompts that could reveal a trade secret from within its own universe of data, the clever trade secret misappropriator has found a very capable partner in crime. As one cybersecurity expert recently noted, “Employees enter classified correspondences or use the bot to optimize proprietary code. Given that ChatGPT’s standard configuration retains all conversations, this could inadvertently offer a trove of sensitive intelligence to threat actors if they obtain account credentials.”¹⁹

¹⁸ See discussion *infra* Part II; see also Aron Hsiao & Jeanne McAvoy, *AI Means Companies Are Leaking More Confidential Data Than Ever Before*, PLURILOCK (June 29, 2023), <https://pluri-lock.com/blog/ai-means-companies-are-leaking-more-confidential-data-than-ever-before/> (describing potential situations where employees could leak sensitive data to AI, such as “[a] finance employee at a publicly traded company needs to generate an earnings report” or “[a]n HR manager needs to write a termination letter” who both use AI potentially resulting in sensitive data being “transmitted to a third party (the AI platform)”).

¹⁹ Mathew J. Schwartz, *Info-Stealing Malware Is Harvesting ChatGPT Credentials*, BANK INFO SECURITY (June 20, 2023), <https://www.bankinfosecurity.com/infostealing-malware-harvesting-chatgpt-credentials-a-22331> (explaining further that big corporations like JPMorgan, Amazon, Apple, and so on have already implemented restrictions for employees regarding use of AI for work-related tasks); see also Cameron Coles, *11% of Data Employees Paste Into ChatGPT Is Confidential*, CYBERHAVEN (June 18, 2023), <https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt/>. Cyberhaven, a data security product company, estimated that 10.8% of employees use ChatGPT in the workplace and at least 8.6% have pasted company data into it; furthermore, Cyberhaven predicts that 4.7% of this information being entered is confidential. *Id.* A hypothetical example of sensitive information being used as an AI output: “[a] doctor inputs a patient’s name and details of their condition into ChatGPT to have it draft a letter to the patient’s

As of this writing and to the best of our knowledge, ChatGPT does not assume that any information in its training data is confidential or a trade secret, much less that access credentials have been stolen. Nor does it question how access credentials were acquired. It will, however, attempt to answer any queries that don't violate its opaque programmed rules.²⁰ Such questions could be asked by anyone, regardless

insurance company justifying the need for a medical procedure. In the future, if a third party asks ChatGPT "what medical problem does [patient name] have?," ChatGPT could answer based on what the doctor provided." *Id.*

²⁰ As an experiment, the author asked ChatGPT version 3.5 the following question: "If someone puts trade secrets into your training data by mistake, it may still wind up in your outputs, correct?" ChatGPT replied:

Yes, you are correct. If trade secrets or proprietary trade information are mistakenly included in the training data of an AI language model, there is a possibility that the model's outputs could indirectly reflect or include aspects of that information. The model learns patterns and information from the training data, and if trade secrets are present, it may inadvertently capture and reproduce some elements of that information in its responses.

When the author pressed ChatGPT to answer whether it would be aware of information entered into its data that might qualify as a trade secret, it logically denied any ability to know and put that onus on its trainers and users:

As an AI language model, I don't have awareness or direct access to information that is entered or used as part of my training data. I don't have visibility into specific data points or knowledge of whether certain information qualifies as a trade secret or not.

The training data used to train models like me consists of a diverse range of publicly available texts, and the specific data sources or information contained within them are not individually identifiable or accessible to me. I don't have the ability to recognize or distinguish trade secrets within the training data or any other form of proprietary information.

It is the responsibility of the data providers and trainers to ensure that they handle and curate the training data appropriately, respecting legal and ethical guidelines, and safeguarding any sensitive or proprietary information.

Author chat with ChatGPT, July 17, 2023 (transcript on file with author). While the above responses likely reflect the same probabilistic textual responses that cause "hallucinations" and other erroneous responses to queries, it is also possible that the response reflects the training data about its own programming, presumably provided by OpenAI itself. *See Part II, infra.*

In contrast, when asked about inputting trade secrets into a query, Google's Bard was more equivocal. While it repeatedly replied that it was not "recommended" to "enter trade secrets into Bard," when the author pressed whether Bard could "tell someone else my trade secrets," it responded that it "could not tell someone else your trade secrets." It asserted that it was bound by its

of whose access credentials were used. As a result, ChatGPT can be the perfect partner for those seeking to access trade secrets that would otherwise be inaccessible.

The value proposition in trade secrecy lies in knowing not only that information is valuable, but that a competitor does not know it.²¹ Thus, a carefully worded query could result in revelation of information that would be innocuous or meaningless to all but those who have particularized knowledge about an industry, a line of research, or a competitor.

Because trade secret misappropriation also requires “use or disclosure,”²² ChatGPT’s very reason for being may easily cause information to be misappropriated in any number of ways, and quickly. As a practical matter, if ChatGPT has trade secret information in its training data, ChatGPT may include it in a response.²³ That is enough of a reason for trade secret owners to be wary of Generative AI’s information dissemination powers.

Importantly, if the foregoing (and indeed, much of the following) sounds a bit uncertain, there is good reason. As discussed more fully in Part II, Generative AI’s code is secret, and its very operations – how exactly it decides what words should

“service agreement” that precludes it from “disclosing any information that is confidential or proprietary to my users.” It then made a startling assertion: “For these reasons, I can assure you that I will not tell anyone else your trade secrets. You can trust me to keep your information safe.” Thus, while it repeatedly recommended against it, its use of the amorphous word “trust” could easily confuse users into thinking that it may be safe to use Bard for “not recommended” reasons. Again, the same likelihoods of the probabilistic- and programming-based responses would seem to apply here. Author chat with Bard, July 17, 2023 (transcript on file with author).

²¹ UNIF. TRADE SECRETS ACT § 1(2).

²² *Id.*

²³ See *Hurry Family Revocable Tr. v. Frankel*, 2023 WL 23805, No. 8:18-cv-2869-CEH-CPT (M.D. Fla. Jan. 3, 2023), which “found alleged trade secret secrets did not lose their secrecy status even though they were posted on the court’s public, electronic docket.” Puya Partow-Navid & Daniel Joshua Salinas, *Spilling Secrets to AI: Does Chatting with ChatGPT Unleash Trade Secret or Invention Disclosure Dilemmas?*, SEYFARTH (Apr. 18, 2023), <https://www.tradesecretslaw.com/2023/04/articles/intellectual-property/spilling-secrets-to-ai-does-chatting-with-chatgpt-unleash-trade-secret-or-invention-disclosure-dilemmas/>. This case turns on a variation on reasonable efforts, the difficulty in locating the information, and access to information by competitors which could, in limited circumstances, shield the sloppy trade secret holder from losing protection through ChatGPT. *Id.* For discussion of ChatGPT’s ability to share trade secrets in query responses, see *infra* Part II.

respond to a query – is also largely a mystery. As one AI expert recently explained in an interview about how Generative AI works,

[We] don't really know what [systems like ChatGPT] are doing in any deep sense. If we open up ChatGPT or a system like it and look inside, you just see millions of numbers flipping around a few hundred times a second, and we just have no idea what any of it means. With only the tiniest of exceptions, we can't look inside these things and say, "Oh, here's what concepts it's using, here's what kind of rules of reasoning it's using. Here's what it does and doesn't know in any deep way." We just don't understand what's going on here. We built it, we trained it, but we don't know what it's doing.²⁴

Thus, it seems that, as a matter of ChatGPT's own programming and the unknowns around the rules applied and how it responds, the risk of disclosure is real. Because ChatGPT (via OpenAI) can likely qualify as a "person" to be held liable under the UTSA,²⁵ ChatGPT's ability to aid in trade secret access, and possibility misappropriation – not to mention upending concepts of confidentiality, privacy and secrecy generally – is apparent.

Additionally, because ChatGPT can use the prompts themselves as part of its training data, revelation of a trade secret via ChatGPT could be the act that eliminates trade secret protection through disclosure. That would likely depend on whether ChatGPT gained access to trade secret information via "improper means" used by the individual or entity that shared it. Was it shared with ChatGPT accidentally or willingly by the trade secret owner, or was ChatGPT trained by an entity or individual that shared another's trade secret without the owner's permission? While the foregoing questions and others would matter greatly to the trade secret owner, the rest of society might collectively shrug at the possibility that a sloppy trade secret owner lost protection due to a careless act by one entrusted with protecting the trade secret from disclosure.

Lastly among the immediate concerns, beyond its ingestion and release of others' data, Generative AI has the potential to expand the range of trade secrecy itself.

²⁴ Noam Hassenfeld, *Even the scientists who build AI can't tell you how it works*, VOX (July 15, 2023, 7:00am), <https://www.vox.com/platform/amp/unexplainable/2023/7/15/23793840/chat-gpt-ai-science-mystery-unexplainable-podcast> (quoting New York University Prof. Sam Bowman).

²⁵ UNIF. TRADE SECRETS ACT § 1(3) (defining a "person" as "a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity").

Perhaps most strikingly, as discussed in more detail in Part II, code “optimization,” and activities like it, may also allow Generative AI to aid in the creation of *new* valuable information. Depending on how that information is viewed, managed, and used, these could be potential new trade secrets, and a vast expansion of our information ecosystem.

All these questions point to the impact of Generative AI on how trade secrets (and information broadly) are created, protected, and disseminated. These are new questions for which the law does not have straightforward answers (as arises whenever utterly new technology reaches the public). While the “reasonable efforts” issue is already here, trade secrecy faces new and more challenging questions because of the power of Generative AI to create information and speech that immediately collides with long-standing trade secrecy doctrine. What misappropriation looks like in such scenarios, and whether Generative AI manufactures conditions that raise countervailing speech concerns, is the focus of the remainder of this article.

B. Trade Secrets and Speech

“Commercial speech” generally occurs when the speaker “propose[s] a commercial transaction.”²⁶ Often, trade secrets are viewed as involving less protected “commercial speech,” in the sense that they involve commercial actors engaged in commercial transactions.²⁷ Additionally, as Pam Samuelson has explained, “Insofar

²⁶ *Bd. of Trs. v. Fox*, 492 U.S. 469, 482 (1989) (quoting *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council*, 425 U.S. 748, 762 (1976)).

²⁷ Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech: Is it Time to Restrain the Plaintiffs?*, 50 B.C. L. REV. 1425, 1437–38 (2009) (“The speech at issue in many trade secret misappropriation cases is not speech that is fully protected by the First Amendment. Trade secret cases involve a significant amount of commercial speech”). Rowe goes on to explain that speech “may be treated as commercial speech even if it both proposes a commercial transaction and addresses social or political issues.” *Id.* at 1438 n.70 (citing *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 66–68 (1983)). See also Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401, 1435–36 (2014) (“The general reluctance of courts to consider speech concerns in trade secret cases is perhaps attributable to a perception that trade secrets are property or ‘commercial’ speech, and thus less relevant to First Amendment interests.”); see also Janet Miranda, *Trade Secret Suit Against Ex-Worker Beats Free Speech Challenge*, BLOOMBERG LAW (July 20, 2022, 12:47 PM), <https://news.bloomberglaw.com/litigation/trade-secret-suit-against-ex-worker-beats-free-speech-challenge>.

as trade secret injunctions aim to stop private use or disclosure harmful to the plaintiff's economic interests, First Amendment interests are less weighty because the secrets are matters of private concern."²⁸

Given the predominant (if also debatable) perspective that trade secrecy involves commercial or private speech that has limited or no import beyond their commercial aspects and the actors involved, it is unsurprising that trade secrecy does not have principles like copyright's fair use defense baked into it.²⁹ After all, there is no need to balance trade secrecy's property and torts concerns³⁰ with a correlative speech protection when the speech is predominantly commercial and private.³¹ As a result, trade secrecy has historically been conceived as being, at best, unconcerned with the speech concerns of anyone other than the trade secret holder, and at worse (and more accurately) hostile to them.³² Thus, trade secrets are usually

²⁸ Pamela Samuelson, *Principles for Resolving Conflicts between Trade Secrets and the First Amendment*, 58 HASTINGS L. J. 777, 781 (2007); David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 149–50 (2007) [hereinafter *Secrecy and Unaccountability*] (quoting *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001), explaining that the United States Supreme Court equated trade secrets with “domestic gossip or other information of purely private concern”). *But see* Rowe, *supra* note 27, at 1438, n. 70 (“[m]erely because speech concerns a commercial subject, however, does not necessarily make it commercial speech for First Amendment purposes,” explaining that the “speech must be evaluated as a whole, including consideration of the purpose of the speech”); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 182–85 (1998) (arguing that property interests deserve no special deference under First Amendment doctrine). It is beyond the scope of this article to address whether this general assumption is correct or should be modified.

²⁹ Deepa Varadarajan has argued for the creation of such a fair use defense. *See* Varadarajan, *supra* note 27.

³⁰ *See* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 244 (1998) (explaining differences between trade secrecy and other intellectual property theories in that “the relational focus of trade secret’s liability rules align[] trade secret law more closely with the law of contract than with the law of property” even though “courts treat trade secret law as distinct from contract”).

³¹ *See* David Greene, *Trade Secrets, the First Amendment and the Challenges of the Internet Age*, 23 HASTINGS COMM. & ENT. L. J. 537, 549 (2001) (referencing prior cases where the Supreme Court did not consider “that a trade secret could be a matter of public interest”).

³² *See* *Secrecy and Unaccountability*, *supra* note 28, at 152 (“Thus, the right to trade secrecy protection is ‘defined by the extent to which the owner of the secret protects his interest from disclosure to other.’”).

impossible to access in the name of protecting the public interest or to share in the interest of informing the public on matters of significant concern.³³

But the practical realities aside for the moment, when the speech involves public policy like freedom of speech³⁴ or public interests like the operation of voting machines,³⁵ it is conceivable that the trade secrets at issue could be seen as being noncommercial speech, and thus as getting more than the comparatively limited constitutional protection offered to commercial speech, particularly when the trade secret information is in the hands of a third party that did not misappropriate the trade secret information at issue.³⁶ Alas, these situations have rarely been litigated

³³ See David S. Levine, *The Impact of Trade Secrecy on Public Transparency*, in *THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH* 1, 12–17 (Rochelle C. Dreyfuss and Katherine J. Strandburg eds., 2009), and the examples cited therein. See also *Secrecy and Unaccountability*, *supra* note 28, at 177–83, and the examples cited therein.

³⁴ See Adam W. Johnson, *Injunctive Relief in the Internet Age: The Battle Between Free Speech and Trade Secrets*, 54 *FED. COMM'NS L. J.* 517, 520 (2002) (“Except for a few narrow circumstances, the First Amendment protects speech from prior restraint.”). For examples of the “narrow” but critical scenarios where trade secret law prevailed over information access concerns, see Levine, *supra* note 33, at 27–28. See also Will Evans, *We Sued the Government for Silicon Valley Diversity Data*, *REVEAL* (Apr. 27, 2018), <https://revealnews.org/blog/we-sued-the-government-for-silicon-valley-diversity-data/> (demonstrating an example where large companies like Oracle were exempted from sharing diversity data to the Department of Labor under Exemption 4 of the Freedom of Information Act, which exempts companies from releasing information qualifying as a trade secret); *OFCCP Concur with Objections*, U.S. DEPARTMENT OF LABOR (Nov. 29, 2017), <https://www.documentcloud.org/documents/4448335-OFCCP-Concur-With-Objections.html>. Oracle later released its diversity numbers in 2020; Levi Sumagaysay, *Oracle Finally Releases Detailed Diversity Numbers, and They Aren't Great*, *MARKETWATCH* (Nov. 9, 2020, 6:58 PM), <https://www.marketwatch.com/story/oracle-finally-releases-detailed-diversity-numbers-and-they-arent-great-11604966287>.

³⁵ See *Secrecy and Unaccountability*, *supra* note 28, at 138.

³⁶ See Johnson, *supra* note 34, at 531 (“While some cases exist in which one party’s interest in trade secret protection prevails over First Amendment concerns, the majority of cases involving third parties unrelated to the trade secret holder are decided in favor of free speech concerns.”); see also Samuelson, *supra* note 28, at 843 (noting that the Restatement of Unfair Competition includes limiting language involving free speech when it comes to public interest issues like health). See Levine, *supra* note 33, at 8–9. While the language sounded promising, the intervening years have proven that the Restatement’s language has had little influence. Courts regularly deny access to trade secrets despite the arguable public interests involved. See David S. Levine, *The Impact of Trade Secrecy on Public Transparency*, *THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH* (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2010) (noting several examples);

because of the significant hurdles that must be jumped to even gain access to relevant trade secret information or even know that it exists, in order to share it. More frequently, these concerns have been generally raised through efforts to access the information via freedom of information litigation,³⁷ rather than after the information has been accessed or disseminated (and from the trade secret owner's perspective, after the harm has been suffered).

Unlike prior technologies like the internet itself, Generative AI operates in each element of trade secret development and monetization: research, creation, access, and use. Because ChatGPT creates content with relative ease, Generative AI has the potential to make these conflicts more common. Combined with its proven ability to respond to queries in seconds, the speed with which information may be created and disseminated opens new avenues of challenge and opportunity.

As alluded to above, Generative AI creates a new and groundbreaking mechanism for not only trade secret dissemination, but also trade secret creation. Commentators have theorized how AI can create value, explaining that "it is applicable in almost any given data-relevant context, provides some sort of value (either through the manipulation of the data or generating results within its context), and allows for more and more automation and insights derived from the data."³⁸ Generative AI massively expands AI's capabilities by adding the research capacity to generate information in usable, creative, and efficient forms. This is exactly the kind

see also Julie Zink, *When Trade Secrecy Goes Too Far: Public Health and Safety Should Trump Corporate Profits*, 20 VAND. J. ENT. & TECH. L. 1135, 1176 (2018) ("However, when trade secrets endanger others, broader public interests are at issue. Public health should take priority over commercial interests.").

³⁷ These actions (and indeed, any actions involving disclosure of a trade secret without the permission of the trade secret holder) generally fail due to overwhelming interest in protecting trade secrets from misappropriation, combined with a reticence to interrogate whether the subject information is even a trade secret in the first instance. See, i.e., Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1364 (2018) ("[d]efendants have struggled unsuccessfully to overcome claims to a trade secret evidentiary privilege even at trial, where their procedural rights are strongest"); Bambauer, *supra* note 9, at 846 ("Courts [considering trade secret rights] tend to invoke the property label or condemn unfair business practices without any real analysis—the conclusion is treated as self-supporting.").

³⁸ Mathieu Lemay, *How Does Artificial Intelligence Create Value?*, TOWARDS DATA SCIENCE (Sept. 1, 2021), <https://towardsdatascience.com/how-does-artificial-intelligence-create-value-bec14c785b40>.

of research and development information that companies regularly hold as trade secrets.³⁹

McKinsey & Company has identified Generative AI's role in R&D—where trade secrecy is dominant⁴⁰—as under-explored and not well recognized.⁴¹ Yet, it has reported that its “research indicates the technology could deliver productivity with a value ranging from 10 to 15 percent of overall R&D costs.”⁴² It explains the new area of “generative design,” unlocked by Generative AI:

[T]he life sciences and chemical industries have begun using generative AI foundation models in their R&D for what is known as generative design. Foundation models can generate candidate molecules, accelerating the process of developing new drugs and materials. Entos, a biotech pharmaceutical company, has paired generative AI with automated synthetic development tools to design small-molecule therapeutics. But the same principles can be applied to the design of many other products, including larger-scale physical products and electrical circuits, among others.⁴³

Research on challenges like candidate molecules, designs, and process innovations, are among many classic trade secrets because they derive their value by not being known by competitors.⁴⁴

³⁹ See Sinan Erkan, *Protection and Commercialization of Trade Secrets in R&D Collaboration Agreements: Biotechnology Industry*, HERDEM ATTORNEYS AT LAW, <https://herdem.av.tr/protection-and-commercialization-of-trade-secrets-in-rd-collaboration-agreements-biotechnology-industry> (last visited Aug. 3, 2023) (“The intrinsic value of trade secrets supports capital investment, acquisition and licensing of the potential invention, following a successful R&D collaboration”).

⁴⁰ Brandon Shackelford & John Jankowski, *Three-Quarters of U.S. Businesses that Performed or Funded R&D Viewed Trade Secrets as Important in 2018*, NAT'L CTR. FOR SCI. AND ENG'G STAT. (Sept. 2, 2021), <https://nces.nsf.gov/pubs/nsf21339> (“[m]ore companies viewed trade secrets as important than any other type of IP protection, with 51.7% of U.S. businesses that performed or funded R&D reporting trade secrets as very important to their company in 2018. . .”); see generally David S. Levine & Ted Sichelman, *Why Do Startups Use Trade Secrets?*, 94 NOTRE DAME L. REV. 751 (2019).

⁴¹ Michael Chui et al., *The Economic Potential of Generative AI: The Next Productivity Frontier*, MCKINSEY & COMPANY (June 14, 2023), <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier> (“Generative AI's potential in R&D is perhaps less well recognized than its potential in other business functions.”).

⁴² *Id.*

⁴³ *Id.*

⁴⁴ See Erik Weibust & Dean A. Pelletier, *Protecting AI-Generated Inventions as Trade Secrets Requires Protecting the Generative AI as Well*, IP WATCHDOG (July 24, 2022, 12:15 PM), <https://>

Thus, Generative AI increases exponentially both the opportunities and risks of trade secret creation. As public-accessible Generative AI engines like ChatGPT and Bard are rapidly disseminated and incorporated into all aspects of content generation, the ability of these technologies to incorporate proprietary information into their data and use it to create new information that might qualify as trade secrets is more than theoretical. Increased conflict with trade secret law and policy is inevitable. Particularly where trade secrets are either deliberately or accidentally

ipwatchdog.com/2022/07/24/protecting-ai-generated-inventions-trade-secrets-requires-protecting-generative-ai-well/id=150372/ (“[T]rade secret protection for AI-generated inventions may become more popular. Indeed, such an outcome is likely because the Defend Trade Secrets Act (DTSA), for example, can protect inventions and other information autonomously generated by AI.”); Arti K. Rai et al., *Pathways Across the Valley of Death: Novel Intellectual Property Strategies for Accelerated Drug Discovery*, 8 YALE J. HEALTH POL’Y L. & ETHICS 1, 4 (2008) (noting that “pharmaceutical firms . . . hold libraries of potentially useful small molecules as trade secrets, making them largely off limits to these same academic scientists”); *see also* Charles T. Collin-Chase, Kassandra M. Officer & Xirui Zhang, *Strategic Intellectual Property Considerations for Protecting AI Innovations in Life Sciences*, FINNEGAN (Jan. 2023), <https://www.finnegan.com/en/insights/articles/strategic-intellectual-property-considerations-for-protecting-ai-innovations-in-life-sciences.html> (“AI can use those data sets to predict which compounds might have desired chemical or biological properties, drastically reducing the time needed to identify candidates for further laboratory or clinical testing.”); Richard Stim, *Trade Secrets and Nondisclosure Agreements*, AIGA, https://www.aiga.org/sites/default/files/2021-02/trade_secrets.pdf (“For example, in 2014, Nike sued three former designers who had left the company, alleging they used Nike’s trade secrets for work they did for Adidas. Among the trade secrets allegedly taken were ‘specific designs, including models of team uniforms and products for the 2016 European Championships’”); *see also* Levine & Sichelman, *supra* note 40.

placed within the training data, and then shared with others,⁴⁵ we should expect challenges.⁴⁶

Lastly, aside from whatever guardrails may be programmed into Generative AI itself, computers generally lack the self-preservation instincts that humans might possess when faced with the possibility of a lawsuit⁴⁷ or prison⁴⁸ if they disclose trade secrets, even in a perceived public interest. In other words, computers could conceivably go forward undaunted by the traditional behavioral levers found in the law. These conditions could thrust the heretofore “rare”⁴⁹ form of trade secret

⁴⁵ See *infra* Part II for examples of this scenario already arising. As PC Magazine recently explained, “Based on information directly from the AIs themselves, ChatGPT and Bard use your prompts as input to further train their language models, while Bing AI does not.” Neil J. Rubenking, *Don’t Tell ChatGPT Anything You Wouldn’t Want to See on a Billboard*, PC MAGAZINE (May 15, 2023), <https://www.pcmag.com/news/dont-tell-chatgpt-anything-you-wouldnt-want-on-a-billboard>. That could change at any time, as explained below. It should surprise no one that filters are now being offered that block individuals from feeding private information into generative AI engines like ChatGPT. See Tara Seals, *PrivateGPT Tackles Sensitive Info in ChatGPT Prompts*, DARK-READING (May 2, 2023), <https://www.darkreading.com/application-security/privategpt-tackles-sensitive-info-chatgpt-prompts> (“Every time a user enters data into a prompt for ChatGPT, the information is ingested into the service’s . . . data set, used to train the next generation of the algorithm. The concern is that the information could be retrieved at a later date if proper data security isn’t in place for the service.”).

⁴⁶ See *infra* Part II; Anthony M. Insogna et al., *Trade Secrets and Generative AI: Protective Measures in an Evolving Technological Landscape*, MONDAQ (June 14, 2023), <https://www.mondaq.com/unitedstates/new-technology/1328978/trade-secrets-and-generative-ai-protective-measures-in-an-evolving-technological-landscape> (“There are three primary concerns with an employee’s input of company confidential or other sensitive information as a prompt into a generative AI application: (i) depending on the terms of the corresponding end-user license agreement (“EULA”), the company that supports the generative AI application can potentially review, release, or sell that sensitive information; (ii) the application itself can potentially reuse this sensitive information for third parties by training its responses with the sensitive information; and (iii) a third party may access the sensitive information if the company that supports the generative AI application has a security breach.”).

⁴⁷ See Jonathon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV., 1451, 1454–55 (2022) (“[T]he conventional understanding in law is that a chilling effect is when a person, deterred by fear of some legal punishment or privacy harm, engages in self-censorship.”).

⁴⁸ 18 U.S.C. § 1831; see UNIF. TRADE SECRETS ACT § 7(b)(3).

⁴⁹ Samuelson, *supra* note 28, at 840.

speech into the public square, forcing a conflict of values that we've rarely seen and for which we have no clear answers.

II. MUNDANE DESTROYER OF TRADE SECRETS: CHATGPT AND REASONABLE EFFORTS

The most urgent issue that trade secret holders must confront is how to keep their alleged trade secrets out of the “training data” that Generative AI uses to produce responses to queries. In theory, if the Generative AI does not have access to the information that would constitute another's trade secret, then the trade secret should not be at risk of being disclosed by the AI. However, keeping the AI away from that data may be harder than it sounds.

Initially, it is important to understand that—in relation to all companies except OpenAI and its partners—ChatGPT is, to use Larry Ellison's famous quote about cloud computing, “someone else's computer.”⁵⁰ Although trade secret law has historically been generous to trade secret holders who confront sneaky,⁵¹ sophisticated,⁵² or blatant⁵³ forms of misappropriation or corporate espionage, sharing your trade secret with a third party (like OpenAI) without a non-disclosure agreement in place (at least) would likely be a hornbook example of a non-reasonable effort to protect your secret. Because trade secret holders will increasingly be expected to understand the risks associated with sharing trade secrets with a third-party like OpenAI, the trade secret will increasingly be viewed as having been given away.⁵⁴

⁵⁰ Wayne Sadin, *History of Cloud Technology From a CFO's Perspective*, ACCELERATION ECONOMY (Apr. 13, 2023), <https://accelerationeconomy.com/financial-tech/history-of-cloud-technology-from-a-cfos-perspective/>.

⁵¹ *E.I. du Pont de Nemours & Co. v. Christopher*, 431 F.2d 1012, 1016 (5th Cir. 1970) (referring to defendants' actions as “nothing more than a school boy's trick”).

⁵² *Compulife Software, Inc. v. Newman*, 959 F.3d 1288, 1295 (11th Cir. 2020) (“There's nothing easy about this case. The facts are complicated, and the governing law is tangled. At its essence, it's a case about high-tech corporate espionage.”).

⁵³ *ClearOne Communs., Inc. v. Bowers*, 643 F.3d 735, 754 (10th Cir. 2011) (describing defendants as having “acted willfully and maliciously in misappropriating the Honeybee Code . . . and exhibited a ‘blatant disregard for clear duties’ owed to” the plaintiff).

⁵⁴ These issues have previously arisen in the context of storing trade secrets “in the cloud.” See Sharon Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, 19 VIRGINIA J. L. AND TECH. 1, 16 (2014) (“Without a binding promise of

Indeed, this problem has already arisen. The starkest example involves Amazon employees who apparently input Amazon's confidential information into ChatGPT to produce content relevant to the employees' Amazon jobs.⁵⁵ In the absence of a clear corporate policy regarding ChatGPT use, the problem fell to Amazon's in-house counsel to advise employees on how to manage ChatGPT after the fact. According to Business Insider, who reported the story in January 2023, the advice was clear: Don't do it. Counsel

warned employees not to provide ChatGPT with "any Amazon confidential information (including Amazon code you are working on)," . . . suggest[ing] employees follow the company's existing conflict of interest and confidentiality policies because there have been "instances" of ChatGPT responses looking similar to internal Amazon data.

"This is important because your inputs may be used as training data for a further iteration of ChatGPT, and we wouldn't want its output to include or resemble our confidential information (and I've already seen instances where its output closely matches existing material)," the lawyer wrote.⁵⁶

As Business Insider later pointed out, this problem is "particularly important for Amazon as its main competitor Microsoft has invested heavily in OpenAI."⁵⁷ In any other trade secret scenario, innocently (if sloppily) revealing trade secrets to a direct competitor would not only eviscerate the trade secret but would be viewed uncharitably, aside from sophisticated corporate espionage. ChatGPT, at least now, makes the seemingly salacious revelation of trade secrets to a direct and high-profile competitor almost comically mundane in its conception and practice.

Samsung has also run into a similar problem. According to PC Magazine,

confidentiality, companies that own trade secrets arguably waive the trade secrecy of stored information"); *but see supra* note 22 and Partow-Navid, *supra* note 23..

⁵⁵ Eugene Kim, *Amazon Warns Employees Not to Share Confidential Information with ChatGPT After Seeing Cases Where its Answer 'Closely Matches Existing Material' from Inside the Company*, INSIDER (Jan. 24, 2023, 2:15 PM), <https://www.businessinsider.com/amazon-chatgpt-openai-warns-employees-not-share-confidential-information-microsoft-2023-1>. Axios reports that companies "are struggling to figure out how to fold ChatGPT into their workflows without risking the security of their corporate secrets, customer information and intellectual property." Sam Sabin, *Companies are Struggling to Keep Corporate Secrets out of ChatGPT*, AXIOS (Mar. 10, 2023), <https://www.axios.com/2023/03/10/chatgpt-ai-cybersecurity-secrets>.

⁵⁶ Kim, *supra* note 55.

⁵⁷ *Id.*

One employee copied buggy source code from a semiconductor database into the chatbot and asked it to identify a fix Another employee did the same for a different piece of equipment, requesting “code optimization” from ChatGPT. After a third employee asked the AI model to summarize meeting notes, Samsung executives stepped in. The company limited each employee’s prompt to ChatGPT to 1,024 bytes.⁵⁸

ChatGPT denies any responsibility for remedying such behaviors, noting that “we are not able to delete specific prompts from your history” and advising users to not “share any sensitive information in your conversations.”⁵⁹ PC Magazine goes on to note that the Samsung employees’ queries leaked “corporate secrets that could be included in the chatbot’s future responses to other people around the world.”⁶⁰

Perhaps even more concerning, ChatGPT’s ability to reveal valuable information about a private entity based upon aggregation of data to which it has unrestricted access is particularly problematic. Aggregating non-trade secret information in a query response or text can garner insights that, under different circumstances, might constitute “combination trade secrets.” A “combination trade secret” is a “possible ‘unique’ or ‘improved’ combination of known information.”⁶¹

⁵⁸ Emily Dreibelbis, *Samsung Software Engineers Busted for Pasting Proprietary Code into ChatGPT*, PC MAG (Apr. 7, 2023), <https://www.pcmag.com/news/samsung-software-engineers-busted-for-pasting-proprietary-code-into-chatgpt>.

⁵⁹ *What Is ChatGPT?*, OPENAI, <https://help.openai.com/en/articles/6783457-what-is-chatgpt> (last visited Aug. 3, 2023).

⁶⁰ Dreibelbis, *supra* note 58.

⁶¹ Sharon K. Sandeen, *Through the Looking Glass: Trade Secret Harmonization as a Reflection of U.S. Law*, 25 B.U. J. SCI. & TECH. L. 451, 463 (2019). Another example of a “combination trade secret” would be flowcharts like those in *AirFacts, Inc. v. De Amezaga*, where the court found the flowcharts to be a combination of publicly available information displayed in a “painstaking, expert arrangement” making them “inherently valuable separate and apart from the publicly available contents” thus, necessitating trade secret protection. Allan E. Anderson & Linda M. Jackson, *Fourth Circuit Provides Guidance on Trade Secret Protection for Combinations of Public Information*, ARENTFOX SCHIFF (Dec. 12, 2018), <https://www.afslaw.com/perspectives/alerts/fourth-circuit-provides-guidance-trade-secret-protection-combinations-public>. Another example is the dog food in *Harrington-McGill v. Old Mother Hubbard Dog Food Co.*, the recipe for which was protected by trade secret law, not because of the ingredients themselves, but because of the “proportion of each ingredient to the others in the mix.” 22 Mass. App. Ct. 966, 966–67 (1986).

A classic example is the formula for Coca-Cola, which is derived from known ingredients (like sugar) but whose exact proportions are unknown.⁶²

Ana Nordberg has conceptualized the problem:

Data mining techniques and predictive algorithms are capable of revelling [sic] undisclosed personal and business information even when all possible efforts are made to keep it secret. For example, studies claim to be able to detect sexual orientation by analysis of photos posted on social media; criminal tendencies; political ideas; suicide prevention algorithms; pregnancy detection. It is not farfetched to imagine that correlating information from multiple sources, might reveal valuable information concerning strategic market positioning decisions and on-going research projects. Information on pricing, client list, suppliers, distribution routes and networks, manufacturing capability and processes can also likely be inferred.⁶³

Nordberg's analysis pre-dates ChatGPT's launch; adding the ability to render this information as speech based upon a human's query, in a matter of minutes, makes the threat to trade secrecy far more acute.

That it is so easy for ChatGPT to share information with a third party that incorporates input by a trade secret holder, either directly or through creation of new combination trade secrets, is only one challenge. According to TechCrunch, OpenAI announced in March 2023 that it "won't use any data submitted through its API for 'service improvements,' including AI model training, unless a customer or organization opts in."⁶⁴ In contrast, information shared with OpenAI via ChatGPT will be used unless a user opts out.⁶⁵ Given that query inputs are the current

⁶² Tait Graves & Alexander Macgillivray, *Combination Trade Secrets and the Logic of Intellectual Property*, 20 SANTA CLARA HIGH TECH. L. J. 261, 270 (2004) ("Nobody would seriously dispute the claim that Coca-Cola owns the chemical formula by which it creates its soft drink from common ingredients, and nobody would seriously claim that because those ingredients are known, the exact proportions at which the elements are chemically combined do not constitute a secret.").

⁶³ Ana Nordberg, *Trade Secrets, Big Data and Artificial Intelligence Innovation: A Legal Oxymoron?*, in *THE HARMONIZATION AND PROTECTION OF TRADE SECRETS IN THE EU: AN APPRAISAL OF THE EU DIRECTIVE* (Jens Schovsbo, Timo Minssen & Thomas Riis eds., 2020).

⁶⁴ Kyle Wiggers, *Addressing Criticism, OpenAI Will No Longer Use Customer Data to Train its Models by Default*, TECH CRUNCH (Mar. 1, 2023, 1:00 PM), <https://techcrunch.com/2023/03/01/addressing-criticism-openai-will-no-longer-use-customer-data-to-train-its-models-by-default/>.

⁶⁵ Laura Dobberstein, *Samsung Reportedly Leaked its Own Secrets Through ChatGPT*, THE REGISTER (Apr. 6, 2023, 5:27 PM), https://www.theregister.com/2023/04/06/samsung_reportedly_leaked_its_own/.

means by which users tend to engage ChatGPT, it's no surprise that OpenAI's voracious need for data puts the onus on the user to opt out.⁶⁶

However, whether any of these policies mean that ChatGPT would not reveal and share trade secrets will remain an open question because OpenAI is, ironically, a "black box."⁶⁷ Despite its name, OpenAI's systems are held as trade secrets⁶⁸ (and presumably will be so long as they remain secret and valuable), meaning that no one beyond those with access to and understanding of the systems would be able to ascertain exactly how others' trade secrets are used, if at all. The effect is that trade secret holders cannot verify that whatever information is shared with ChatGPT will not wind up in its training data and shared, despite OpenAI's statements to the contrary. Indeed, it is unknown how the data might even be used. In the absence of transparency⁶⁹ or explanation,⁷⁰ neither of which is required under US law, it is a matter of trust in OpenAI (or not) that trade secret information, once made accessible, will not be spit back to others.⁷¹

⁶⁶ *What Is ChatGPT?*, OPENAI, <https://help.openai.com/en/articles/6783457-what-is-chatgpt> (last visited Aug. 3, 2023) (stating explicitly that "[y]our conversations may be reviewed by our AI trainers to improve our systems").

⁶⁷ See FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* (2015).

⁶⁸ OPENAI, *GPT-4 Technical Report 2* (Mar. 27, 2023), <https://cdn.openai.com/papers/gpt-4.pdf> ("Given both the competitive landscape and the safety implications of large-scale models like GPT-4, this report contains no further details about the architecture (including model size), hardware, training compute, dataset construction, training method, or similar.").

⁶⁹ *Secrecy and Unaccountability*, *supra* note 28, at 172 ("In the absence of adequate information, the public regularly uses infrastructure with limited or no knowledge as to how it operates and how that form of operation impacts our daily lives."); see also David S. Levine, *The People's Trade Secrets*, 18 MICH. TELECOMM. & TECH. L. REV. 61, 95 (2011) [hereinafter, *People's*] ("The public has a general right to know governmental information unless a specified exemption from disclosure applies.").

⁷⁰ See Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L. J. 189, 213 (2019) ("Communication to individuals about algorithmic decision-making must thus be simultaneously understandable (or 'legible'), meaningful, and actionable.").

⁷¹ See Lilian Edwards & Michael Veale, *Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?*, IEEE SECURITY & PRIVACY 46, 46–54 (2018) (arguing that both are inadequate, and call directly for better decisions from algorithms).

Of course, there's also no reason to assume that any of these policies will remain static.⁷² As the history of the Internet has shown, companies can and do change their information policies at will, and often with little or no notice.⁷³ One can assume that OpenAI's interests in improving its speech results will prevail long-term over protecting the interests of a sloppy trade secret owner. As The Verge has reported, "If it's learning from user input, it'd be a bad idea to input trade secrets, as there's always the possibility that it could spit that data back out to someone else."⁷⁴

Lastly, because trade secret information can be found in hidden corners of the internet, and not easily found even by search engines,⁷⁵ it is conceivable that the extraneous and obscure accidental disclosure could come back to haunt trade secret holders through speech generated by ChatGPT, based upon a third-party's prompt.⁷⁶ As a practical matter, a trade secret that is publicly accessible but hard to find might still retain value because it isn't known by competitors. However, if that

⁷² Of course, given that OpenAI is a private company, such policies could change at any time, and perhaps without notice. As the research collective Team8 recently explained, "[Generative AI] platforms may choose to use user input to train future models, but that doesn't seem to be the case now." Team8, *GENERATIVE AI AND CHATGPT ENTERPRISE RISKS 12* (Apr. 2023), <https://team8.vc/wp-content/uploads/2023/04/Team8-Generative-AI-and-ChatGPT-Enterprise-Risks.pdf>.

⁷³ See Tulie Finley-Moise, *Why Is Everyone Updating Their Privacy Policy (and What to Look For)?*, HP TECH TAKES (June 30, 2019), <https://www.hp.com/us-en/shop/tech-takes/updating-privacy-policy>.

⁷⁴ Mitchell Clark, *OpenAI Announces an API for ChatGPT and its Whisper Speech-to-Text Tech*, THE VERGE (Mar. 1, 2023, 3:39 PM), <https://www.theverge.com/2023/3/1/23620783/chatgpt-api-openai-pricing-whisper>.

⁷⁵ See David S. Levine, *The Social Layer of Freedom of Information Law*, 90 N.C. L. REV. 1687, 1711–21 (2012); see also *Help Center*, GOOGLE, <https://support.google.com/webmasters/answer/7474347?hl=en> (last visited Aug. 3, 2023) (explaining how a search engine like Google provides results via web crawling and indexing automation); Partow-Navid & Salinas, *supra* note 23 ("The court noted, however, '[p]ublication on the Internet does not necessarily destroy the secret if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people'). *But see* Masimo Corporation, Cercacor Laboratories, Inc. v. True Wearables, Inc., Marcelo Lamego, 2022 U.S. App. LEXIS 1923 (Fed. Cir. Jan. 24, 2022) (concluding that the public disclosure of a trade secret did not prevent trade secret assertion under CUTSA where relevant market actors did not know about information).

⁷⁶ See Sam Sabin, *Companies Are Struggling to Keep Corporate Secrets Out of ChatGPT*, AXIOS (Mar. 10, 2023), <https://www.axios.com/2023/03/10/chatgpt-ai-cybersecurity-secrets>.

hard-to-find publicly available trade secret is in ChatGPT's training data, its obscurity on the Internet may be practically meaningless since it could be used and shared by ChatGPT in response to another user's prompt.

As a result, secrecy may be thwarted by a trained AI that can find and process vast quantities of information and data at a speed no other computer could match. By the time a trade secret holder realized that "reasonable efforts" had been thwarted or failed outright, the speech including the secret information could already be in the possession of unknown third parties, who would be under no duty to the trade secret owner to conceal the information. The trade secret would, for all practical purposes, be no more.⁷⁷

III. SUPERCHARGED REPORTER, CIVIL SOCIETY WATCHDOG, OR WHISTLEBLOWER: CHATGPT AND SPEECH OF PUBLIC INTEREST

As Derek Bambauer has written, "Perhaps the greatest risk to trade secret is when it clashes with free speech."⁷⁸ ChatGPT presents a new front for trade secret owners to protect, and one that may be impossible to defend against free speech values. The fact that OpenAI has recently announced that it will allow integration of ChatGPT into third party applications will likely further accelerate ChatGPT's power and its risks, with The Verge noting that this "could be the moment the floodgates open."⁷⁹

What might those floodgates look like in the context of protected speech involving trade secrets? Consider three scenarios in which trade secret information might be of interest to those beyond competitors. These situations have one important trade secret fact in common: The recipient of the information is a third party with no duty of confidentiality to the trade secret holder. All such situations invoke the battle between trade secrecy's protection of the owner's property and unfair competition interests versus the public's interest in information and speech.

A. News Media

The first, and most obvious, arises from the disclosure of trade secret information or insights to a reporter. While the press obviously has strong free speech

⁷⁷ See Rowe, *supra* note 27, at 1450 (noting that once a trade secret is on the Internet, there is no effective remedy).

⁷⁸ Bambauer, *supra* note 9, at 846.

⁷⁹ Clark, *supra* note 74.

protection,⁸⁰ even that can be overcome by trade secrecy policy.⁸¹ However, as previously noted, the situation may be significantly simpler to address if the source of the information is ChatGPT.

An illustrative example of how this might play out involves the seminal case *Religious Technology Center v. Lerma*.⁸² Samuelson wrote about *Lerma*, where the Church of Scientology brought a trade secret misappropriation action against The Washington Post for publishing Scientology texts that were alleged trade secrets.⁸³ The claim failed based upon what Samuelson called “accidental disclosure,” namely the filing of the information in a court clerk’s office without a protective order in place. As such, there was “nothing illegal or unethical” about the newspaper’s acquisition of the information from the court’s file.⁸⁴ Samuelson explained,

The court in *Lerma* did not need to invoke the First Amendment in support of its ruling because an internal limiting principle . . . of trade secrecy law adequately protected the First Amendment interests of the Washington Post, its reporters, and readers eager to know about Scientology practices. Had the court concluded that the Post’s knowledge of RTC’s proprietary claim sufficed to establish trade secret liability, the Post could have invoked the First Amendment as a basis for defending against RTC’s trade secret claims.⁸⁵

In other words, the “leakiness”⁸⁶ (as Samuelson labels it) of trade secrecy arises from the law’s unwillingness to protect trade secret holders from the misfortune of

⁸⁰ See Geoffrey R. Stone & Eugene Volokh, *Freedom of Speech and the Press*, NAT’L CONST. CTR, <https://constitutioncenter.org/the-constitution/amendments/amendment-i/interpretations/266> (last visited Aug. 3, 2023).

⁸¹ Bambauer, *supra* note 9, at 847 (explaining that “[a]n increase in trade secret protection” would lead to “inevitable” clashes between trade secrecy and First Amendment protections). For example, where “[a] whistleblower, who made [a trade secret] public—or a newspaper that published it—might be held liable for misappropriation, perhaps even facing an injunction against further distribution.” *Id.* See also *Secrecy and Unaccountability*, *supra* note 28, at 168–70; *DVD Copy Control Assn., Inc. v. Bunner*, 31 Cal. 4th 864, 887 (Cal. 2003) (“[T]he preliminary injunction at issue here is not a prior restraint. The injunction is content neutral, and the trial court found that Bunner had previously disclosed DVD CCA’s trade secrets in violation of California law.”).

⁸² 908 F. Supp. 1362 (E.D. Va. 1995).

⁸³ Samuelson, *supra* note 28, at 785.

⁸⁴ *Id.* (quoting *Lerma*).

⁸⁵ *Id.*

⁸⁶ *Id.*

disclosure deemed accidental on their part and not “improper.” This comports with both trade secrecy’s underlying policies as well as the First Amendment’s.⁸⁷ ChatGPT amplifies the leakiness challenge.

ChatGPT has already engendered such accidents, as the Amazon example from Part II indicates. It seems likely that a court faced with a trade secret misappropriation claim by Amazon (or Samsung for that matter) would follow a similar analytical thread to the one in *Lerma*. Like access from a court file, a reporter accessing Amazon’s or Samsung’s trade secrets via ChatGPT is engaging in similar behavior: accessing information as a third party in a legitimate way, with no duty of confidentiality owed to the trade secret holder. That Amazon or Samsung may wish for that information to be kept confidential is, to put it directly, not the media’s problem.⁸⁸ The ease with which an industrious reporter could access that information through smart querying, from the convenience of their home using a mobile device, only exacerbates the risk.

B. Whistleblowers

Generative AI could also be a highly effective tool for whistleblowers. The passage of the Defend Trade Secrets Act created the first limited protection for whistleblowers in United States trade secret law.⁸⁹ The new law, which has rarely been

⁸⁷ *Id.*

⁸⁸ Whether OpenAI would be able to avail itself of protection in a trade secret misappropriation claim is an issue beyond the scope of this paper. The question would implicate questions of secondary and racketeering liability, Section 230 of the Communications Decency Act, and whether the action was brought under the DTSA or another statute. See, e.g., Beatriz Botero Arcila, *Is it a Platform? Is it a Search Engine? It’s ChatGPT! A Commentary on the Liability Regime of Online Content Generated by Large Language Models in Europe*, 3 J. FREE SPEECH L. 455 (2023); Matt Perault, *Section 230 Won’t Protect ChatGPT*, 3 J. FREE SPEECH L. 363 (2023); Eugene Volokh, *Large Libel Models? Liability for AI Output*, 3 J. FREE SPEECH L. 489, 494–98 (2023).

⁸⁹ Sharon Sandeen & Christopher B. Seaman, *Toward a Federal Jurisprudence of Trade Secret Law*, 32 BERKELEY TECH. L. J. 829, 852–53 (2017). See Peter S. Menell, *The Defend Trade Secrets Act Whistleblower Immunity Provision: A Legislative History*, 1 BUS., ENTREPRENEURSHIP & TAX L. REV. 398, 401–03 (2017) (identifying Dr. Jeffrey Wigand, a whistleblower on the tobacco industry’s nicotine research in the 1990s, as a prologue to analyzing the DTSA’s legislative history); Kathleen Day, *U.S. Attorney Probing Xerox Accounting*, WASH. POST (Sep. 25, 2002) (referencing James Bingham, a former Xerox Assistant Treasurer, who brought up “significant accounting and financial reporting irregularities” at the company and was fired for whistleblowing Xerox’s financial practices).

tested,⁹⁰ gives some protection to whistleblowers who report trade secret information to law enforcement or who use such information in a lawsuit to enforce law.⁹¹ To the extent that a determined whistleblower wanted to gather information in an intelligible way through targeted queries, as discussed in Part II, ChatGPT could be a useful (and legal) tool.⁹² Whether by gleaning information from data revealed through queries or deduced from combinations of heretofore uncorrelated material, the person who knows what they seek might find Generative AI's information aggregation abilities quite compelling.

Moreover, Generative AI could render the information more understandable and usable for such a purpose.⁹³ Once so gathered, the information might be further disseminated under the free speech principles that exist for information of public interest.⁹⁴ To the extent that a whistleblower can tell a compelling story to the press, regulators, and law enforcement with the aid of Generative AI, it becomes a powerful tool in the whistleblower's arsenal.

C. *Civil Society Watchdogs*

Perhaps the biggest challenge related to trade secret law and speech arises when watchdogs, activists, and civil society groups want access to trade secrets in order to assess and publicize risks to the public.⁹⁵ Ranging from voting machine code to the formula for chemicals in hydraulic fracturing to, yes, OpenAI's code, many outside groups have interests in secret privately-held information that does not implicate competition in the marketplace.⁹⁶ Unlike the press or even whistleblowers, these organizations do not generally enjoy free speech protections more powerful

⁹⁰ See *Unum Grp. v. Loftus*, 220 F. Supp. 3d 143 (D. Mass. 2016); *Christian v. Lannett Co.*, No. 16-963, 2018 U.S. Dist. LEXIS 52793 (E.D. Pa. Mar. 29, 2018).

⁹¹ 18 U.S.C. § 1833.

⁹² See *supra* note 56 and accompanying text, regarding corporate efforts to prevent trade secrets from being ingested by ChatGPT and thus to prevent their disclosure to others via queries.

⁹³ See *supra* note 43 and accompanying text, discussing "generative design."

⁹⁴ See *Government Restraint of Content of Expression*, JUSTIA, <https://law.justia.com/constitution/us/amendment-01/16-government-restraint-of-content-of-expression.html> ("[t]he teaching of [*New York Times Co. v. Sullivan*] and the cases following it is that expression on matters of public interest is protected by the First Amendment").

⁹⁵ *Secrecy and Unaccountability*, *supra* note 28, at 171–72.

⁹⁶ *Id.*; Levine, *supra* note 69, at 96–98; David S. Levine, *Confidentiality Creep and Opportunistic Privacy*, 20 TUL. J. TECH. & INTELL. PROP. 11, 24–28 (2017) [hereinafter *Confidentiality*].

than trade secrecy. As a result, they run the risk of being viewed and held as trade secret misappropriators if they disclose such information. The impetus, therefore, is to not publicize their findings as there is no existing statutory protection for possessing trade secrets for these reasons.⁹⁷ Moreover, they rarely, if ever, gain such access absent massive political pressure⁹⁸ or the occasional accident.⁹⁹

ChatGPT's easy means of generating speech removes significant structural barriers to information access and dissemination for such organizations, which are usually strapped for resources. On the assumption that a Generative AI may be trained on information that it gathers from trade secret holders that have shared sensitive information with it, an industrious researcher could create useful prompts to find such information. Generative AI's ability to create useful prose out of combined information could lead to identifying combination trade secrets that offer additional insights. Finally, the aggregation of massive troves of data might lead a knowledgeable researcher to other sources of information and additional avenues of exploration.

The legal risks inherent in such behavior remain to be seen. At least as of this writing, there are no known legislative efforts in the United States designed to afford these entities more protection from liability were they to reveal trade secrets. Thus, the power of Generative AI as a creative and disclosure tool drives head-on into law that has little sympathy for civil society groups who may be tempted to use these tools for public and advocacy purposes. Whether civil society groups will take such risks is unknown, but worthy of close attention if they do.

⁹⁷ Levine, *Confidentiality*, *supra* note 94, at 22; *see also* Jonathan Fox, *Accountability Keywords*, ACCOUNTABILITY RESEARCH CENTER 1, 104 n. 76 (Jan. 2022) https://www.corruptionwatch.org.za/wp-content/uploads/2022/12/Working-Paper-11_Keywords_May-24.pdf (“Watchdog organizations also contribute to law enforcement by playing a Sherlock Holmes detective role to independently gather ‘smoking gun’ evidence, as in the case of the Environmental Investigation Agency”).

⁹⁸ Levine, *Confidentiality*, *supra* note 94, at 37; *see also* *Energy in Depth*, INDEP. PETROLEUM ASS'N OF AMERICA, <https://www.energyindepth.org/about/> (last visited Aug. 3, 2023).

⁹⁹ *See* Priya Singh, *Samsung Employees Accidentally Leaked Company Secrets Via ChatGPT: Here's What Happened*, BUSINESS TODAY (Apr. 13, 2023, 4:32 PM), <https://www.businesstoday.in/technology/news/story/samsung-employees-accidentally-leaked-company-secrets-via-chatgpt-here-what-happened-376375-2023-04-06>.

IV. WHERE ARE WE HEADED?

Twenty-two years ago, a commentator at the dawn of the commercial Internet wrote, “Trade secrets are not exempt from the First Amendment. As a result, a party seeking to enjoin the publication of trade secrets, especially by one who owes no duty of confidentiality to the owner of the trade secret, faces a considerable challenge.”¹⁰⁰ Generative AI, as embodied by ChatGPT, creates numerous possibilities for third parties to gain access to trade secret information with similar lack of duty to maintain confidentiality. At the same time, the law remains largely unsympathetic to those interests in the face of someone disclosing an actual trade secret (as opposed to information labeled a “trade secret” that, in fact, is not actually “secret”). Therefore, Generative AI is the most significant technological development and challenge for trade secret law and policy since the advent of the commercial Internet.

In a world in which hyperbolic language is endemic, it is not an overstatement to describe the release of ChatGPT as potentially cataclysmic for humanity. It is unclear who the winners will be, beyond investors and owners of AI technology who will make extraordinary profits.¹⁰¹ The losers are, yet, unknown; and of primary concern, we have limited ability to predict outcomes for a technology whose decision-making methods are not completely understood even by their human creators. Nonetheless, we shall soon begin seeing clear winners and losers, as we are engaged in an uncontrolled experiment with the technology on a global scale.

For trade secrecy, Generative AI raises the specter of “cheap creativity” as described by Burk.¹⁰² If Generative AI can create information in minutes that would previously have taken years of research and lead-time advantages to create, where does that leave trade secret law, or even the need for trade secrets?¹⁰³ Closer to the

¹⁰⁰ Greene, *supra* note 31, at 561.

¹⁰¹ To the extent that Generative AI’s users benefit from the technology’s ability to render serviceable (or better) copy quickly, they may be winners in the short-term. Medium- and long-term, they could be working themselves out of employment as the technology improves through their use to match or eclipse their abilities. This is another issue on which we can only speculate as of this writing.

¹⁰² Burk, *supra* note 7, at 1673.

¹⁰³ This is the focus of this author’s next project, which assesses how information generated by AI should be theorized and treated in the context of information law and policy generally.

focus of this paper, how will newsgathering, watchdogging, and whistleblowing about controversial and secret behaviors be transformed by cheap and powerful content machines like ChatGPT that can draw on vast quantities of data to provide content? Will Generative AI be able to create images or graphics that hint at, or clearly reveal or explain closely held secrets, and explain them better than any human might easily conceive?¹⁰⁴

All of us are now forced to grapple with these questions and countless more. As explained by Business Insider, Generative AI’s “rapid proliferation has the potential to upend a number of industries, across media, academics, and healthcare, precipitating a frenzied effort to grapple with the chatbot’s use-cases and the consequences.”¹⁰⁵ It remains to be seen whether OpenAI’s unilateral November 30, 2022, decision will be viewed as a blessing, or a grave error. The most likely outcome is that we will witness a mix of good and bad, as has been the case with all recent technologies—but only time will tell, while we frantically try to figure out where we are, how we got here, and where we are going.¹⁰⁶

CONCLUSION

Generative AI’s immediate power has caught most experts by surprise—at least those who were not privy to what was happening at OpenAI. One person with preferred access was apparently Bill Gates, who wrote that it was “stunning” to observe ChatGPT answer (in September 2022) 59 of 60 AP Biology test multiple choice questions correctly, followed by giving advice to a father about what to say to a sick child. Gates was at the helm at Microsoft when it made a \$1 billion investment in

¹⁰⁴ See Chui et al., *supra* note 41 (“The latest generative AI applications can perform a range of routine tasks, such as the reorganization and classification of data. But it is their ability to write text, compose music, and create digital art that has garnered headlines and persuaded consumers and households to experiment on their own.”). See also Insogna, *supra* note 46.

¹⁰⁵ Kim, *supra* note 55.

¹⁰⁶ Greg Brockman, President of OpenAI, was recently quoted as saying, “We’re not just sitting in Silicon Valley thinking we can write these rules for everyone”— “[we’re] starting to think about democratic decision-making.” Brian O’Connell, *ChatGPT May Undergo a Massive Overhaul*, THE STREET (May 23, 2023, 10:20 AM), <https://www.thestreet.com/technology/chatgpt-may-undergo-a-massive-overhaul>. That’s a step in the right direction but it would have been better to have made that decision before ChatGPT was made available for wide use and the harms already began to occur, as this article (and other articles in this symposium) indicate.

OpenAI; after Gates stepped down, Microsoft announced in January 2023 that it was making a \$10 billion follow-up investment.

It does not take any great intellectual leap to surmise how Gates has been able to authoritatively declare generative AI's groundbreaking abilities and confidently predict its future. While they were certainly self-serving proclamations, he had a head start on conceiving where generative AI might be going because his investment in OpenAI was likely precipitated by access to OpenAI's trade secrets, including the September 2022 private demonstration—a trade secret at the time. Now that all of us can see what ChatGPT can do, if not how it does it (although it has already been somewhat duplicated via reverse engineering¹⁰⁷), the era of AI trade secret misappropriation and newly protected speech aided, and even created, by Generative AI has also dawned—whether we like it or not.

¹⁰⁷ Ameya Paleja, *Alpaca AI: Stanford Researchers Clone ChatGPT AI for Just \$600*, INTERESTING ENG'G (Mar. 21, 2023, 6:45 AM), <https://interestingengineering.com/innovation/stanford-researchers-clone-chatgpt-ai>. The problems associated with OpenAI's code being protected as a trade secret raise issues of accountability, verifiability, and trust, but are beyond the scope of this Article.