AI SECRETS REGISTRATION

*Yang CHEN**

ABSTRACT

The surprisingly rapid development of Artificial Intelligence ("AI") and its increasingly sweeping use across industries are testing the resilience of traditional intellectual property doctrines. Trade secret law is equally experiencing a doctrinal reshuffle as it becomes an important mechanism for protecting what this Article terms "AI secrets." While this protection incentivizes continuous innovation and sustains long-term investment, firms' unrestrained reliance on trade secrecy poses a pressing issue: it legally constructs an opacity that severely exacerbates AI transparency concerns and constrains meaningful stakeholder scrutiny.

Current scholarship and regulatory responses primarily rely on mandated-disclosure approaches to reconcile this tension. However, this Article argues that these approaches are inherently limited because the conflict between AI secrets and transparency is rooted in the structural features of trade secret law itself—notably, the inherent indeterminacy of its scope. Because the boundaries of protectable trade secrets are not fixed ex ante *but are instead determined only through* ex post *judicial decisions, firms can unilaterally overclaim secrecy, effectively shielding even non-secret information from public scrutiny unless and until a court intervenes.*

To address these structural failures and supplement current regulatory approaches, this Article proposes a structural redesign of trade secret law when applied to AI secrets: a formal AI secrets

---

* Ian Yang Chen, S.J.D., LL.M., University of Pennsylvania Carey Law School; Assistant Professor, School of Law, City University of Hong Kong. Thank you for the comments, suggestions, and support from Gideon Parchomovsky, John Villasenor, Guobin Cui, Jyh-An Lee, Peter Yu, Tanya Aplin, Ebers Martin, Josef Drexl, Ruth Okediji, Xin Dai, Xiaodong Ding, Tianxiang He, Shu Li, Jingzhou Sun, Zishuo Li, and other participants in the 2026 Conference of "The Digital Shift: Redefining Global Value Chains in a Connected World" and Leuven IP and AI Conference 2026. Thanks for Yixuan Bai's excellent research assistance throughout. All errors are my own.

registration system. Drawing on comparative insights from existing registration, recordation, and third-party review mechanisms in representative jurisdictions, specifically the U.S. copyright registration system, China's local data registration systems, and the European Union's AI and data governance frameworks, this Article develops a conceptually grounded and pragmatically adaptable proposal. Ultimately, this foundational framework aims to facilitate future global implementation, offering a viable structural solution to resolve the transnational tension between AI secrecy and transparency demands while achieving ancillary benefits.

TABLE OF CONTENTS

INTRODUCTION 760
I. TRADE SECRECY AND AI SECRECY 767
A. The Law of Trade Secrets 767
B. AI Secrets 771
II. AI SECRETS AND TRANSPARENT AI 776
A. Public Authority Delegation and the "Secret Governance" 778
B. Private Harms and Accountability 780
C. Current Focuses and Responses 784
III. AI TRANSPARENCY CONCERNS: THE STRUCTURAL FAILURE OF TRADE SECRET LAW 787
A. Structural Features: Resilience and Flexibility in Trade Secret Law 788
B. The Structural Failures: Inherent Susceptibility to Strategic Overclaiming 789
IV. AI SECRETS REGISTRATION 795
A. AI Secrets Registration System 795
1. Applicable Scope 795
2. Registration System 796
3. Legal Effects of (Non)Registration 799
4. Disclosure, Public Scrutiny, and Register's Duties 801
B. Addressing Structural Failures, Achieving Allied Benefits .804
C. Limitations and Future Directions 808
CONCLUSION 810

INTRODUCTION

The surprisingly rapid development of Artificial Intelligence ("AI"), particularly the generative AI and its increasingly sweeping use across industries, are giving rise to unprecedented legal challenges, test-

ing, and in some respects threatening, the resilience of traditional legal doctrines across multiple fields of law. For instance, generative AI is claimed to have turned copyright law upside down, rendering any straightforward applications of traditional doctrines, such as human authorship, originality, and fair use, considerably more difficult.[1] Deepfakes, powered by AI, are threatening not just the individual personality rights but also more systematic harms on the whole society.[2] Patent law is facing its own distinct doctrinal collapse, in part because of the mounting involvement of AI in the innovation process.[3] Though trademark law appears relatively more distant from AI, some have worried that AI, by significantly lowering information costs for consumers, might supplant the source-identifying function of trademarks, rendering many trademarks "superfluous."[4]

Trade secret law, a relatively less developed member of the intellectual property ("IP") family that has recently begun to attract increased

---

1. *See* Mark A. Lemley, *How Generative AI Turns Copyright Law Upside Down*, 25 COLUM. SCI. & TECH. L. REV. 190, 195-97 (2024); *see also* Matthew Sag & Peter K. Yu, *The Globalization of Copyright Exceptions for AI Training*, 74 EMORY L.J. 1163, 1176-77 (2025) (explaining copyright issues related to AI training); Dan L. Burk, *Cheap Creativity and What It Will Do*, 57 GA. L. REV. 1669, 1681-82, 1696-1700 (2023) (exploring how cheap creativity, if recognized by copyright law, may destroy the whole creative industry); Edward Lee, *Prompting Progress: Authorship in the Age of AI*, 76 FLA. L. REV. 1445, 1462-63 (2024) (describing the copyrightability of AI-generated works); Yang Chen, *Two Roads Diverge and Converge in the AI Era: Computer-Generated Works as an Exception for Human Authorship?*, 28 COLUM. SCI. & TECH. L. REV. (forthcoming) (manuscript at 9-11) (on file with the *Hofstra Law Review*) [hereinafter "Chen, *Two Roads*"] (highlighting AI copyrightability issues in different jurisdictions); Yang Chen, *Reviving 'Computer-Generated Works': Should Hong Kong Copyright Law Adapt the Rule to Harness AI Opportunities?* , 20 J. INTELL. PROP. L. & PRAC. 584, 588-90 (2025) [hereinafter "Chen, *Reviving*"] (describing AI copyrightability issues in Hong Kong); Tianxiang He, *Three Obstacles to AI-Generated Content Copyrightability*, 2026 SING. J. LEGAL STUD. 77, 95 (discussing copyrightability of AI-generated contents).

2. *See, e.g.*, Yang Chen, *Is Chinese Law Well-Prepared for AI Songs?: A Note of Caution on the Over-Expansion of Personality Rights*, 42 CARDOZO ARTS & ENT. L.J. 261, 285-88 (2024); Jane C. Ginsburg & Graeme W. Austin, *Deepfakes in Domestic and International Perspective*, 48 COLUM. J.L. & ARTS 297, 303-04 (2025); Victor Jiawei Zhang & Olivia Shuang Liu, *Deepfake & Deepfaith* 74 BUFF. L. REV. (forthcoming 2026) (manuscript at 1, 6-8, 24-28, 31-34) (on file with the *Hofstra Law Review*); *see generally* Siyi Lin, *The Illusory Problem of Intention in Algorithmic Contracts*, PENN ST. DICK. L. REV. (forthcoming 2026) (discussing the adverse effect of deepfakes in contract law aspect); Jyn-An Lee & Xuan Sun, *Vocal Identity Under Siege by AI Voice Cloning Technologies*, 2026 SING. J. LEGAL STUDS. 46 (discussing issues related to AI Voice Cloning).

3. *See* W. Michael Schuster, *Artificial Intelligence and Patent Ownership*, 75 WASH. & LEE L. REV. 1945, 1988-92 (2018); Lital Helman & Gideon Parchomovsky, *Artificial Inventorship* 9-14 (Univ. Pa. Inst. for L. & Econ., Research Paper No. 24-19, 2024), https://ssrn.com/abstract=4811815.

4. *See* Michael Grynberg, *AI and the "Death of Trademark"*, 108 KY. L.J. 199, 209-10, 215-16 (2019); Meghan Pane, Note, *Navigating the Algorithmic Marketplace: Reassessing Trademark Law in the Age of the Artificially Intelligent Consumer*, 77 RUTGERS U.L. REV. 197, 214-15 (2024).

attention from scholars, practitioners, and policymakers,[5] is experiencing its own doctrinal reshuffle in response to AI. The protection requirements, notably the "not readily ascertainable" standard and the reasonable measures to maintain secrecy, require redefinition.[6] Specifically, AI may render many previously protected trade secrets readily ascertainable, thereby stripping them of trade secret protection.[7] At the same time, it demands new and more types of measures from secret holders to safeguard confidential information against inadvertent leakage whether through their own use of AI tools or through third-party discovery enabled by AI.[8] Meanwhile, whether the acquisition of trade secrets using AI tools amounts to actionable trade secret misappropriation remains a heatedly debated question among scholars, with no clear answer in sight.[9]

At first glance, the relationship between AI and trade secrets appears uncomfortable. Yet it also has its "sweet moments": the protection of AI systems relies heavily on trade secrecy.[10] It has been well documented that, regardless of whether and to what extent the components of AI systems qualify for trade secrecy protection, companies maintain their factual secrecy and claim protection from trade secret law.[11] Firms

---

5. The U.S. Federal attention to trade secret protection spiked in 2013. *See* EXEC. OFF. OF THE PRESIDENT, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS (2013), https://www.justice.gov/criminal-ccips/file/938321/download [https://perma.cc/3KKV-TWK7]. The history of Chinese trade secret law began much more recently, starting roughly from 1993. *See* Yang Chen, *Development of China's Trade Secrets Law in the US' Shadow: Negative Consequences for China and Suggestions*, 17 U. PA. ASIAN L. REV. 138, 148-53, 155-56 (2022) [hereinafter "Chen, *Development of China's Trade Secrets Law*"]; Yang Chen, *Rebalancing the Burden of Proof for Trade Secrets Cases in China: A Detailed Scrutiny and Comparative Analysis of Article 32*, 84 U. PITT. L. REV. 827, 839-42 (2023) [hereinafter, "Chen, *Rebalancing*"] (highlighting the new and novel burden-shifting clauses that were added to China's trade secrets law in 2019); Yang Chen, *Under Double Shadows: How U.S.–China Trade Relations and Path Dependence Shape China's IP Preliminary Injunction System*, 33 ASIA PAC. L. REV. 68, 77-78 (2025) [hereinafter "Chen, *Under Double Shadows*"] (detailing the preliminary junction available to trade secrets cases was added in 2018).

6. *See* John G. Sprankling, *Trade Secrets in the Artificial Intelligence Era*, 76 S.C. L. REV. 181, 194-95, 206 (2024); David S. Levine, *Generative Artificial Intelligence and Trade Secrecy*, 3 J. FREE SPEECH L. 559, 562-64 (2023).

7. *See* Sprankling, *supra* note 6, at 206-08; Camilla A. Hrdy, *Trade Secrecy Meets Generative AI*, 100 CHI.-KENT L. REV. 317, 330-32 (2025).

8. *See* Sprankling, *supra* note 6, at 208-10; Hrdy, *supra* note 7, at 324-28.

9. *See* Sprankling, *supra* note 6, at 210-14; Camilla A. Hrdy, *Keeping ChatGPT a Trade Secret While Selling It Too*, 40 BERKELEY TECH. L.J. 75, 131-42 (2025); Levine, *supra* note 6, at 564; Yang Chen, *The Promise and Perils of Enterprise Data as Trade Secrets*, 29 STAN. TECH. L. REV. 1, 48-54 (2025).

10. *See infra* Part II.

11. *See, e.g.*, Sharon K. Sandeen & Tanya Aplin, *Trade Secrecy, Factual Secrecy and the Hype Surrounding AI*, *in* RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND ARTIFICIAL INTELLIGENCE 443, 451-58 (Ryan Abbott ed., 2022); Rita Matulionyte & Jyh-An Lee, *Transparent*

may claim trade secrecy protection for not just the source code, algorithms, training data, the overall system architecture underpinning AI systems but even any business applications of them.[12] The loose subject matter requirement of the modern trade secret law facilitates firms' reliance in part.[13] As such, AI systems may contain many layers of what this Article terms "AI secrets." The widely recognized availability of trade secret law as a means of protecting AI systems against competitors' free-riding may generate substantial economic benefits, including incentivizing AI developers' continuous innovation and sustaining long-term investment in AI developments, [14] particularly in areas where other IP laws, notably copyright and patent law, fail to provide effective protection.[15]

While trade secret law does serve a beneficial function in the AI era, its allowance for firms' unrestrained reliance on it poses a pressing issue: concerns about AI transparency.[16] Indeed, it is well recognized

---

AI, Confidential Information and Public Interest Defence: Healthcare as a Case Study 13-15 (Chinese Univ. Hong Kong, Research Paper No. 2025-27, 2025); Hrdy, *supra* note 9, at 94-108; Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 125 (2019) [hereinafter "Katyal, *Private Accountability*"]; Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1225-29 (2019) [hereinafter "Katyal, *The Paradox*"]; Jeanne C. Fromer, *Machines as the New Oompa-Loompas: Trade Secrecy, the Cloud, Machine Learning, and Automation*, 94 N.Y.U. L. REV. 706, 716-18 (2019); Rochelle C. Dreyfuss, *Trade Secrets and Deep Secrets* 7-8 (N.Y.U. Sch. L., Law and Economics Working Paper No. 24-37, Public Law and Legal Theory Working Paper No. 24-40, 2024); John Villasenor, *Artificial Intelligence, Trade Secrecy, and the Challenge of Transparency*, 25 N.C. J.L. & TECH. 495, 507-10 (2024).

12. *See* Hrdy, *supra* note 9, at 94-108; Sylvia Lu, *Data Privacy*, *Human Rights, and Algorithmic Opacity*, 110 CALIF. L. REV. 2087, 2098-100 (2022).

13. *See infra* Parts II–III.

14. It is one of the most classical economic benefits of granting exclusive rights over intangible assets for information holders. *See, e.g.*, Mark A. Lemley, *The Economics of Improvement in Intellectual Property Law*, 75 TEX. L. REV. 989, 993-99 (1997) [hereinafter "Lemley, *The Economics of Improvement*"]; Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 262-64 (1998); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 329-33 (2008) [hereinafter "Lemley, *Surprising Virtues*"]; Chen, *Reviving*, *supra* note 1, at 591; ROBERT P. MERGES, JUSTIFYING INTELLECTUAL PROPERTY 2-3 (2011); Reto M. Hilty et al., *Intellectual Property Justification for AI*, *in* ARTIFICIAL INTELLIGENCE AND INTELLECTUAL PROPERTY 64-68 (Jyh-An Lee et al. eds., 2021).

15. A typical example is the datasets used for AI model training, which may not receive copyright protection due to a failure to satisfy the originality requirement. In such cases, trade secret law may remain the only IP regime capable of offering protection. *See* Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 18-20 (2018). For a detailed account on how and to what extent trade secret law can protect enterprise data, see Chen, *supra* note 9, at 21-26; Yang Chen, *Against Trade Secrets Protection for "Semi-public" Databases*, 2026 SING. J. LEGAL STUDS. 107, 107-28.

16. For recent discussions on trade secrecy and AI transparency concerns, see Perry Keller & Tanya Aplin, *Reconciling Trade Secrets and AI Public Transparency*, CAMBRIDGE L.J. (forthcoming 2026) (manuscript at 6-11) (on file with the *Hofstra Law Review*); Villasenor, *supra* note 11, at 520-31; Matulionyte & Lee, *supra* note 11, at 7; Ulla-Maija Mylly, *Transparent AI? Navigating*

that AI systems are shrouded in opacity, which significantly constrains meaningful scrutiny by relevant stakeholders, including regulatory bodies, consumers, and public interest groups.[17] One of the main reasons for AI opacity lies in its technical complexity as the "machine learning algorithms, a widely adopted subset of AI systems[,]" would continually change and transform their logic and internal structures when they learn from experiences. [18] It creates technical challenges even for AI developers themselves, let alone for stakeholders outside the corporate veil.[19] Accordingly, developing explainable AI ("XAI") has long been a major focus within the industry.[20]

Yet, technical opacity is merely one factor. The availability of, and firms' (over) reliance on and (over) claiming of, AI trade secrets contributes at least as much to the AI transparency concerns,[21] and it is this legally constructed opacity on which this Article centers. Scholars have long recognized the tension between trade secret law and demands for AI transparency and have sought to develop solutions to reconcile the two.[22] For example, more than five years ago, Katyal began to warn about the problems posed by source code secrecy underlying algorithmic

---

Between Rules on Trade Secrets and Access to Information, 54 INT'L REV. INTELL. PROP. & COMPETITION L. 1013, 1017-19 (2023); Lu, *supra* note 12, at 2116-18.

17. *See* Lu, *supra* note 12, at 2098-100; Matulionyte & Lee, *supra* note 11, at 7-12.

18. Sylvia Lu, *Regulating Algorithmic Harms* 37-38 (Univ. Mich. L. Sch., L. & Econ., Working Paper No. 277, 2024).

19. *See id.* at 37; Lu, *supra* note 12, at 2098.

20. *See* Feiyu Xu et al., *Explainable AI: A Brief Survey on History, Research Areas, Approaches and Challenges*, *in* NATURAL LANGUAGE PROCESSING AND CHINESE COMPUTING 564-67, 572 (J. Tang et al. eds., 2019) (documenting the history, major research areas, methods, and challenges in explainable artificial intelligence); Rudresh Dwivedi et al., *Explainable AI (XAI): Core Ideas, Techniques, and Solutions*, 55 ACM COMPUTING SURV. 194:1, :3-4, :8, :20-21, :29-30 (2023) (exploring the core ideas of explainable AI, major interpretability techniques, and practical solutions to the "black box" problem in modern machine learning); Xiaoming Liu et al., *From Black Box to Glass Box: A Practical Review of Explainable Artificial Intelligence (XAI)*, AI Nov. 2025, at 4-6, 8, 11-15.

21. *See, e.g.*, Lu, *supra* note 12, at 2099-100; Lu, *supra* note 18, at 37-38; Matulionyte & Lee, *supra* note 11, at 17-19; Keller & Aplin, *supra* note 16, at 8-11.

22. *See, e.g.*, Alyssa M. Carlson, *The Need for Transparency in the Age of Predictive Sentencing Algorithms*, 103 IOWA L. REV. 303, 321-24 (2017) (documenting the tension when secret algorithmic systems were used in sentencing); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1396-99 (2018) (noting the tension when secret algorithmic systems were used in criminal cases); Jyh-An Lee, *Algorithmic Bias and the New Chicago School*, 14 L., INNOVATION & TECH. 95, 109-11 (2022); Lu, *supra* note 12, at 2139-40; Sprankling, *supra* note 6, at 217-18; Ljupcho Grozdanovski, *My AI, My Code, My Secret–Trade Secrecy, Informational Transparency and Meaningful Litigant Participation Under the European Union's AI Liability Directive Proposal*, COMPUT. L. & SEC. REV.: INT'L J. TECH. L. & PRAC., Feb. 2025, at 1, 4-5 (exploring the tension in the litigation and court proceedings concerning AI harms).

systems, [23] particularly in contexts where algorithms developed by private companies are used in important public decision-making and are insulated from public scrutiny through claims of trade secrecy. [24] The solutions proposed by the current literature to solve the tension mainly called for stronger regulatory interventions to mandate more disclosure of AI secrets, particularly where AI systems are used to make or inform decisions affecting important public interests, such as credit scoring, or where they are deployed in industries in which safety and trustworthiness are paramount.[25]

However, as only a few scholars briefly alluded,[26] this Article argues that the tension between AI secrets and transparency is rooted in structural features of trade secret law itself, notably, the inherent indeterminacy of its scope.[27] Because the boundaries of protectable trade secrets are not fixed *ex ante* but are instead determined only through *ex post* judicial decisions, firms can overclaim secrecy and withhold information from scrutiny unless and until a court draws the line.[28] In other words, firms can maintain factual secrecy over vast swaths of information surrounding AI and unilaterally characterize them as legally secret, thereby effectively shielding even non-secret information from public scrutiny. [29] Therefore, while current proposals to mandate greater disclosure or to refine public-interest and whistleblower defenses suffer inherent limitations and offer some partial responses to this tension, viewing the problem through the lens of structural features of trade secret law points toward the need for a more fundamental, structural solution to supplement the current approaches.

Accordingly, to address the tension between AI secrets and transparency by supplementing the current regulatory approaches, this Article proposes a structural redesign of trade secret law when applied to AI secrets: a formal AI secrets registration system. To build this model, the Article draws on comparative insights from existing registration, recordation, and third-party review mechanisms in representative

---

23. *See* Katyal, *The Paradox*, *supra* note 11, at 1237-42.

24. *See* Katyal, *Private Accountability*, *supra* note 11, at 105-07.

25. *See, e.g.*, Sylvia Lu, *Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial Intelligence*, 23 VAND. J. ENT. & TECH. L. 99, 131-35, 138-41 (2020); Villasenor, *supra* note 11, at 520-25; Lee, *supra* note 22, at 109-11; Dreyfuss, *supra* note 11, at 10-12.

26. *See, e.g.*, Sandeen & Aplin, *supra* note 11, at 443-44, 446-48 (explaining how companies always rely on trade secret law to claim AI secrets and conflate factual secrecy with legal secrecy); Villasenor, *supra* note 11, at 526-28; Katyal, *The Paradox*, *supra* note 11, at 1227-29, 1269 (explaining the same in the source code context).

27. *See infra* Part III.

28. *See infra* Part III.

29. *See* Sandeen & Aplin, *supra* note 11, at 443-45.

jurisdictions.[30] It specifically examines the three major digital economies poised to lead global regulation[31]—the United States (via its copyright registration system), China (through its local data registration platforms), and the European Union (under its AI and data governance frameworks).[32] By synthesizing these approaches, this Article seeks to develop an innovative proposal that is both conceptually grounded and pragmatically adaptable across different legal regimes.[33] Ultimately, this foundational framework is designed to facilitate future global implementation, offering a viable path to resolve the transnational conflict between proprietary AI claims and public transparency demands.

Before turning to its normative proposal, this Article proceeds in three stages. Parts I and II provide the descriptive groundwork by examining the most recent disputes, cases, and regulatory responses concerning AI secrets and the resulting transparency tensions.[34] Part I introduces the basic contours of modern trade secret law and explains why it has become both resilient and attractive as a means of protecting AI secrets.[35] Part II documents how AI secrets interfere with demands for public transparency and surveys the existing responses in major jurisdictions and in the scholarly debates, which suffer limitations.[36] These descriptive accounts are followed by Part III, which offers the Article's analytical core. It argues that the structural features of trade secret law, notably the indeterminacy of its scope, evolve into structural failures when applied in the AI context, thereby exacerbating the tension between AI secrecy and transparency, and that this problem calls for a more structural solution.[37] Part IV then sets out the proposed registration system for AI secrets in detail and explains how it would mitigate this tension by addressing the structural failures and bringing ancillary bene-

30. *See infra* Part IV.A.

31. *See generally* ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY (2023) (construing China, the United States, and the European Union as three "digital empires" competing to promulgate regulatory frameworks that shape other jurisdictions); Charles C. Wang et al., *AI Governance in China: A Tale of Three Digital Empires*, 48 U.C. L. S.F. INT'L L. REV. 143 (2025).

32. *See infra* Part IV.A; the proposal also builds on the preliminary insights provided by Keller and Aplin regarding "the incorporation of binding third party review of trade secret claims into public transparency challenge and contestation rights for AI systems." *See* Keller & Aplin, *supra* note 16, at 30.

33. *See infra* Part IV.C.

34. *See infra* Parts I–II.

35. *See infra* Part I.

36. *See infra* Part II.

37. *See infra* Part III.

fits.[38] It concludes by setting out the limitations, addressing potential objections and offering responses.[39]

I. TRADE SECRECY AND AI SECRECY

A. The Law of Trade Secrets

Despite its common law origin, modern trade secrecy protection in the United States mainly relies on state statutes modeling from the Uniform Trade Secrets Act ("UTSA").[40] While the theoretical foundations of trade secret law remain contested, the dominant contemporary approach is to conceptualize trade secrets as a form of IP.[41] For a long time, civil plaintiffs could bring only state-law claims for trade secret misappropriation, as no federal civil cause of action was available.[42] The situation persisted until the enactment of the Defend Trade Secrets Act ("DTSA") in 2016, which, for the first time, allows trade secret holders to bring federal claims.[43] However, one critical feature of the DTSA that distinguishes it from other federal IP regimes is its tolerance of state

38. *See infra* Part IV.A–B.

39. *See infra* Part IV.C.

40. *See* UNIF. TRADE SECRETS ACT (UNIF. L. COMM'N 1985). One exception is New York State, which still relies on common law to protect trade secrets. *See* Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317, 352-53, 355 (2015); Charles Tait Graves & Sonia K. Katyal, *From Trade Secrecy to Seclusion*, 109 GEO. L.J. 1337, 1348-49, 1405 n.330 (2021); Joseph P. Fishman & Deepa Varadarajan, *Earning Trade Secrets*, 109 CORNELL L. REV. 1381, 1400 & n.73 (2024).

41. For theoretical debates, compare Bone, *supra* note 14, at 259-60 (questioning trade secrets' IP nature) and Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803, 1810-13 (2014) (questioning the same) with Lemley, *Surprising Virtues*, *supra* note 14, at 328-32 (justifying trade secrets as IP rights), and Deepa Varadarajan, *The Trade Secret-Contract Interface*, 103 IOWA L. REV. 1543, 1550 (2018) ("In recent decades, trade secrets have come to be seen as a species of intellectual property "). China's Civil Code explicitly categorizes trade secrets as a type of IP right. *See* Chen, *Development of China's Trade Secrets Law*, *supra* note 5, at 190. Trade secret is considered as one of the IP subject matters in the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPs") agreement. *See* Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, 1869 U.N.T.S. 299, 316-17 [hereinafter TRIPS Agreement].

42. *See* David S. Levine & Christopher B. Seaman, *The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act*, 53 WAKE FOREST L. REV. 105, 113-15 (2018).

43. *See* 18 U.S.C. §§ 1832–33, 1835–36, 1838–39. Completely separate from the DTSA private right of action, federal law has long had a criminal trade secret statute (Economic Espionage Act). *See* Camilla A. Hrdy, *The Value in Secrecy*, 91 FORDHAM L. REV. 557, 568-69, 569 n.61 (2022); Levine & Seaman, *supra* note 42, at 114-15. Major developments in trade secret protection in other jurisdictions, such as the European Union and China, also began roughly during the same period. *See* Chen, *supra* note 9, at 10.

trade secret law.[44] Whereas federal patent and copyright law generally preempt state laws that offer equivalent protection,[45] the DTSA expressly refrains from preempting trade secret claims available under existing state law.[46] As such, there now exist two parallel paths for trade secret holders in the United States, who may elect to proceed under state law or federal law, or pursue both in parallel.[47] It is, however, important to note that the DTSA largely mirrors the UTSA, with both sharing similar requirements for trade secrecy protection.[48]

One of the main purposes underlying both the UTSA and DTSA is to harmonize the trade secrecy protection across the United States.[49]Accordingly, despite some historical requirements that once pertained to common law trade secrecy protection,[50] modern trade secret law provides only three requirements. First, information should be secret, that is, not generally known or readily ascertainable, to qualify for trade secret protection.[51] Indeed, maintaining factual secrecy is the starting point of trade secret protection. The secrecy of information is not assessed by reference to the general public; rather, it is sufficient that the information

---

44. *See* 18 U.S.C. § 1838 (explaining that this chapter does not preempt or displace any other remedies, including under state law, for trade secret misappropriation); Hrdy, *supra* note 43, at 569 n.64. *But see* Jennifer E. Rothman, *Copyright Preemption and the Right of Publicity*, 36 U.C. DAVIS L. REV. 199, 226-27, 226 n.116 (2002) (noting federal copyright law preempts state law when two requirements are met); Camilla A. Hrdy, *Getting Patent Preemption Right*, 24 J. INTELL. PROP. L. 305, 308-11, 313-14 (2017) (explaining when state patent laws are preempted).

45. *See, e.g.*, Rothman, *supra* note 44, 225-43 (explaining federal preemption for state copyright law); Hrdy, *supra* note 44, 308-11, 313-14 (explaining federal preemption for state patent law).

46. *See* Brittany S. Bruns, *Criticism of the Defend Trade Secrets Act of 2016: Failure to Preempt*, 32 BERKELEY TECH. L.J. 469, 489-91 (2017); Orly Lobel, *The DTSA and the New Secrecy Ecology*, 1 BUS., ENTREPRENEURSHIP & TAX L. REV. 369, 370-71 (2017).

47. *See* Hrdy, *supra* note 43, at 568-69; Fishman & Varadarajan, *supra* note 40, at 1404.

48. *See* Fishman & Varadarajan, *supra* note 40, at 1404-05; Sharon K. Sandeen & Christopher B. Seaman, *Toward a Federal Jurisprudence of Trade Secret Law*, 32 BERKELEY TECH. L.J. 829, 866-67 (2017).

49. *See* Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493, 502-03 (2010); Seaman, *supra* note 40, at 325-26, 352-53; David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 769, 773-76 (2009) (arguing, before the enaction of DTSA, that one reason to federalize trade secret law is to further harmonize state laws).

50. *See, e.g.*, Camilla A. Hrdy & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV. 1, 21-22 (2021) (explaining the common-law continuous use requirement); Fishman & Varadarajan, *supra* note 40, at 1395-99 (explaining the common-law original acquisition or investment requirement).

51. *See* UNIF. TRADE SECRETS ACT § 1(4)(i) (UNIF. L. COMM'N 1985); 18 U.S.C. § 1839(3)(B); *cf.* CAL. CIV. CODE § 3426.1(d) (West 1995) (demonstrating that "readily ascertainable" is not a requirement in California version of the UTSA).

remains factually secret within relevant industry or business. [52] While disclosure to industry members or parties who can obtain economic benefit from them will destroy the trade secret protection, trade secret law permits, and even encourages, carefully controlled sharing with internal personnel and selected external partners in order to facilitate the efficient use of the secret information without sacrificing its secrecy.[53] Second, the information must possess actual or potential commercial or economic value that is at least partially attributable to its secrecy. [54] Finally, companies should have employed reasonable measures, whether physical, technical, or contractual, to maintain the information's secrecy.[55] Requiring information holders to adopt reasonable but not excessive secrecy measures, for one thing, serves to curb an inefficient arms race between trade secret holders and potential appropriators and to ease the burden on information holders of guarding against every possible avenue of disclosure. [56] For another, the requirement of reasonable secrecy measures places recipients of the information on notice of its secret nature, thereby allowing them to adjust their conduct accordingly.[57] One familiar with trade secret law would immediately think of Coca-Cola's fizzy drink formula as the paradigmatic example of a protectable trade secret, which has "lived" for more than 130 years.[58] Coca-Cola continues to maintain this commercially successful and valuable formula as a factual secret through multiple layers of measures, such as storing it in a secure vault and limiting full access to the formula to only two employees at any given time.[59]

While formulas, techniques, methods, or processes are typical subject matters of trade secret protection, the scope of protectable trade se-

---

52. *See* Sandeen & Aplin, *supra* note 11, at 452; UNIF. TRADE SECRETS ACT § 1 cmt ("The language 'not being generally known to and not being readily ascertainable by proper means by other persons' does not require that information be generally known to the public for trade secret rights to be lost. If the principal ~~person~~ persons who can obtain economic benefit from information ~~is~~ are aware of it, there is no trade secret." (alterations in original)).

53. *See* Lemley, *Surprising Virtues*, *supra* note 14, at 332-37.

54. *See* UNIF. TRADE SECRETS ACT § 1(4)(i); 18 U.S.C. § 1839(3)(B).

55. *See* UNIF. TRADE SECRETS ACT § 1(4)(ii); 18 U.S.C. § 1839(3).

56. *See* Chen, *supra* note 9, at 44-45; Douglas Lichtman, *How the Law Responds to Self-Help*, l J.L. ECON. & POL'Y 215, 232 (2005); Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 42-43 (2007); Lemley, *Surprising Virtues*, *supra* note 14, at 333-34.

57. *See* Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357, 377-78 (2017).

58. *Is the Coca-Cola Formula Kept Secret Because the Company Has Something to Hide?*, THE COCA-COLA Co. (FAQ), https://www.coca-cola.com/ng/en/about-us/faq/is-the-coca-cola-formula-kept-secret-because-the-company-has-som [https://perma.cc/YF7P-G546] (last visited July 18, 2026).

59. *How Does Coca-Cola Protect Their Recipe*?, TANGIBLY, https://www.tangibly.com/how-does-coca-cola-protect-their-recipe [https://perma.cc/Z52P-3T7W] (Mar. 18, 2026).

crets extends far beyond what one might initially imagine.[60] The current law defines the subject matter of trade secret protection extremely broadly, extending in principle to any valuable information that satisfies the requirements.[61] The overly broad and uncertain boundaries of the trade secret subject matter reach have allowed firms to assert trade secret claims over information with little or even no connection with marketplace competition, such as workplace diversity data or even information relating to corporate wrongdoing.[62] As will be detailed below, this entrenched practice of expansive trade secret claiming, facilitated by the loose subject matter requirement, is one of the main reasons why assertions on AI secrets stand in sharp tension with goals of AI transparency.[63]

Unlike copyright, patent, and trademark, there is not any registration system available for trade secrets, nor any governmental bodies examining whether the information qualifies as trade secrets or not.[64] This means that, theoretically, commercially valuable information can receive trade secret protection once it is kept secret through reasonable measures. Yet the rights conferred by trade secret law are far weaker than those provided by patent law: they reach only misappropriation and do not prohibit legitimate means of acquisition, notably reverse engineering and independent development.[65] Misappropriation encompasses both the acquisition of trade secrets by improper means, such as theft, cyber espionage, or bribery, and the disclosure or use of trade secrets in

---

60. UNIF. TRADE SECRETS ACT § 1(4); 18 U.S.C. § 1839(3).

61. UNIF. TRADE SECRETS ACT § 1(4) ("'Trade secret' means information, including "); 18 U.S.C. § 1839(3) ("[T]he term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including "); Eric E. Johnson, *Trade Secret Subject Matter*, 33 HAMLINE L. REV. 545, 551, 553-54 (2010); JAMES POOLEY, TRADE SECRETS § 1.01 (2021) ("Virtually any useful information can qualify as a trade secret.").

62. *See* Graves & Katyal, *supra* note 40, at 1350-52.

63. *See infra* Part III.

64. *See* Varadarajan, *supra* note 41, at 1552; Chagai Vinizky, *Trade Secrets Registry*, 35 PACE L. REV. 455, 469, 472, 487-88 (2014); Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401, 1409-10 (2014) (noting that patent protection requires registration and examination before rights are granted); Rebecca Tushnet, *Registering Disagreement: Registration in Modern American Trademark Law*, 130 HARV. L. REV. 867, 875-77 (2017) (describing the trademark registration system). Though registration is not a prerequisite for copyright protection, the U.S. Copyright Registration Office still accepts and examines the requests from copyright holders to register their works. *See* Dotan Oliar et al., *Copyright Registrations: Who, What, When, Where, and Why*, 92 TEX. L. REV. 2211, 2215 (2014). For a discussion on how the Office recently rejected registration of AI-generated works, see Chen, *Two Roads*, *supra* note 1, at 12-13.

65. UNIF. TRADE SECRETS ACT § 1 cmt. ("Proper means include: 1. Discovery by independent invention; 2. Discovery by 'reverse engineering' "); 18 U.S.C. § 1839(6)(B) ("[D]oes not include reverse engineering, independent derivation, or any other lawful means of acquisition ").

breach of an explicit or implied duty of confidence.[66] Third parties who disclose or use trade secrets with the requisite knowledge of their improper acquisition or disclosure may also be held liable for trade secret misappropriation.[67]

B. AI Secrets

The loose subject matter requirement of trade secret law offers tremendous opportunities for components of AI systems to receive trade secret protection. Indeed, some typical components that underpin the AI systems, such as programs, code, data (compilations), and patterns, are explicitly listed as the paradigmatic examples of protectable subject matters under trade secret law.[68] Yet the lists in the current laws are nonexhaustive, and as mentioned, the subject matter is defined very broadly,[69] which gives leniency for information related to AI to qualify for trade secret protection. [70] Clearly, not all AI secrets claimed by firms genuinely qualify for the protection, as they need to satisfy the three aforementioned requirements. [71] However, it is well established that a number of typical components of AI systems have substantial potential to satisfy the three requirements, thereby qualifying for trade secret protection.[72]

Source code, the backbone of AI systems, has long been enjoying trade secret protection.[73] Even though copyright is one of the standard methods for protecting source code, which is generally considered as a type of copyrightable literary work,[74] as argued by Hrdy, trade secret law offers "an important additional layer of protection for code."[75] In contrast to copyright, trade secret law is not constrained by the "substantial similarity" standard or the fair use doctrine, providing broader protection for source code in both respects. [76] Indeed, the intrinsic qualities of source code make it uniquely suited for trade secret protection. Even when a software system is deployed for public use, firms can make available only the machine-executable object code while maintaining the

66. UNIF. TRADE SECRETS ACT § 1(1)–(2); 18 U.S.C. § 1839(5)–(6).

67. UNIF. TRADE SECRETS ACT at § 1(2); 18 U.S.C.A. § 1839(5).

68. *See* UNIF. TRADE SECRETS ACT § 1(4); 18 U.S.C. § 1839(3); Hrdy, *supra* note 9, at 95-96, 100, 102; Hrdy, *supra* note 7, at 337-40; Villasenor, *supra* note 11, at 508.

69. *See supra* notes 61-62 and accompanying text.

70. Sprankling, *supra* note 6, at 202-03, 207.

71. *See* Sandeen & Aplin, *supra* note 11, at 451-55, 457-58.

72. Hrdy, *supra* note 7, at 338-39.

73. *See* Katyal, *The Paradox*, *supra* note 11, at 1208-09, 1226-29.

74. TRIPS Agreement, *supra* note 41, at 304; 17 U.S.C. § 101.

75. Hrdy, *supra* note 9, at 100.

76. *Id.* at 100-01.

human-readable source code as a factual secret.[77] As such, courts have long recognized its eligibility for trade secret protection, and software developers have correspondingly relied on trade secret law to protect it.[78]

It is well understood that the development of a generative AI model requires a massive amount of training data.[79] While training data may include copyrighted materials such as published materials, written works, and sounds, thereby triggering potential copyright infringement issues,[80] it also implicates issues of trade secret protection. First, trade secret law may protect the whole training dataset as long as AI developers keep them secret.[81] Indeed, AI developers have strong incentives to adopt measures to prevent competitors from learning what training datasets were used to train their systems, because disclosure may confer a competitive advantage on competitors when they develop their own models.[82] Trade secret law's application to training datasets is not undermined by the fact that some data points within the datasets are public information, which is normally the case for most training datasets.[83] Trade secret law's resilience in extending protection for large-scale databases irrespective of some components being public data is well documented.[84] Second, not just the quantity but also the quality of the training data selected and compiled matters for AI model training.[85] Therefore, in addition to the final datasets themselves, information about which data was selected and compiled to train the system, as well as what data points are more valuable than others in model training, information that AI developers also tend to keep secret, may likewise qualify for trade secret protection.[86]

In the AI context, algorithms, normally referring to the processes and sets of instructions used to train AI models or to build the software

77. *See id.* at 100.

78. *See* Michael Risch, *From Patents to Trade Secrets*, *in* RESEARCH HANDBOOK ON EMPIRICAL STUDIES IN INTELLECTUAL PROPERTY LAW 101, 108 (Estelle Derclaye ed., 2023); Katyal, *The Paradox*, *supra* note 11, at 1207-09.

79. *See, e.g.*, Andrew W. Torrance & Bill Tomlinson, *Training is Everything: Artificial Intelligence, Copyright, and "Fair Training"*, 128 DICK. L. REV. 233, 243 (2023).

80. *See id.*; Matthew Sag, *Copyright Safety for Generative AI*, 61 HOU. L. REV. 295, 303-06 (2023). For a general understanding of the copyright infringement test, see Yang Chen, *Copyright Infringement Test (Re)visited: U.S. Spillover into China Yielding a Similar Test?*, 48 COLUM. J.L. & ARTS 184, 191-97 (2025).

81. *See* Hrdy, *supra* note 9, at 103-04.

82. *See id.*

83. *See id*. at 104-05; Sandeen & Aplin, *supra* note 11, at 453-54.

84. Hrdy, *supra* note 9, at 104-05; Sandeen & Aplin, *supra* note 11, at 453-54; Chen, *supra* note 9, at 21-26 (explaining how the recognition of private data and data compilations as trade secrets has been consistent and growing).

85. *See* Hrdy, *supra* note 9, at 103 n.177; Torrence & Tomlinson, *supra* note 79, at 242.

86. *See* Hrdy, *supra* note 9, at 103.

programs that underpin AI systems, are another paramount component of any AI system.[87] Some scholars claimed algorithms as "natural" trade secrets as they are not revealed to the public, too complicated to comprehend, and may survive reverse engineering attempts. [88] This is particularly true when algorithms are generated by the AI itself through machine learning; as these algorithms continue to evolve from new data, they become increasingly incomprehensible and difficult to decipher.[89] It is legally irrelevant whether creators or owners fully comprehend or possess affirmative knowledge of these AI-generated algorithms for trade secret protection to attach. [90] So long as the algorithms remain secret, specifically, not readily ascertainable, they qualify for trade secret protection, provided that the other two requirements are satisfied.[91] In fact, trade secret law probably remains the only available IP law that offers protection for algorithms. [92] This is because algorithms, as mathematical instructions or abstract ideas, do not qualify for either copyright or patent protection.[93]

AI systems have strong potential to benefit from trade secret protection not only for the aforementioned example components but for many others.[94] In fact, firms are actively claiming trade secret protection for different AI components.[95] In *Neural Magic, Inc. v. Meta Platforms,*

---

87. *See* Andrew Williams, *What Is an Algorithm? Defining and Applying Algorithms*, FORBES (Feb. 1, 2024), https://www.forbes.com/sites/technology/article/what-is-an-algorithm [https://perma.cc/433Z-E2DJ]; Hrdy, *supra* note 9, at 87.

88. *See* Charlotte A. Tschider, *Beyond the "Black Box"*, 98 DENV. L. REV. 683, 700, 710-11 (2021); Hrdy, *supra* note 9, at 95.

89. *See* Tschider, *supra* note 88, at 690.

90. *See* Villasenor, *supra* note 11, at 508-10.

91. *See* Risch, *supra* note 78, at 108.

92. *See* Gregory Gerard Greer, *Artificial Intelligence and Trade Secret Law*, 21 U. ILL. CHI. REV. INTELL. PROP. L. 252, 263 (2022); Risch, *supra* note 78, at 101-02; Tschider, *supra* note 88, at 710-12.

93. *See* Greer, *supra* note 92, at 263; Risch, *supra* note 78, at 101-02; Tschider, *supra* note 88, at 711-12.

94. For example, trade secret law can protect the overall system architecture, and system prompts of an AI system as well as the knowledge and information of how to fine-tune an AI model. *See, e.g.*, Hrdy, *supra* note 9, at 106-08; Villasenor, *supra* note 11, at 508; First Amended Complaint at 1-3, OpenEvidence, Inc. v. Pathway Med., Inc., No. 1:25-cv-10471, 2025 WL 751619 (D. Mass. Aug. 15, 2025) (claiming system prompts of the AI model as trade secrets).

95. *See, e.g.*, Loop AI Labs Inc. v. Gatti, 195 F. Supp. 3d 1107, 1114, 1117 (N.D. Cal. 2016) (demonstrating that a startup company that developed AI technology sued against competitors, asserting misappropriation of its AI secrets, such as "confidential modeling and discussions regarding its development and experimentation of supervised and unsupervised artificial intelligence technology." The court, however, held that the plaintiff failed to identify the trade secrets with reasonable particularity); Priority Payment Sys., LLC v. Signapay, Ltd., 161 F. Supp. 3d 1294, 1298-1300 (N.D. Ga. 2016) (finding that source code for computer software merchant management systems constituted a trade secret under the Georgia Trade Secrets Act where the plaintiff's success was due largely to its proprietary systems and the company implemented various security measures includ-

Inc.,[96] for example, the plaintiff, Neural Magic, asserted that a former employee had misappropriated its proprietary algorithms designed to allow machine-learning neural networks to run at high speeds on standard processors.[97] Neural Magic alleged that these secrets were disclosed to Meta, which then incorporated the logic into its own source code and published it on GitHub, an open-source development platform. [98] As such, Neural Magic sued both the former employee and Meta, in part under the Massachusetts UTSA and the DTSA, for trade secret misappropriation.[99] The district court ruled that Neural Magic survived the motion for summary judgment on eleven of twelve categories of trade secrets it claimed and could proceed to trial,[100] which led to a settlement in 2023.[101]

In early 2025, an AI company named OpenEvidence Inc., which developed and maintained an AI platform for medical information, initiated a litigation against Pathway Medical, Inc., a Canadian corporation which also offers services to medical professionals and healthcare cen-

---

ing confidentiality provisions and employee security policies); WeRide Corp. v. Kun Huang, 379 F. Supp. 3d 834, 841-42, 845-47 (N.D. Cal. 2019) (claiming several components of a self-driving car technology, such as source code and algorithms, as trade secrets under DTSA and CUTSA); Zabit v. Brandometry, LLC, 540 F. Supp. 3d 412, 415-17, 419, 425, 427 (S.D.N.Y. 2021) (claiming an algorithm underlying a stock market index using brand data and stock prices as trade secrets under the DTSA but failed to satisfy the secrecy and reasonable secret measures requirements); T2 Modus, LLC v. Williams-Arowolo, No. 4:22-CV-00263, 2023 WL 6221429, at *5 (E.D. Tex. Sept. 25, 2023) (finding descriptions of trade secrets in very "conclusory terms such as 'artificial intelligence,' 'machine learning,' or 'proprietary software' insufficient without including additional specific information"); Neural Magic, Inc. v. Meta Platforms, Inc., 659 F. Supp. 3d 138, 152-56, 186 (D. Mass. 2023) (finding the algorithms as trade secrets with a majority of them surviving the motion for summary judgment); Omniq Corp. v. Redlpr, LLC, No. 2:19-cv-437-CW-DBP, 2025 WL 525044, at *5-6 (D. Utah Feb. 18, 2025) (recognizing the specific workings of an optical character recognition algorithm used in vehicle recognition software as a trade secret under the DTSA and Utah's UTSA but finding that the plaintiff failed to show the defendants knew the specific operational steps of the algorithm); First Amended Complaint, *supra* note 94, at 1-3, 9, 12-13 (stating system prompts underpinning its AI medical information platform, information about its proprietary medical knowledge, clinical reasoning patterns, diagnostic methodologies, and treatment recommendations that form the AI model knowledge base as trade secrets under the DTSA and suing the defendant for executing dozens of prompt injection attacks to acquire them); NEXT Payment Solutions, Inc. v. CLEAResult Consulting, Inc., 163 F.4th 1091, 1095-98 (7th Cir. 2026) (holding that the plaintiff failed to identify trade secrets in its software modules with sufficient specificity under the DTSA where it did not identify any specific algorithms, source code, or methodologies underlying the software's functionality).

96. 659 F. Supp. 3d 138 (D. Mass. 2023).

97. *Id.* at 153-56.

98. *Id.* at 155-56.

99. *Id.* at 150-51.

100. *Id.* at 151.

101. *See* Sarah Speight, *Meta and AI Software Startup Settle Trade Secrets Suit*, WIPR (Aug. 10, 2023), https://www.worldipreview.com/rankings/global-trade-secrets/meta-and-ai-software-startup-settle-trade-secrets-suit-24219 [https://perma.cc/E9RV-GLAE].

ters in the United States.[102] In its amended complaint, OpenEvidence alleged that Pathway engaged in prompt injection attack to obtain system prompts that define how the AI model behaves and responds and represent its underlying algorithms as well as data forming the knowledge base of the platform. [103] OpenEvidence claimed these system prompts and data, distilled and acquired by Pathway, were protectable trade secrets under the DTSA,[104] and that Pathway's behavior constituted the use of improper means to acquire those trade secrets.[105] Following Pathway's acquisition by Doximity, Inc., OpenEvidence voluntarily dismissed all of its claims against Pathway, yet initiated another litigation against Doximity, asserting substantially similar claims and arguments under the DTSA and other laws.[106]

In late 2025, a video technology company, VideoLabs Inc., sued two of its prior consultants who were hired to develop and refine Turing AI, an AI-powered patent analysis and IP management tool.[107] VideoLabs claimed the Turing AI, notably its confidential technology, workflows, and proprietary know-how, as protectable trade secrets under the DTSA.[108] It alleged that the two prior consultants withheld access to the

---

102. Complaint for Misappropriation of Trade Secrets, Violation of Computer Fraud and Abuse Act, Violation of the Digital Millennium Copyright Act, Breach of Contract, and Unfair Competition, OpenEvidence Inc. v. Pathway Med., Inc., No. 1:25-cv-10471, 2025 WL 751619 at *1, *5, *7 (D. Mass. Aug. 15, 2025).

103. First Amended Complaint at 19, 30, OpenEvidence Inc. v. Pathway Med., Inc., No. 1:25-cv-10471, 2025 WL 751619 (D. Mass. Aug. 15, 2025). For more discussions on other techniques, see James Fahey, *Distillation of Models in AI: Efficiency, Cost, and Intellectual Property Considerations*, MEDIUM (Feb. 2, 2025), https://medium.com/@fahey_james/distillation-of-models-in-ai-efficiency-cost-and-intellectual-property-considerations-dc0d6173fecf [https://perma.cc/58GW-6DW4]. For similar allegations in the Deepseek vs OpenAI context, see Scott Young, *DeepSeek, ChatGPT, and the Global Fight for Technological Supremacy*, HARV. L. TODAY (Feb. 25, 2025), https://hls.harvard.edu/today/deepseek-chatgpt-and-the-global-fight-for-technological-supremacy [https://perma.cc/WX74-JTL4].

104. First Amended Complaint, *supra* note 103, at 42-43.

105. *Id.* at 43.

106. Notice of Voluntary Dismissal Without Prejudice at 1, OpenEvidence Inc. v. Pathway Med., Inc., No. 1:25-cv-10471, 2025 WL 751619 (D. Mass. Aug. 15, 2025); Amended Complaint at 28-30, 32-33, OpenEvidence Inc. v. Doximity, Inc., No. 1:25-cv-11802 (D. Mass. Oct. 29, 2025). *But see* Complaint at 10-11, OpenEvidence Inc. v. Doximity, Inc., No. 1:25-cv-11802 (D. Mass. June 20, 2025).

107. *See VideoLabs Files Suit Accusing Consultants of Trade-Secret Theft over Turing AI Patent Tool, Alleging Extortion*, COMPLETE AI TRAINING (Dec. 30, 2025), https://completeaitraining.com/news/videolabs-files-suit-accusing-consultants-of-trade-secret [https://perma.cc/V7V4-NYPJ]; *When AI Patent Tools Become the Most Valuable Trade Secrets*, TANGIBLY, https://www.tangibly.com/when-ai-patent-tools-become-the-most-valuable-trade-secrets [https://perma.cc/L7XV-WAW2] (last visited July 18, 2026).

108. Complaint at 14-15, VideoLabs, Inc. v. Siccardo, No. 5:25-cv-11001 (N.D. Cal. Dec. 26, 2025); *When AI Patent Tools Become the Most Valuable Trade Secrets*, *supra* note 107.

system and demanded for an equitable share from VideoLabs, which VideoLabs characterized as an "outrageous misappropriation of trade secrets."[109]

Civil litigation aside, trade secret protection over AI components also arises in criminal cases. For instance, in 2026, a former Google software engineer was convicted for stealing trade secrets in part related to the AI technology of Google, such as information relating to the hardware infrastructure and software platforms that allow Google to train and serve AI models.[110]

II. AI SECRETS AND TRANSPARENT AI

AI secrets exist for their justifiable reasons. After all, one could argue that without trade secret protection for these AI components, free-riding issues may persist, thereby harming AI developers' incentives to continue innovation or AI investors' incentives to continue investment.[111] The outcome might be inefficient, particularly in the context where other IP laws cannot offer meaningful protection.[112] Yet the critical, allied issue with AI secrets is that they are susceptible to being invoked against any requests for transparency of AI systems, thus obscuring the potential harms caused by AI.[113]

If an AI system is utilized to automatically assess the recidivism risk of a defendant, and the trial court incorporates that assessment into its sentencing decision, the defendants may respond by requesting disclosure of the details of the system. This request typically touches upon a number of AI secrets mentioned above, such as the training datasets used to develop the model, the specific risk factors considered, and the algorithmic weighing of each factor. Because they are claimed as trade secrets by private AI developers, the request may fail, and the defendant

---

109. *When AI Patent Tools Become the Most Valuable Trade Secrets*, *supra* note 107.

110. Verdict Form at 1-7, United States v. Ding, No. 3:24-cr-00141-VC (N.D. Cal. Jan. 29, 2026); Press Release, U.S. Dep't of Just., Former Google Engineer Found Guilty of Economic Espionage and Theft of Confidential AI Technology (Jan. 29, 2026), https://www.justice.gov/usao-ndca/pr/former-google-engineer-found-guilty-economic-espionage-and-theft-confidential-ai [https://perma.cc/D6VL-AAKS].

111. *See supra* note 14; Lemley, *The Economics of Improvement*, *supra* note 14, at 989, 993-99; Bone, *supra* note 14, at 262-64; Lemley, *Surprising Virtues*, *supra* note 14, at 329-33; Chen, *Reviving*, *supra* note 1, at 591; MERGES, *supra* note 14, at 2-3; Hilty et al., *supra* note 14, at 64-68.

112. For example, algorithms cannot receive protection from either copyright or patent law with trade secret law being the only option available. *See supra* notes 87-93 and accompanying text.

113. Lu, *supra* note 18, at 37-38. For a typology of AI harms that may exist today due to wide usage of AI, see *id.* at 19-39.

cannot scrutinize the system for any potential built-in bias or mistakes made by the AI.[114]

Imagine another scenario. Suppose a private hospital widely adopts an AI system integrated into its electronic health record system. Whenever a patient visits a doctor, the AI system automatically records and transcribes the conversation, drafts clinical notes, provides potential diagnoses, and recommends treatment plans. Now, a public-interest group composed of medical experts becomes concerned about the potential built-in bias of the system and the accuracy of its medical recommendations and accordingly requests that the AI developer disclose the details of the system, similar to the first scenario. Such requests are typically met with refusal: developers routinely claim that these details constitute valuable assets protected by trade secret law, thereby foreclosing meaningful public scrutiny and opportunities to prevent or mitigate potential AI-related harms.[115]

These scenarios are not merely hypothetical; they are grounded in a growing body of real-world disputes where AI secrets directly clash with the need for transparency.[116] As AI increasingly permeates both the private sphere and essential public sectors,[117] these conflicts will only intensify.[118] Against this background, this Part pursues two aims. First, it maps how, in practice, AI developers' assertions of secrecy over AI components have come into tension with demands for AI transparency, drawing on cases and real-world disputes.[119] Second, it surveys existing

---

114. The fact pattern is adapted from the notoriously famous case *State v. Loomis*, 881 N.W.2d 749, 752-57, 761 (Wis. 2016). For more details of this original case, see Recent Case, Sentencing Guidelines—Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing.—State v. Loomis, *881 N.W.2d 749 (Wis. 2016)*, 130 HARV. L. REV. 1530-34 (2017); Katyal, *Private Accountability*, *supra* note 11, at 87; *cf.* Villasenor, *supra* note 11, at 520 (explaining that private orders issued by courts may allow parties to access trade secrets without having them lose trade secret status).

115. This hypothetical scenario is adapted from a real-world example. *See* Reylee Billingsley, *AI Reshapes Healthcare but Often Adopts Bias*, CRONKITE NEWS (Oct. 7, 2025), https://cronkitenews.azpbs.org/2025/10/07/ai-reshapes-healthcare-but-adopts-bias [https://perma.cc/LK9J-PE2Y]; For more insights on the tension between trade secret and use of AI in the medical or healthcare industry, see Matulionyte & Lee, *supra* note 11, at 17-19.

116. *See infra* Part II.A–B.

117. *See Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*, OECD (Sept. 18, 2025), https://doi.org/10.1787/795de142-en [https://perma.cc/UW4J-5BPD]; *see also* STRENGTHENING AI FOUNDATIONS: DIGITAL PROGRESS AND TREND REPORT 2025, WORLD BANK GRP. 5-11 (2025), https://openknowledge.worldbank.org/server/api/core/bitstreams/f2509a0f-7153-4f32-b180-bc11e90c4940/content [https://perma.cc/377R-M7LT].

118. *See Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*, *supra* note 117; STRENGTHENING AI FOUNDATIONS: DIGITAL PROGRESS AND TREND REPORT 2025, *supra* note 117, at 8, 10-11.

119. *See infra* Part II.A–B.

academic, legislative, and regulatory responses to this tension and argues that these approaches only partially alleviate the problem because they rest on a questionable presumption—namely, that the AI secrets claimed by firms are genuine trade secrets.[120] Accordingly, additional proposals, not based on the presumption, are required to complete the menu of options for resolving this tension.[121]

A. Public Authority Delegation and the "Secret Governance"

AI secrets intersect and conflict significantly with transparency demands in the context of "Secret Governance." This occurs when a public authority effectively delegates its decision-making power to an algorithmic system, while permitting private vendors to use trade secrecy as a shield against public scrutiny.[122] While *State v. Loomis*[123] predates the emergence of today's advanced AI systems, it implicates essentially the same fundamental tension that now characterizes the AI context—namely, the conflict between claims of trade secrecy and demands for transparency.[124] In *Loomis*, from which the foregoing first hypothetical scenario is adapted, the trial court relied in part on a Correctional Offender Management Profiling for Alternative Sanctions ("COMPAS") risk assessment report in determining the defendant's sentence.[125] Although the defendant knew about what factors that COMPAS considered, he was never informed of, nor permitted to obtain, any information regarding the algorithms underpinning the system, particularly how different factors were weighed.[126] The reason for rejection was due to trade secret protection claimed by the developer of COMPAS.[127]

Similarly, as shown in *Rayner v. New York State Department of Corrections and Community Supervision*,[128] the New York State Department of Corrections and Community Supervision ("DOCCS") kept using the same risk-assessment tool, COMPAS, in parole decision-making.[129] However, when a clinical law professor at Fordham Law

120. *See infra* Part II.C.

121. *See infra* Part IV.

122. *See, e.g.*, Katyal, *Private Accountability*, *supra* note 11, at 105-07; Wexler, *supra* note 22, at 1358-74; Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1273-90 (2020); Deepa Varadarajan, *Business Secrecy Expansion and FOIA*, 68 UCLA L. REV. 462, 482-83 (2021).

123. 881 N.W.2d 749 (Wis. 2016).

124. *See id*. at 761; *see also* Recent Case, *supra* note 114, at 1533-35.

125. *Loomis*, 881 N.W.2d at 754-55.

126. *Id.* at 761; *see also* Katyal, *Private Accountability*, *supra* note 11, at 87.

127. *Loomis*, 881 N.W.2d at 761, 769.

128. 81 Misc. 3d 281 (N.Y. Sup. Ct. 2023).

129. *Id.* at 282-83.

School submitted a request under the Freedom of Information Law seeking disclosure of "the formulas for calculating the risk and needs scales used" in COMPAS, the request was denied on the grounds that the information was trade secret.[130] The court affirmed the denial, concluding that the formulae, algorithms, risk and needs scales, and normative data underlying COMPAS were trade secrets.[131] Similar cases reflecting the tension abound prior to the AI era.[132]

The tension will only become more pronounced when advanced AI systems, characterized by complex infrastructure, intricate algorithms, and vast training datasets that developers consider core assets,[133] emerge to assist or even supplant public decision-making. As documented in detail by the Electronic Privacy Information Center ("EPIC"), across the United States, state and local governmental agencies are experimenting with AI tools and outsourced their services and decisions to them, such as automated facial recognition, risk scoring, eligibility screening for government services, and predictive policing AI systems.[134] Those AI systems are, however, normally developed and licensed to the govern-

130. *Id.* at 283-84.

131. *Id.* at 286-91.

132. *See, e.g.*, Todd v. Hause, 371 P.3d 705, 708-10 (Colo. App. 2015) (explaining the Colorado Department of Public Health and Environment's ("CDPHE") utilization of a software program licensed to the Department by a private manufacturer that linked data gathered from breath test machines to a centralized database to record and manage breath alcohol test results for DUI enforcement, where the court held that the software's source code and accompanying raw data qualified as a trade secret exempt from disclosure under the Colorado Open Records Act); Hou. Fed'n of Tchs., Loc. 2415 v. Hou. Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1172-77, 1179 (S.D. Tex. 2017) (explaining the Houston Independent School District's ("HISD") implementation of the Educational Value-Added Assessment System ("EVAAS"), a proprietary algorithmic system developed by private software company SAS, to measure teacher effectiveness by tracking teachers' impact on student test scores over time, where the court found that HISD violated procedural due process because the district delegated the calculation of teacher EVAAS scores entirely to SAS, which treated the algorithms and software as trade secrets and refused to divulge them to either HISD or the teachers themselves); Ark. Dep't of Hum. Servs. v. Ledgerwood, 530 S.W.3d 336, 338-39 (Ark. 2017); Elder v. Gillespie, 54 F.4th 1055, 1059-60, 1064-65 (8th Cir. 2022) (explaining the Arkansas Department of Human Services' ("DHS") implementation of the Resource Utilization Groups ("RUGs") assessment tool, a proprietary algorithmic system (initially developed for nursing homes and adapted by the state) to allocate Medicaid home-care hours for people with severe disabilities, where the courts found that DHS violated procedural due process because the department implemented the system without sufficient notice, and the algorithmic nature of the system and its treatment as proprietary prevented beneficiaries from understanding how their reduced care hours were calculated or effectively challenging the arbitrary cuts, which formed the basis of the procedural due process violations found by the courts). For more similar cases or disputes, see Bloch-Wehba, *supra* note 122, 1273-90.

133. *See supra* Part I.B.

134. *See* Grant Fergusson, *Outsourced & Automated: How AI Companies Have Taken over Government Decision-Making*, ELEC. PRIV. INFO. CTR. 2-4, 6-10 (Sept. 2023), https://epic.org/wp-content/uploads/2023/09/FINAL-EPIC-Outsourced-Automated-Report-w-Appendix-Updated-9.26.23.pdf [https://perma.cc/KU5X-3A9H].

ment by private vendors, notably, Deloitte, Optum, IBM, Thomson Reuters, and LexisNexis.[135] While disclosing the technical details and training data of these AI systems could mitigate potential harms arising from errors or bias, private vendors routinely claim trade secret protection to avoid disclosure.[136] For instance, EPIC requested the Illinois Department of Employment Security to open records of the unemployment fraud detection system developed by Pondera, a Thomson Reuters company acquired in 2020,[137] which is also used by the District of Columbia's Department of Human Services and Department of Employment Services.[138] The records requested by EPIC included its "source code, results from tests of its error rates, the factors that it took into account, and other information." [139] However, most of them were classified as "proprietary and confidential" with only a small number of documents disclosed with no further explanation.[140]

Indeed, in 2021, EPIC extensively studied the use of automated decision-making ("ADM") systems by the D.C. government in the areas of "health, economic opportunity, housing, criminal justice, education, children and family services, transportation, and contracting and procurement."[141] It originally tried to acquire the primary sources by sending Freedom of Information Act ("FOIA") requests to several governmental authorities but soon realized they could not rely solely on them as "[i]nformation about data sources or factors used in the systems and how the factors affect scores were shielded because of confidentiality or trade secret protections."[142]

B. Private Harms and Accountability

Beyond the public sector, private firms also develop and deploy AI systems that, despite their commercial origins, can inflict significant harms, such as impairing privacy, autonomy, equality, and safety.[143] Yet,

---

135. *See id.* at 37-40.

136. *See id*. at 8-9, 21-23.

137. *EPIC Screening and Scoring Spotlight: Pondera's Fraud Prediction Algorithms for Public Benefits*, ELEC. PRIV. INFO. CTR., https://epic.org/pondera-surveillance [https://perma.cc/RN58-LHGH] (last visited July 18, 2026).

138. Thomas McBrien et al., *Screened & Scored in the District of Columbia*, ELEC. PRIV. INFO. CTR. 11, 17, 24-25 (Nov. 2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf [https://perma.cc/HHS8-6WY2].

139. *Id.* at 17.

140. *Id.* at 17-18.

141. *Id.* at 42.

142. *Id.* at 42-43.

143. *See* Lu, *supra* note 18, at 19-34.

by asserting AI secrets, these firms may shield their AI systems from scrutiny and evade liability for the resulting harms.

On December 29, 2025, xAI, the AI company owned by Elon Musk, filed a federal lawsuit in the District Court for the Central District of California, challenging California's recent AI transparency law entitled Assembly Bill 2013 ("AB 2013"). [144] AB 2013 requires AI developers to publicly disclose the information on the training datasets of their AI models. [145] One of the main reasons California mandates disclosure of AI training datasets is its growing concern that AI models, such as Grok developed by xAI, are "facilitating the large-scale production of deepfake nonconsensual intimate images that are being used to harass women and girls across the internet, including via the social media platform X."[146] As such, the main aim is to address the potential risks and harms posed by AI technology to consumers.[147] xAI claimed, however, all "information about how it develops, trains and refines its unique gen AI models" as trade secrets protected under state and federal law.[148] As such, it argued that AB 2013, by mandating public disclosure of these trade secrets, essentially eliminated xAI's right to exclude others from appropriating its trade secrets, amounting to a per se taking without just compensation.[149] xAI sought a preliminary injunction on the enforcement of AB 2013, which was rejected by the district court.[150] When it comes to the trade secret claims, however, the reason for the rejection lies in the insufficient identification of protectable trade secrets at that stage.[151] It means that, had xAI described the information with sufficient particularity,[152] it *might* have succeeded in enjoining the mandated disclosure by invoking AI trade scerets—potential harms to

144. Complaint, X.AI LLC. v. Bonta, No. 2:25-cv-12295, slip op. at 1-7 (C.D. Cal. filed Dec. 29, 2025).

145. *Id.* at 3.

146. Press Release, Rob Bonta, Attorney General, Attorney General Bonta Launches Investigation into xAI, Grok over Undressed, Sexual AI Images of Women and Children (Jan. 14, 2026), https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-investigation-xai-grok-over-undressed-sexual-ai [https://perma.cc/V4KL-3LUB].

147. *See id. But cf.* Complaint, *supra* note 144, at 4 (questioning the consumer protection goals of AB 2013).

148. Complaint, *supra* note 144, at 3-4, 19-26.

149. *Id.* at 33-35.

150. *See* Plaintiff X.AI LLC's Notice of Motion and Motion for Preliminary Injunction at 1-3, *Bonta*, No. 2:25-cv-12295-JGB-SSC (C.D. Cal. Jan. 16, 2026); X.AI LLC v. Bonta, No. CV 25-12295 JGB (SSCx) (C.D. Cal. Mar. 4, 2026), ECF No. 35. (order denying preliminary injunction).

151. *See Bonta*, slip op. at 5-6.

152. *See id.* at 6.

consumers could continue to accrue, and any harms already caused by its AI model might be difficult to fully detect or adequately redress.[153]

The public faces a double bind: for one thing, even strong transparency laws like California's AB 2013 can be actively resisted by firms claiming their AI secrets, at least prolonging the disclosure schedule. [154] For another, where such laws are absent, the problem is even worse: AI companies operate in total secrecy, shielding the potential errors and biases of their AI systems, leaving victims with no recourse other than costly, lengthy, and uncertain lawsuits. For example, in 2023, a class action lawsuit was filed against UnitedHealth Group, Inc. and naviHealth, Inc. (collectively "UHC") for their use of nH Predict, an AI algorithm, to improperly deny elderly patients' care claims under the Medicare Advantage health insurance coverage issued by UHC.[155] The plaintiffs allege that UHC knew about the high error rate (ninety percent) of nH Predict but kept using it in claims determination.[156] UHC, however, denies any use of nH Predict.[157] In 2025, while the District Court for the District of Minnesota allowed some claims of plaintiffs, notably breach of contract, to proceed, it partially granted UHC's motion to dismiss and rejected claims it considered as preempted by the federal Medicare Act.[158] As some commentators worried, the court's rejection of those claims left patients "stuck navigating complex and slow Medicare regulations," with the core issue in the case blurred—AI algorithmic decision-making in healthcare.[159] As the litigation slowly progresses, the potential harms to patients remain unaddressed.[160]

Furthermore, companies increasingly rely on secret AI systems to automate their hiring processes, exposing job applicants to discriminatory harms that are hard to detect or challenge. On January 20, 2026, a

---

153. *See, e.g.*, Jasmine Mithani, *Women and Girls Are Taking Grok to Court over Sexualized Deepfakes*, THE 19TH (Mar. 17, 2026), https://19thnews.org/2026/03/women-girls-lawsuit-grok-ai-deepfakes [https://perma.cc/3NRP-ML46].

154. *See, e.g.*, Complaint, *supra* note 144, at 3-4.

155. *See* Plaintiff's Class Action Complaint at 1, Est. of Lokken v. UnitedHealth Grp., Inc., 766 F. Supp. 3d 835 (D. Minn 2025) (No. 0:23-cv-03514); Est. of Lokken v. UnitedHealth Grp., Inc., 766 F. Supp. 3d 835, 840-41 (D. Minn. 2025).

156. Plaintiff's Class Action Complaint, *supra* note 153, at 1-2; *Est. of Lokken*, 766 F. Supp. 3d at 841.

157. *Est. of Lokken*, 766 F. Supp. 3d at 841.

158. *See id.* at 845-49.

159. Rebecca Bower, *The Lokken Lawsuit: A Clash Between AI, Individualized Care, and the Court's Confusion*, J. HIGH TECH. L. BLOG (Nov. 11, 2025), https://sites.suffolk.edu/jhtl/2025/11/11/the-lokken-lawsuit-a-clash-between-ai-individualized-care-and-the-courts-confusion [https://perma.cc/6MB7-AV89].

160. For updates on the litigation, see *Estate of Gene B. Lokken v. UnitedHealth Group, Inc.*, O'NEILL INST. (Apr. 8, 2026), https://litigationtracker.law.georgetown.edu/litigation/estate-of-gene-b-lokken-the-et-al-v-unitedhealth-group-inc-et-al [https://perma.cc/JBB3-4J99].

class action lawsuit was filed in California against Eightfold AI, an AI hiring platform.[161] The complaint alleges that Eightfold AI provides a secret AI screening tool to numerous Fortune 500 companies, such as Microsoft and PayPal, to collect information on their job applicants and generate scores predicting their likelihood of success on the job.[162] As alleged succinctly in the complaint:

> Eightfold's technology lurks in the background of job applications for thousands of applicants who *may not even know Eightfold exists*, let alone that Eightfold is collecting personal data, such as social media profiles, location data, internet and device activity, cookies and other tracking, to create a profile about the candidate's behavior, attitudes, intelligence, aptitudes and other characteristics that applicants never included in their job application. These job applicants have *no meaningful opportunity to review or dispute Eightfold's AI-generated report* before it informs a decision about one of the most important aspects of their lives—whether or not they get a job.[163]

Similarly, in *Mobley v. Workday, Inc.*,[164] the plaintiff alleged that the AI-driven applicant-screening tool licensed by Workday, a leading provider of enterprise human resources management systems to a wide range of employers, systematically discriminated against African American, disabled, and older job applicants by rejecting them at disproportionate rates. [165] Nevertheless, despite applicants' structural inability to understand how AI systems assess them, Workday opposed, even during discovery, the disclosure of algorithms and other information essential to evaluating the system's internal decision-making processes.[166] Although the case primarily turns on the question of AI vendor liability,[167] it also exposes the similar tension between

---

161. *See* Class Action Complaint for Violations of the Fair Credit Reporting Act, California Investigative Consumer Reporting Agencies Act and Unfair Competition Law at 2-4, 7, Kistler v. Eightfold AI Inc., No. C26-00214 (Cal. Super. Ct. Jan. 20, 2026) [hereinafter Class Action Complaint for Violations of the Fair Credit Reporting Act].

162. *Id.* at 2; Jody Godoy, *AI Company Eightfold Sued for Helping Companies Secretly Score Job Seekers*, REUTERS (Jan. 21, 2026), https://www.reuters.com/sustainability/boards-policy-regulation/ai-company-eightfold-sued-helping-companies-secretly-score-job-seekers-2026-01-21 [https://perma.cc/87Z9-BERV].

163. Class Action Complaint for Violations of the Fair Credit Reporting Act, *supra* note 161, at 2 (emphasis added).

164. 740 F. Supp. 3d 796 (N.D. Cal. 2024).

165. *Id.* at 802-03.

166. *See* Chris Marr, *Workday Discovery Dispute Is Pivotal Moment for AI Bias Lawsuits*, BLOOMBERG L. (June 16, 2025), https://news.bloomberglaw.com/daily-labor-report/workday-discovery-dispute-is-pivotal-moment-for-ai-bias-lawsuits [https://perma.cc/K4C6-MVPG].

167. *Mobley*, 740 F. Supp. 3d at 804-08; Annette Tyman, *Mobley v. Workday: Court Holds AI Service Providers Could Be Directly Liable for Employment Discrimination Under "Agent" Theory*, SEYFARTH (July 19, 2024), https://www.seyfarth.com/news-insights/mobley-v-workday-court-

claims of AI secrets and principles of transparency.[168] Had Workday's AI tools been subject to meaningful scrutiny, whether by the broader public, the government, or public interest organizations, systematic biases might have been identified at an earlier stage, before causing harms to job applicants, many of whom may never realize that they were subject to discriminatory treatment. Yet, more than three years have passed since the case was first filed, and no final outcome has been reached. [169] Alarmingly, private actors are also deploying similar algorithmic screening tools in other contexts, such as renter or tenant screening, where their use may likewise produce systematic harms.[170]

C. Current Focuses and Responses

The tension between AI secrets and public transparency has attracted growing attention from both scholars and policymakers. Indeed, ever since source code secrecy emerged as a foundational feature of algorithmic systems, scholars have been calling for expanded mandates for disclosure, whether through existing transparency laws, new legislative interventions, or reforms to trade secret law doctrines.[171] For example, Bloch-Wehba argues that a suitable solution to AI opacity in the public sector still lies in updating existing transparency laws, notably FOIA. [172] She contends that courts should more critically examine attempts of AI system holders to invoke trade secret protection to shield algorithmic decision-making processes from public oversight. [173] She further calls for legislative movements to mandate more affirmative disclosure of key information about algorithmic

---

holds-ai-service-providers-could-be-directly-liable-for-employment-discrimination-under-agent-theory.html [https://perma.cc/LNN8-W5FK].

168. *See Mobley*, 740 F. Supp. 3d at 807-08.

169. *See* Docket, Mobley v. Workday, Inc., No. 3:23-cv-00770 (N.D. Cal. Feb. 21, 2023), https://www.courtlistener.com/docket/66831340/mobley-v-workday-inc [https://perma.cc/9RJ3-M4VK] (showing that litigation is ongoing as of Feb. 2026).

170. *See, e.g.*, Complaint at 5-10, Nat'l Ass'n of Consumer Advocs. v. RentGrow, Inc., No. 2024-CAB-006253 (D.C. Super. Ct. Oct. 1, 2024), https://plus.lexis.com/api/permalink/315a4889-6af0-4735-8767-df31908e0dcb/?context=1530671 [https://perma.cc/8WWR-ERJG] (alleging that RentGrow automatically generates tenant screening reports that contain serious errors and biases, which cause consumers to lose out housing opportunities); Complaint & Request for Investigation, Injunction, & Other Relief at 5-7, In re Airbnb, Inc. (FTC filed Feb. 26, 2020), https://epic.org/documents/in-re-airbnb [https://perma.cc/K2DE-STTR] (alleging that Airbnb uses secret algorithms to screen renters).

171. *See, e.g.*, Bloch-Wehba, *supra* note 122, at 1307-08; Lu, *supra* note 25, at 131-39; Tschider, *supra* note 88, at 715, 720-23; Katyal, *The Paradox*, *supra* note 11, at 1250-53; Sprankling, *supra* note 6, at 218-20; Villasenor, *supra* note 11, at 529-32; Lee, *supra* note 22, at 110-11; Dreyfuss, *supra* note 11, at 10-12.

172. Bloch-Wehba, *supra* note 122, at 1313-14.

173. *Id.*

systems used by governmental agencies, noting that FOIA operates only as a reactive regime that requires only the disclosure of existing records in response to individual requests, rather than proactive transparency. [174] Building on a different regulatory model, Lu draws on the Securities and Exchange Commission's disclosure framework to propose new algorithmic disclosure requirements. [175] Under this approach, AI firms would be required to disclose critical information about their algorithmic systems to shareholders, enabling monitoring and scrutiny aimed at preventing potential harms. [176] Villasenor, instead, argues that, to preserve AI secrets while promoting transparency, AI transparency requirements can call for disclosure of high-level descriptions of the concerned AI systems that do not implicate AI secrets.[177] For example, even where training datasets themselves may be protected as AI secrets, AI companies can nonetheless be required to disclose negative information, including whether particular categories of data, those more likely to generate bias or error, were excluded from the training process.[178]

Other scholars propose reforming existing trade secret law doctrines to facilitate greater disclosure of AI secrets. Katyal draws attention to the whistleblower doctrine in the DTSA and argues that it can be used to encourage more internal employees who discover potential harms caused by AI systems to disclose relevant AI secrets in the public interest. [179] Similarly, Sprankling proposes expanding the existing DTSA whistleblower protection to grant broad immunity to any internal members who disclose AI secrets to a designated governmental official when they have reasonable belief that an AI system poses harms to public health or safety.[180] Likewise, Matulionyte and Lee, albeit under the Australian common law context, argue for broadening the public interest defense to facilitate disclosure by information recipients under duty of confidence to ensure adequate transparency surrounding AI medical devices.[181]

Despite their distinct approaches, these proposals share a common focus: enhancing the disclosure of AI related information to enable more

174. *Id.* at 1314.
175. Lu, *supra* note 25, at 127-28, 138-39.
176. *Id.* at 138-39.
177. Villasenor, *supra* note 11, at 529.
178. *Id*. at 529-30.
179. Katyal, *Private Accountability*, *supra* note 11, at 131-37.
180. Sprankling, *supra* note 6, at 218-20.
181. Matulionyte & Lee, *supra* note 11, at 29-35.

effective public scrutiny. [182] Indeed, this focus also characterizes the prevailing regulatory responses adopted by policymakers across jurisdictions in their efforts to alleviate AI opacity. In the United States, several states have introduced new acts that mandate more disclosure of information related to AI systems. [183] Notably, California's Generative AI Training Data Transparency Act mandates that developers disclose a high-level summary of the training datasets for AI systems made available in the state. [184] This includes disclosing dataset sources, the number and types of data points, and a description of how the data was cleaned, processed, or modified[185]—categories that xAI claimed as their trade secrets. [186] In a similar vein, the Colorado AI Act requires developers of high-risk AI systems to make critical technical documentation, including high-level summaries of the type of training data and a description of the data governance measures implemented to assess the suitability, representativeness, and potential bias of the datasets used.[187]

The shared scholarly and regulatory focus on enhancing the disclosure of AI-related information does help mitigate the potential harms posed by AI systems by making more information available for public scrutiny. As such, it is clearly one of the current paths for governments to continue in the future. However, these mandated-disclosure approaches have clear limitations, as it has to deal with AI developers' AI secrets claims with great caution. The main reason is that, *if the information claimed by AI developers truly amounts to trade secrets*, mandated-disclosure might be considered an unconstitutional taking, as disclosing

182. Katyal, *Private Accountability*, *supra* note 11, at 131-37; Sprankling, *supra* note 6, at 218-20; Matulionyte & Lee, *supra* note 11, at 29-35.

183. *See e.g.*, COLO. REV. STAT. § 6-1-1702(2) (2026) (mandating that developers of high-risk AI provide deployers with "high-level summaries" of training data and detailed documentation on data governance measures—including efforts to mitigate bias and ensure the suitability of data sources—to prevent algorithmic discrimination); TEX. BUS. & COM. CODE ANN. § 552.051(d) (West 2026) (establishing disclosure requirements for government agencies and healthcare providers to ensure "clear and conspicuous" notice when consumers interact with AI, while notably exempting most private commercial and employment contexts from similar transparency mandates); CAL. CIV. CODE § 3111(a) (West 2026) (requiring generative AI developers to post a "high-level summary" of training datasets on their websites, specifically mandating disclosure of dataset sources, the number of data points used, and whether the data includes copyrighted materials or personal information); 775 ILL. COMP. STAT. 5/2-101 (2026) (amending the Illinois Human Rights Act to prohibit algorithmic discrimination in employment decisions and mandating that employers provide prior notice to applicants and employees when AI is used in recruitment, hiring, or disciplinary processes).

184. CAL. CIV. CODE § 3111.

185. *Id.* (listing, in total, twelve examples for information relating to training datasets that should be disclosed to the public).

186. *See supra* note 148 and accompanying text.

187. COLO. REV. STAT. § 6-1-1702(2).

trade secrets destroys their competitive advantage outright.[188] In other words, whether under established transparency frameworks like FOIA or newly enacted state AI acts, a developer's mere assertion of AI secrets can significantly obstruct the disclosure process.[189] This is because when AI secrets are asserted, critical and complex questions arise that require delineation, notably, whether the claimed information satisfies trade secret requirements.[190] This delay occurs regardless of the claim's ultimate legal merits or the rigor of the court's scrutiny, as the procedural requirements to adjudicate trade secret validity are inherently time-consuming.[191] As will be argued in the next Part, this is due to the inherent and structural features of the trade secret law, which essentially limit the functions of these scholarly proposals and policy responses. [192] Therefore, a potential complementary path to the mandated-disclosure approaches is to focus on the structural features of trade secret law and to develop solutions under which AI developers' secrecy claims would not unduly delay or undermine regulatory oversight of AI systems.[193]

That being said, the following Part critically examines how the structural features of trade secret law contribute to the tension between AI secrets and transparency, and how it limits the effectiveness of the mandated-disclosure approaches.[194] It then sets out this Article's normative proposal, which targets the structural features and supplements the mandated-disclosure approaches.[195]

III. AI TRANSPARENCY CONCERNS: THE STRUCTURAL FAILURE OF TRADE SECRET LAW

While AI transparency evidently clashes with AI secrets, the tension is premised on the assumption that all AI-related information claimed by AI developers as AI secrets constitute protectable trade secrets. The presumption, however, often fails due to unique structural fea-

188. *See* Complaint, *supra* note 144, at 33-35.

189. When AI developers attempt to invoke trade secret protection for their AI-related information, the FOIA and many state regulatory frameworks exhibit significant deference, providing statutory safeguards that prevent mandatory disclosures from compromising a developer's proprietary AI secrets. *See, e.g.*, COLO. REV. STAT. § 6-1-1702(6); Varadarajan, *supra* note 122, at 484-95 (detailing FOIA's exemptions for trade secrets and other confidential information).

190. *See* Bloch-Wehba, *supra* note 122, at 1300-03; Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 153-59 (2018).

191. For example, the disputes on trade secret identification itself are difficult, complex, and costly. *See* Charles Tait Graves & Brian D. Range, *Identification of Trade Secret Claims in Litigation: Solutions for a Ubiquitous Dispute*, 5 NW. J. TECH. & INTELL. PROP. 68, 72-75 (2006).

192. *See infra* Part III.B.

193. *See infra* Part IV.A–B.

194. *See infra* Part III.A.

195. *See infra* Part III.B.

tures of trade secret law—its inherently uncertain and expansive protection boundaries.[196] As will be detailed below, while these structural features were once celebrated as a primary strength of trade secret law compared to patent law, they have evolved into structure failures in modern days and particularly in the context of AI secrets.[197]

A. Structural Features: Resilience and Flexibility in Trade Secret Law

The most salient feature of trade secret law lies in the inherent indeterminacy of its protection scope or boundaries. Indeed, the law heavily relies on firms' self-help measures to offer protection with no need for any pre-approval process.[198] Firms are afforded ample opportunity to assert trade secret protection over their information, dispensing the need to go through the lengthy and costly registration and examination processes required by patent law.[199] In turn, the absence of any formal registration system means that trade secret holders are not legally required to define any boundary or scope of their claimed trade secrets prior to litigation. [200] It is only after initiating legal action that firms must identify the scope of their claimed trade secrets with a certain degree of specificity.[201] Consequently, unlike in the patent context, where firms must incur the upfront costs of constructing their claims for patent examination, trade secret law preserves a firm's time and resources by requiring the identification of trade secrets only when a specific dispute arises.[202]

This flexibility offered by trade secret law is one of the main reasons firms choose trade secret law instead of patent law for their innovative ideas.[203] Particularly for start-ups with constrained funding,

196. *See* Sandeen & Aplin, *supra* note 11, at 444-45; Villasenor, *supra* note 11, at 526-29.

197. *See infra* Part III.B.

198. Trade secret law recognizes the self-help measures adopted by information holders to safeguard their secrets, while dispensing their needs to adopt overly excessive measures. *See* Chen, *supra* note 9, at 44-45; Lichtman, *supra* note 56, at 230-32; Risch, *supra* note 56, at 42-43; Lemley, *Surprising Virtues, supra* note 14, at 333-34.

199. *See* Andrew A. Schwartz, *The Corporate Preference for Trade Secret*, 74 OHIO ST. L.J. 623, 645 (2013). Firms may use confidentiality agreements to claim a lot of information as their protectable trade secrets. *See* Camilla A. Hrdy & Christopher B. Seaman, *Beyond Trade Secrecy: Confidentiality Agreements That Act Like Noncompetes*, 133 YALE L.J. 669, 689-93 (2024).

200. *See* Varadarajan, *supra* note 41, at 1552; Varadarajan, *supra* note 64, at 1411; Graves & Range, *supra* note 191, at 72.

201. *See* Elizabeth A. Rowe, *Snapshot of Trade Secret Developments*, 60 WM. & MARY L. REV. ONLINE 45, 55-58 (2019); Peter J. Toren, *Beyond State Law: The Ninth Circuit's New Framework for DTSA Trade Secret Identification*, IPWATCHDOG (Aug. 27, 2025, 11:01 AM), https://ipwatchdog.com/2025/08/27/beyond-state-law-ninth-circuits-new-framework-dtsa-trade-secret-identification [https://perma.cc/7L3K-N9GH] (discussing the identification requirements in notable state laws as well as their influence on the federal law).

202. *See* Varadarajan, *supra* note 41, at 1552; Graves & Range, *supra* note 191, at 72.

203. *See* Schwartz, *supra* note 199, at 644-45.

trade secret law can serve as a more cost-efficient alternative, allowing them to redirect resources that would otherwise be spent on claims construction, and patent application and examination toward continued investment in Research & Development ("R&D").[204]

Meanwhile, as mentioned, the modern trade secret law is rather resilient concerning its subject matter coverage, embracing essentially all information.[205] It thus renders trade secret law a popular choice for firms to protect their unpatentable information, notably technical information that may fail novelty or non-obviousness requirements, or business information.[206] For instance, as mentioned above, when algorithms face difficulties in receiving protection from either copyright or patent law, trade secret law's resilience in subject matter coverage offers a last resort for firms to protect their algorithms from misappropriation.[207]

As such, trade secret law's streamlined protection process, lack of a requirement for pre-identification of boundaries, and broad subject matter coverage define a unique set of features that information holders welcome as a supplemental or even substitute path to patent protection.[208] However, the very features that make trade secret law a flexible and resilient protection route for innovative information also render it a powerful tool for strategic abuse.[209] As elaborated below, the absence of *ex-ante* boundary identification through an official registration process, coupled with loose subject matter and other protection requirements, once being virtues of efficiency, now facilitate a system of overclaiming that stifles AI transparency.[210]

B. The Structural Failures: Inherent Susceptibility to Strategic Overclaiming

The very features of trade secret law that once provided resilience and flexibility to innovators are now vulnerable to exploitation by AI developers to overclaim AI secrets, effectively extending trade secret

---

204. *See* David S. Levine & Ted Sichelman, *Why Do Startups Use Trade Secrets?*, 94 NOTRE DAME L. REV. 751, 761-63 (2018); Stuart J.H. Graham et al., *High Technology Entrepreneurs and the Patent System: Results of the 2008 Berkeley Patent Survey*, 24 BERKELEY TECH. L.J. 1255, 1310-12 (2009).

205. *See supra* notes 60-62 and accompanying text; Chen, *supra* note 9, at 13-14.

206. *See* Levine & Sichelman, *supra* note 204, at 758-59; Graham et al., *supra* note 204, at 1312; Daniel C. Munson, *The Patent-Trade Secret Decision: An Industrial Perspective*, 78 J. PAT. & TRADEMARK OFF. SOC'Y 689, 690 (1996).

207. *See supra* notes 92-94 and accompanying text.

208. *See* W. Nicholson Price II, *Expired Patients, Trade Secrets, and Stymied Competition*, 92 NOTRE DAME L. REV. 1611, 1616-18 (2017); Levine & Sichelman, *supra* note 204, at 763-66.

209. *See* Graves & Katyal, *supra* note 40, at 1351-52.

210. *See see infra* text accompanying notes 211-27.

protection to information that should remain publicly available for scrutiny. Indeed, the overclaiming issue is not a novel problem under the modern trade secret law, and scholars are proposing new limiting doctrines to cabin its expansive reach.[211] However, only few scholars have explicitly linked the problem of overclaiming, driven by trade secret law's unique features, to the context of AI transparency.[212] As such, this Article contributes to this emerging discourse by arguing that a significant portion of the AI transparency concerns stem from such overclaiming, which can be another regulatory focus to release substantial information for public scrutiny without getting entangled in complex disputes over the validity of AI secrets claimed by developers.

As mentioned, trade secret law offers a cost-efficient path for information holders to protect their innovations with no prerequisites for pre-identification and examination.[213] It means that the law gives AI developers broad authority to self-define their AI secrets.[214] Absent any public authority scrutinizing and supervising the self-identification by AI developers, they enjoy significant deference in deciding what to include and how to describe their AI secrets.[215] Trade secret's information paradox explains their nearly unrestrained power to define their own secrets. [216] Because no public authority pre-screens trade secret claims, those outside the corporate veil cannot know what constitutes protectable trade secrets unless they are disclosed, an act that would immediately destroy the trade secret status, if any.[217] Therefore, information holders

---

211. *See, e.g.*, Fishman & Varadarajan, *supra* note 40, at 1405-09, 1411-12 (arguing that current trade secret law is overly protective and proposing the reintroduction of the historical investment requirement); Joseph P. Fishman & Deepa Varadarajan, *Similar Secrets*, 167 U. PA. L. REV. 1051, 1077-79 (2019) (arguing that the law defines "infringing use" too broadly and proposing a narrower version); Varadarajan, *supra* note 64, at 1445-48 (arguing that current trade secret law lacks an effective limiting doctrine and proposing the introduction of a fair use doctrine to address that issue); Hrdy & Seaman, *supra* note 199, at 707-08 (arguing that confidentiality agreements often operate as de facto noncompete clauses that deter employee job-hopping in practice, yet lack the limiting doctrines that normally constrain the overreach of formal noncompete clauses); Hrdy & Lemley, *supra* note 50, at 19-20, 42-43 (arguing that the scope of the current trade secret law is too expansive, reaching information that is not used by holders and proposing the reintroduction of the historical continued use requirement); Longxuan Zhao & Yang Chen, *Legally Supported Bullying? Legal Consciousness on Noncompete Agreements in China*, SOC. & LEGAL STUDS. 1, 16-17 (2026), https://doi.org/10.1177/09646639251411409 [https://perma.cc/W9DX-QQK9] (documenting trade secret overclaiming issue in the context of modern non-compete practices).

212. *See supra* note 26; Sandeen & Aplin, *supra* note 11, at 443-44, 446-48; Villasenor, *supra* note 11, at 526-28; Katyal, *The Paradox*, *supra* note 11, at 1227-29, 1269.

213. *See supra* notes 199-203 and accompanying text.

214. Katyal, *The Paradox*, *supra* note 11, at 1269; Graves & Katyal, *supra* note 40, at 1350.

215. *See* Katyal, *The Paradox*, *supra* note 11, at 1269-70.

216. Christopher Buccafusco et al., *Trade Secrecy's Information Paradox*, 100 NOTRE DAME L. REV. 925, 949 (2025).

217. *Id.* at 958-64.

are entrusted to determine what information is shared with the public and what is maintained factually secret and claimed as secrets. [218] As such, when faced with transparency mandates concerning their AI systems, developers may either define their AI secrets strategically or simply include as many components as possible within their self-designated boundaries.[219] After all, it is standard practice for companies to define their protectable confidential information as broadly as possible in nondisclosure agreements ("NDAs") signed by employees and external business partners. [220] Companies can easily leverage these sweeping NDAs as preliminary evidence of their expansive AI secrets, deterring potential transparency requests.[221]

That connects to another salient feature of trade secret law that exacerbates the overclaiming AI secrets: trade secret law's broad subject matter. Though the broad subject matter eligibility provides the necessary flexibility to accommodate the practical needs of protecting diverse AI components, this very flexibility invites overclaiming. [222] Because trade secret protection can extend to virtually any commercial information without meaningful qualifying conditions, [223] coupled with information holders' unrestricted authority of self-definition, developers can arguably assert every element of an AI system as a potentially protectable secret as they wish.[224] Consequently, establishing a prima facie objection to AI developers' trade secret claims based on subject matter limitations is exceptionally difficult. Absent any explicit categorial limitations found in other IP regimes,[225] trade secret law, in essence, allows AI developers to assert protection over the entirety of their AI systems without having to distinguish eligible from ineligible elements, unless and until those assertions are challenged.[226]

Once a claim is challenged, the three statutory requirements of trade secret protection bear the entire burden of filtering out unprotectable elements. If a claim is successfully challenged, these requirements,

---

218. Graves & Katyal, *supra* note 40, at 1350-51.

219. *Id.* at 1351.

220. *See* Hrdy & Seaman, *supra* note 199, at 693; Varadarajan, *supra* note 41, at 1564-66.

221. Varadarajan, *supra* note 41, at 1566 (explaining that some courts allow contractual expansions of trade secret subject matter).

222. *See* Graves & Katyal, *supra* note 40, at 1350-51.

223. *See supra* note 62 and accompanying text.

224. *See* Graves & Katyal, *supra* note 40, at 1351.

225. For example, patent law categorically excludes abstract ideas from protection. *See* 35 U.S.C. § 101; Alice Corp. v. CLS Bank Int'l, 573 U.S. 208, 217-19 (2014) (holding that abstract ideas implemented on a generic computer are not patent-eligible). Copyright law excludes functional elements from protection. *See* 17 U.S.C. § 102(b) (excluding "procedure[s], process[es], system[s], [and] method[s] of operation" from copyright protection).

226. *See* Graves & Range, *supra* note 191, at 77-78.

in some ways, do serve as gatekeepers to avoid the overclaiming of AI secrets.[227] However, a successful challenge is difficult to achieve. For one thing, given the relatively low evidentiary hurdle that AI developers face in proving that their AI components satisfy the requirements (notably the value and reasonable secrecy measures requirements), succeeding in a challenge is not something we can easily take for granted.

First, the bar to meet the value requirement is notoriously low, and it is very easy to satisfy.[228] Even though scholars have offered various doctrinal interpretation approaches to recalibrate the value requirement,[229] many courts rubber stamp it, presume its satisfaction, or take expansive view over it.[230] Also, under the modern trade secret law, any actual or *potential* economic value that the AI components confer on the holder is sufficient to satisfy the requirement.[231] For instance, as previously noted, some scholars propose new mandated-disclosure requirements that would compel AI developers to reveal negative information, such as the particular types datasets that they deliberately exclude from their training process. [232] However, AI developers may counter these transparency mandates by categorizing this information as negative know-how, a recognized class of trade secrets where the knowledge of what *not* to use may provide potential competitive edge when kept confidential from competitors.[233] Namely, they may argue that such negative information forms an integral part of their data curation strategy in the whole AI training process, enabling them to more effectively reduce bias and improve their models' real-world performance, thereby conferring a

227. *See* Sandeen & Aplin, *supra* note 11, at 451-58.

228. *See* David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 318-19 (2009) [hereinafter Almeling et al., *Federal Courts*] (explaining that nearly eighty-five percent of cases studied did not decide on the value requirement, and the majority of cases where the courts decided on the requirement ruled that the element was satisfied); David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 92 (2010) [hereinafter Almeling et al., *State Courts*] (explaining similar statistics in state court cases). The statistics in Chinese trade secret cases indicate similar features. *See* Yang Chen, *Demystifying China's Trade Secret Law in Action: A Statistical Analysis*, 13 QUEEN MARY J. INTELL. PROP. 198, 215-16 (2023); *see also* Hrdy & Lemley, *supra* note 50, at 27-29.

229. *See, e.g.*, Sandeen & Aplin, *supra* note 11, at 455-56; Hrdy, *supra* note 43, at 576-86.

230. Hrdy, *supra* note 43, at 577; Hrdy & Lemley, *supra* note 50, at 31-41.

231. UNIF. TRADE SECRETS ACT § 1(4) (UNIF. L. COMM'N 1985); 18 U.S.C.A. § 1839(3)(B); *cf.* Hrdy, *supra* note 9, at 99 (detailing the court's rejection of a request for a preliminary injunction because the plaintiff failed to prove that the algorithms possessed independent economic value derived from secrecy, given that the plaintiff had neither commercialized any products nor earned any revenue from them).

232. Villasenor, *supra* note 11, at 529-30.

233. Charles Tait Graves, *The Law of Negative Knowledge: A Critique*, 15 TEX. INTELL. PROP. L.J. 387, 394-400 (2007); POOLEY, *supra* note 61, at § 4.05 ("One of the most significant developments in trade secret law since the original Restatement has been the extension of coverage to information that has 'potential,' or even 'negative' value.").

competitive advantage.[234] After all, the prevailing view is still that the commercial value brought by trade secrets need not be great, just not trivial.[235] The doctrinal threshold is so low that, even if challenged, defendants face an almost insurmountable burden in disproving the commercial value of claimed trade secrets, which explains why the value requirement is often not a contested issue in disputes at all.[236]

Second, although trade secret law requires developers to take affirmative steps to protect their information, this standard does not demand "heroic" measures to ensure absolute secrecy.[237] Rather, the "reasonableness" inquiry is notoriously flexible and fact-specific, imposing a burden that is not overly difficult to meet in practice.[238] While no single measure is legally dispositive,[239] empirical studies indicate that courts increasingly attach disproportionate significance to NDAs to satisfy the reasonable secrecy requirement.[240] Given that the use of NDAs is both effortless and ubiquitous,[241] permitting these agreements to too heavily shoulder the evidentiary burden severely diminishes the substantive rigor of the requirement. After all, requiring employees and business collaborators to sign NDAs are generally aligned with the practices of AI developers that claim AI secrets. For example, as evidenced by the aforementioned recent conviction of a former software engineer for misappropriating Google's AI secrets, the company requires all employees to sign employment agreements containing broad and expansive confidentiality clauses. [242] Setting NDAs aside, AI developers such as Google also implement most other common types of security measures,

---

234. *See What Is Data Curation and Why Does It Matter When Training AI?*, INVISIBLE (Apr. 24, 2025), https://invisibletech.ai/blog/why-data-curation-is-the-key-to-achieving-deployment-ready-ai [https://perma.cc/WZ8U-WNFS]; Tony Rhem, *The Importance of Data Curation and Preparation for AI Solutions*, THE KNOWLEDGE MANAGEMENT DEPOT (Jul. 31, 2025), https://knowledgemanagementdepot.com/2025/07/31/the-importance-of-data-curation-and-preparation-for-ai-solutions [https://perma.cc/6275-L8VM].

235. *See* POOLEY, *supra* note 61, at § 4.05.

236. *See supra* note 228; Almeling et al., *Federal Courts*, *supra* note 228, at 318-19; Almeling et al., *State Courts*, *supra* note 228, at 92; Chen, *supra* note 228, at 215-16; Hrdy & Lemley, *supra* note 50, at 27-29.

237. *See* POOLEY, *supra* note 61, at § 4.04(2).

238. *See id.*; *see also* Varadarajan, *supra* note 41, at 1557-58; Varadarajan, *supra* note 57, at 372-73.

239. *See* Varadarajan, *supra* note 41, at 1557.

240. *See* Almeling et al., *State Courts*, *supra* note 228, at 80-83; Almeling et al., *Federal Courts*, *supra* note 228, at 321-24; Chen, *supra* note 228, at 219-20.

241. *See* Hrdy & Seaman, *supra* note 199, at 682-84.

242. *See* Superseding Indictment at 4-5, United States v. Ding, No. 3:24-cr-00141-VC (N.D. Cal. Feb. 4, 2025).

such as physical safeguards and technical protections, that courts generally consider as part of the reasonableness calculus.[243]

The secrecy requirement probably remains a potentially more effective doctrinal screen, which, at least, can filter out information that is publicly available or readily ascertainable.[244] And then one of the future reform focuses, as proposed by scholars in more general contexts, can be to better calibrate the value and reasonable secrecy measures requirements, while requiring courts to more substantively examine the secrecy requirement.[245] However, when transparency mandates collide with AI secret claims, challenging these assertions is itself burdensome and costly, further compounding the difficulty of securing a successful outcome.[246] Also, even if a challenge succeeds and the disclosure of non-secret AI information is legally mandated, years of litigation may have already passed, significantly delaying meaningful disclosure transparency.[247] Some public harms arising from unsafe AI models that might otherwise be avoided may materialize due to the prolonged timeline of the disclosure.[248]

Consequently, the mandated-disclosure approaches, favored by the recent scholarly and regulatory movements, may remain rather constrained as long as it has to confront AI developers' unchecked assertions of AI secrets. The broad subject matter eligibility of trade secret law, coupled with AI developers' unrestrained authority for self-determination, invites the overclaiming of AI secrets to counter transparency mandates. [249] Even when these claims are challenged, the low threshold for satisfying most trade secret requirements, combined with a typically lengthy and costly litigation process, means that challenges, even if they succeed, may fail to confer benefits that justify the costs.[250] Accordingly, while the mandated-disclosure approaches partially improves AI transparency, there may be other approaches that target these structural features of trade secret law to serve a supplementary role.

---

243. *See id.* at 3-5; *cf.* Almeling et al., *State Courts*, *supra* note 228, at 81-82; Almeling et al., *Federal Courts*, *supra* note 228, at 322; Chen, *supra* note 228, at 220.

244. *See supra* note 52 and accompanying text.

245. *See* Sandeen & Aplin, *supra* note 11, at 455-56; Hrdy, *supra* note 43, at 576-86; Bloch-Wehba, *supra* note 122, at 1313-14.

246. *See* Graves & Katyal, *supra* note 40, at 1350-51; Sharon K. Sandeen, *The DTSA: The Litigator's Full-Employment Act*, 72 WASH. & LEE L. REV. ONLINE 308, 319 (2015).

247. *See, e.g.*, Graves & Katyal, *supra* note 40, at 1350 (explaining that litigation on validating trade secrets can take years); David E. Pozen, *Freedom of Information Beyond the Freedom of Information Act*, 165 U. PA. L. REV. 1097, 1116-17 (2017) (documenting how FOIA requests and follow-up appeal systems are consistently plagued by severe delays).

248. Graves & Katyal, *supra* note 40, at 1350-52, 1377-79.

249. *Id.* at 1370, 1377-79.

250. Graves & Katyal, *supra* note 40, at 1350-51; Sandeen, *supra* note 246, at 318-19.

IV. AI SECRETS REGISTRATION

Against this backdrop, this Part proposes an AI secrets registration system designed to address the structural failures of trade secret law in the context of AI secrets. The first section details the structural design of the proposed system, explaining how it draws comparative insights and support from and builds upon the existing registration or recordation systems in other areas of law across multiple jurisdictions.[251] This is followed by an analysis of how the proposed system can ameliorate the tension between AI secrets and transparency by targeting the aforementioned structural failures and supplementing the mandated-disclosure approaches.[252] It also explores the ancillary benefits that the system can provide.[253] The final section concludes by noting the limitations of the proposal.[254]

A. AI Secrets Registration System

1. Applicable Scope

As a threshold matter, the proposed AI secrets registration system is not an all-encompassing framework for every AI system containing trade secrets. Instead, drawing insights partially from the E.U. AI Act,[255] it only applies to these AI systems already placed on the market or put into service by developers that have the possibility to affect the public. This scope encompasses systems that either provide services directly to end-user consumers, or are licensed to private entities or governmental agencies whose algorithmic decisions can directly impact individual interests. It ensures that any AI systems posing a risk of potential and actual harm and directly conflicting with transparency demands, as exemplified by the categories detailed above, [256] are included in the registration scheme. At the same time, this scope expressly excludes AI systems that have not yet been placed on the market or put into service

251. *See infra* Part IV.A.
252. *See infra* Part IV.B.
253. *See infra* Part IV.B.
254. *See infra* Part IV.C.
255. Council Regulation 2024/1689 of June 13, 2024, Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), 2024 O.J. (L 2024/1689) 7 (EU) [hereinafter Council Regulation 2024/1689].
256. For examples of these applicable scenarios, see *supra* Part II.A–B.

while they are still undergoing research, testing, or development.[257] This exclusion can avoid burdening AI developers when they have not commercialized their AI models, thus saving resources and preserving their incentives to continue innovating. In addition, by focusing exclusively on market-deployed systems that may pose societal risks, this scope inherently excludes those internal AI models developed specifically for the sole purpose of scientific research and development.[258] Ultimately, it aims to avoid overregulation by excluding AI models that are unlikely to pose external societal harms and therefore do not implicate AI transparency conflicts.

1. Registration System

When designing the proposed AI secrets registration system, valuable insights can be drawn from other registration or third-party review systems across different jurisdictions. In fact, China's recent data property registration systems developed by local governments may serve as a model on how the proposed registry may work.[259] Though the data registration systems maintained by local governments vary, a notable number require the registered data to qualify as trade secrets,[260] making them suitable templates for the proposed AI secrets registration system. Specifically, many local data registration systems conduct only a

257. For comparative insights from the EU, see Council Regulation 2024/1689, *supra* note 255, at 46.

258. For comparative insights from the EU, see *id.*

259. *See, e.g.*, *Tianjin Shi Shuju Zhishi Chanquan Dengji Banfa (Shixing)* (天津市数据知识产权登记办法 （试行)) [Provisional Measures for the Registration of Data Intellectual Property Rights of Tianjin (Trial)] (promulgated by Tianjin Intell. Prop. Off., Jan. 8, 2024, effective Jan. 8, 2024), arts. 5-8, https://zscq.tj.gov.cn/zwgk/zcwj/zscqwj/202402/t20240227_6545482.html [https://perma.cc/96GU-QX4H] (China) [hereinafter Provisional Measures for the Registration of Data Intellectual Property Rights of Tianjin (Trial)]; *Beijing Shi Shuju Zhishi Chanquan Dengji Guanli Banfa (Shixing)* (北京市数据知识产权登记管理办法（试行)) [Provisional Administrative Measures for the Registration of Data Intellectual Property Rights (Trial)] (promulgated by Beijing Intell. Prop. Off., May 30, 2023, effective June 19, 2023), arts. 2, 4-5, 10, https://www.beijing.gov.cn/zhengce/shengcefagui/202311/t20231115_3301983.html [https://perma.cc/WQ4K-6U7T] (China) [hereinafter Provisional Administrative Measures for the Registration of Data Intellectual Property Rights (Trial)]; *Shandong Sheng Shuju Zhishi Chanquan Dengji Guanli Guize (Shixing)* (山东省数据知识产权登记管理规则（试行)) [Provisional Rules for the Administration of Data Intellectual Property Rights Registration of Shandong Province (Trial)] (promulgated by Shandong Provincial Admin. for Mkt. Regul., Oct. 16, 2023, effective Oct. 16, 2023), arts. 13-15, http://amr.shandong.gov.cn/art/2023/10/16/art_92482_10304699.html [https://perma.cc/2LA8-YT7F] (China). For an introduction of these local data registration practices, see Liu Jianchen (刘建臣), *Shuju Zhishi Chanquan Dengji de Diceng Luoji* (*数据知识产权登记的底层逻辑*) [*The Underlying Logic of Data Intellectual Property Registration*], 27 HUADONG ZHENGFA DAXUE XUEBAO (华东政法大学学报) [J.E. CHINA U. POL. SCI. & L.] 79, 79-93 (2024) (China).

260. *See* Chen, *supra* note 9, at 8.

formality examination upon receiving a data registration request. [261] Some of these systems conduct limited substantive examinations only when there are salient problems that would prevent registration.[262] These salient issues typically include instances where the data products might harm the public interest, personal privacy, or when they violate laws and regulations. [263] Beyond that, once an application passes the formality review, a public record is generated and published.[264] Nevertheless, to avoid disclosing the contents of the registered data, which could destroy its inherent value, these systems publish only a record consisting of a brief description to the public.[265] This record typically includes just the applicant's information, the name of the dataset, its applicable scenarios, data sources, and a brief summary of the algorithmic rules. [266] More importantly for present purposes, some local systems allow applicants, especially when the underlying data file is large or sensitive, to submit a hash value or verification code generated from the data rather than

261. *See, e.g.*, Provisional Administrative Measures for the Registration of Data Intellectual Property Rights (Trial), *supra* note 259, at arts. 8, 10; Provisional Measures for the Registration of Data Intellectual Property Rights of Tianjin (Trial), *supra* note 259, at art. 9; *Shanghai Shi Shuju Chanpin Zhishi Chanquan Dengji Cunzheng Zanxing Banfa* (上海市数据产品知识产权登记存证暂行办法) [Interim Measures for the Registration and Deposit of Intellectual Property Rights of Data Products in Shanghai] (promulgated by Shanghai Intell. Prop. Admin. & Shanghai Mun. Bureau of Data, Nov. 8, 2024, effective Dec. 8, 2024), art. 6, https://sipa.sh.gov.cn/zwgk_zxxxgk?20241114/628f6a97d7ef4b8c9bbcf4a0408ab909.html [https://perma.cc/MQ78-ELYH] (China) [hereinafter Interim Measures for the Registration and Deposit of Intellectual Property Rights of Data Products in Shanghai]; *Jiangsu Sheng Shuju Zhishi Chanquan Dengji Guanli Banfa (Shixing)* (江苏省数据知识产权登记管理办法（试行）) [Measures for the Administration of Data Intellectual Property Registration of Jiangsu Province (Trial)] (promulgated by Jiangsu Province Data Intell. Prop. Registration Mgmt. Measures, Jan. 10, 2024, effective Feb. 21, 2024), art. 14, https://perma.cc/HN2W-JYAY (China).

262. *See, e.g.*, *Hunan Sheng Shuju Zhishi Chanquan Dengji Guanli Banfa (Shixing)* (湖南省数据知识产权登记管理办法（试行)) [Measures for the Administration of Data Intellectual Property Registration of Hunan Province (Trial)] (promulgated by Hunan Prov. Admin. for Mkt. Regul., Sept. 19, 2024, effective Sept. 19, 2024), arts. 7, 9, https://www.damdjt.com/article/detail/48c2c6862534f737860802646742ade0 [https://perma.cc/C6WE-633J] (China) [hereinafter Measures for the Administration of Data Intellectual Property Registration of Hunan Province (Trial)]; Interim Measures for the Registration and Deposit of Intellectual Property Rights of Data Products in Shanghai, *supra* note 261, at art. 7.

263. *See, e.g.*, Measures for the Administration of Data Intellectual Property Registration of Hunan Province (Trial), *supra* note 262, at art. 11; Interim Measures for the Registration and Deposit of Intellectual Property Rights of Data Products in Shanghai, *supra* note 261, at art. 7.

264. *See* Provisional Administrative Measures for the Registration of Data Intellectual Property Rights (Trial), *supra* note 259, at art. 10.

265. *See, e.g.*, *id.*

266. *See, e.g.*, *id.*; Provisional Measures for the Registration of Data Intellectual Property Rights of Tianjin (Trial), *supra* note 259, at art. 10; Measures for the Administration of Data Intellectual Property Registration of Jiangsu Province (Trial), *supra* note 261, at art 14.

depositing the data itself with the registration platform. [267] The hash operates as a cryptographic fingerprint of the registered information: it fixes the identity and state of the information at the time of registration while leaving the underlying content in the applicant's possession. [268] They then provide a designated window for public objection, after which a certificate of registration is issued to the applicant.[269] The certificate, however, does not create any rights on registered data but merely serve as prima facie evidence of their existence.[270]

Modelled partially on these data registration systems, the proposed AI secrets registration encourages AI developers to affirmatively register the specific components or related information of their applicable AI models that they claim as protected trade secrets. To respond to the cybersecurity concerns raised by requiring developers to transmit sensitive AI-related information to a government-maintained repository, however, the registry would not require the direct submission of the underlying AI secrets at the initial registration stage. Instead, the applicant should submit relevant information about the AI-related information, such as the claimant's identity and contact information, the name of the claimed AI

---

267. See *Guangdong Sheng Shuju Zhishi Chanquan Dengji Shiwu Caozuo Zhiyin (Futu)* (广东省数据知识产权登记实务操作指引（附图）) [Practical Guide to Data Intellectual Property Registration in Guangdong Province (with Illustrations)], Weixin Official Accounts Platform (Mar. 20, 2026), https://mp.weixin.qq.com/s/TTcRmFLpR84FJPtBRzyYTQ [hereinafter Practical Guide to Data Intellectual Property Registration in Guangdong Province (with Illustrations)]; Shuju Zhishi Chanquan 'Tongguan Miji' | Di Jiu Qi (数据知识产权"通关秘笈" | 第九期) [Data Intellectual Property "Customs Clearance Secrets" | Issue 9], Foshan Protection Center (佛山保护中心), Weixin Official Accounts Platform (June 16, 2025), https://mp.weixin.qq.com/s/uNi3-JJb5p3wmJ7gea92RA; *Shenzhen Shi Shuju Zichan Dengji Caozuo Zhiyin* (深圳市数据资产登记操作指引) [Shenzhen Data Asset Registration Operation Guide], SHENZHEN DATA ASSET REGISTRATION SYSTEM, https://sjdj.sist.org.cn/cqdjCms/detail/contentdetail.html?id=dd2c2204-7e92-42f0-befa-c091d7dd3c9b [https://perma.cc/SA3A-SKUP].

268. *See What Is a Hash Value and Hash Function in Cyber Security?*, OBRELA (Mar. 6, 2025), https://www.obrela.com/blog/what-is-a-hash-value-and-hash-function-in-cyber-security [https://perma.cc/9J8M-URAV]; Minshang Yanxi (民商研习), Haxi Zhi (Hash Value) de Gainian Ji Qi Zai Shangye Mimi Cunzhen Zhong de Yingyong (哈希值（Hash Value）的概念及其在商业秘密存证中的应用) [The Concept of Hash Values and Their Application in Trade Secret Evidence Preservation], Weixin Official Accounts Platform (Mar. 8, 2026), https://mp.weixin.qq.com/s/1VAYvWTZozgBGB4I4hpD1A [https://perma.cc/39MP-ENFZ].

269. *See, e.g.*, *Beijing Shi Shuju Zhishi Chanquan Dengji Guanli Banfa (Shixing)* (北京市数据知识产权登记管理办法（试行)) [Provisional Administrative Measures for the Registration of Data Intellectual Property Rights (Trial)], *supra* note 257, arts. 11-13; Provisional Measures for the Registration of Data Intellectual Property Rights of Tianjin (Trial), *supra* note 259, at arts. 10-12; Interim Measures for the Registration and Deposit of Intellectual Property Rights of Data Products in Shanghai, *supra* note 261, at arts. 8-9; Measures for the Administration of Data Intellectual Property Registration of Jiangsu Province (Trial), *supra* note 261, at arts. 14-16.

270. *See* Tang Zhenyou (汤贞友), *Shuju Zhishi Chanquan Dengji de Zhidu Luoji Ji Wanshan* (*数据知识产权登记的制度逻辑及完善*) [*The Institutional Logic and Improvement of Data Intellectual Property Registration*], 2024 [INTELL. PROP.], no. 3 (China).

secrets, a short summary and description of the claimed subject matter, the categories of AI components implicated, the claimed boundaries of the information, and, most importantly, the relevant hash value or hash values generated from the underlying information. The hash-based registration design allows the registry to crystallize the existence, claimed boundary, and temporal state of the information without requiring its direct deposit.

Similarly, the registration system does not legally validate the trade secret status of the recorded AI secrets. In other words, the system does not create or establish any trade secret rights; it merely records the existence of AI secrets as claimed by AI developers. The register's initial role, after receiving the registration request, is also limited to a procedural formality check. Absent any formality issues, the register must register the AI secrets and issue a public notice. Drawing insights from the aforementioned data registration systems as well as the U.S. Copyright Office Public Records System,[271] the public record would contain only brief details, such as the claimant's identity, contact information, and the name of the AI secrets, alongside a brief description of its contents. Following the publication of the record, the register will issue a certification of registration to the applicant. Importantly, this certificate does not vindicate any protectable trade secret rights either; rather, it merely established the factual existence of specific AI components *potentially* protected under trade secret law.

1. Legal Effects of (Non)Registration

To encourage registration, however, developers who fail to register their AI secrets should face negative legal consequences if their AI models subsequently raise transparency concerns. At first glance, designing a registry that incentivizes participation through adverse legal consequences rather than by conferring affirmative benefits may seem counterintuitive. Although registration certainly offers notable benefits to AI developers, which will be detailed below,[272] the design of such a system is not without precedent. The U.S. copyright registration is also voluntary, and the validity of the copyright does not hinge on formal registration. [273] However, registration remains a prerequisite to filing an infringement action for U.S. works in federal court, as well as to

271. For examples on the public records on registered copyrighted works maintained by the U.S. Copyright Office, see *U.S. Copyright Office Public Records System*, U.S. COPYRIGHT OFF., https://publicrecords.copyright.gov [https://perma.cc/T6DX-F7NC] (last visited July 18, 2026).

272. *See infra* Part IV.B.

273. *See* Oliar et al., *supra* note 64, at 2215-16; Robert J. Kasunic, *The Benefits of Registration*, 68 J. COPYRIGHT SOC'Y U.S.A. 83, 85-86 (2020).

recovering statutory damages and attorney fees.[274] Indeed, the ability to bring an infringement action and recover statutory damages and attorney fees has consistently been framed as the "incentives and benefits" established by the U.S. Congress to encourage registration.[275] From a functional perspective, conditioning jurisdictional access and enhanced remedies on registration act as an implicit penalty for non-registration. In practice, the interplay of these structural incentives and corresponding penalties partially drives the popularity of the voluntary copyright registration system among U.S. copyright holders.[276] Accordingly, the incentive-and-penalty framework of the U.S. copyright registration system provides an insightful blueprint for the proposed AI secrets registry regarding non-registration.

To incentivize AI developers to register their AI secrets, there are some special designs of the proposed system. First, non-registration does not preclude the substantive protections afforded to AI developers under trade secret law during trade secret litigation. In the event of alleged misappropriation, developers retain the right to initiate litigation regardless of whether the AI secrets at issue have been registered. Second, when AI developers are subject to transparency mandates under applicable law or regulation, they may only assert trade secret protection as a shield against disclosure if those AI secrets are already registered. In other words, while developers retain the right to sue for the misappropriation of unregistered AI secrets, they are legally precluded from invoking trade secrecy as a defense to bypass transparency or disclosure requirements provided by applicable legislation and regulations. Meanwhile, when AI developers assert registered AI secrets to counter transparency mandates, the official registration record will dictate the boundaries of the claimed AI secrets. Namely, when judicial or administrative bodies consider whether the AI secrets claimed to resist disclosure qualify as genuine trade secrets, the registration record will govern the scope of their analysis. Importantly, however, this registered scope does not dictate the boundaries of the AI secrets in any misappropriation litigation. Accordingly, it is important that the register

274. 17 U.S.C. §§ 411(a), 412.

275. *See* Kasunic, *supra* note 273, at 85-86; Oliar et al., *supra* note 64, at 2215-16.

276. *See* Oliar et al., *supra* note 64, at 2215-16; Robert Brauneis & Dotan Oliar, *An Empirical Study of the Race, Ethnicity, Gender, and Age of Copyright Registrants*, 86 GEO. WASH. L. REV. 46, 51-52 (2018) (analyzing the U.S. Copyright Office catalog, emphasizing the vast scale of the voluntary system by noting that over 14.5 million valid monograph registrations were voluntarily filed between 1978 and 2012 alone); U.S. COPYRIGHT OFFICE, ANNUAL REPORT FISCAL YEAR 2024, 20 (2024), https://www.copyright.gov/reports/annual/2024/ar2024.pdf [https://perma.cc/CGX9-ZKJP] (determining that, by the end of 2024, there have been more than 40 million works registered in the U.S. Copyright Office).

allows AI developers to update their registered AI secrets as their underlying models evolve. Although detailing the specific technical interface that AI developers might use to update their registered secrets falls outside the scope of this Article, the real-time renewal system proposed by Chagai Vinizky for a general trade secret registry serves as an excellent model.[277] Meanwhile, technology such as blockchain may be adopted to maintain the updated recordation, similar to some of China's local data registration systems. [278] Also, because, under the current proposal, developers would mainly need to update the hash values corresponding to their revised AI secrets, the registry could provide a self-service function that allows firms to update those hash values and thereby indicate the newest versions of their registered AI secrets.

1. Disclosure, Public Scrutiny, and Register's Duties

The registry's functions extend beyond mere registration and recordation. To better facilitate AI transparency and reconcile its inherent tension with trade secrecy, this framework proposes allowing public oversight of registered AI secrets. Crucially, this does not imply that the public can freely access or view the registered information, as public disclosure would legally extinguish the trade secret status and irreparably harm the developers' competitive interests. Instead, the public, such as public organizations or concerned individuals, is granted a procedural mechanism, particularly when raising legitimate concerns regarding a deployed AI model, to petition the registry to conduct a thorough, substantive examination of the model's registered secrets. To avoid potential abuses of the petition mechanism, the system may require petitioners to pay a modest petition fee when requesting substantive review. For one thing, petition fees may help defray the administrative and technical costs of the substantive examination. For another, these fees would serve

277. *See* Vinizky, *supra* note 64, at 488-89.

278. *See Changchun Shi Shuju Chanquan Dengji Guanli Banfa* (长春市数据产权登记管理办法) [Changchun Municipal Data Property Rights Registration Management Measures] (promulgated by Changchun Mun. Gov't Servs. & Digitalization Constr. Admin. Bureau, Sept. 10, 2024, effective Sept. 13, 2024), art. 10, https://zscq.tj.gov.cn/zwgk/zcwj/zscqwj/202402/t20240227_6545482.html [https://perma.cc/VDM9-DSHT] (China) [hereinafter Changchun Municipal Data Property Rights Registration Management Measures]; *Shenzhen Shi Shuju Chanquan Dengji Guanli Zanxing Banfa* (深圳市数据产权登记管理暂行办法) [Interim Measures for the Administration of Data Property Rights Registration of Shenzhen Municipality] (promulgated by Shenzhen Mun. Dev. & Reform Comm'n, June 15, 2023, effective July 4, 2023), art. 10, https://www.sz.gov.cn/cn/xxgk/zfxxgj/zcfg/content/post_10692613.html [https://perma.cc/XP5A-TDWZ] (China) [hereinafter Interim Measures for the Administration of Data Property Rights Registration of Shenzhen Municipality].

a gatekeeping function by discouraging frivolous, duplicative, or strategically motivated petitions designed merely to harass AI developers or delay deployment. At the same time, the fee should not be set so high as to chill legitimate public oversight, particularly by civil society organizations, researchers, affected individuals, journalists, or public-interest groups. Accordingly, the registry may adopt a calibrated fee structure: a baseline fee for ordinary petitions, fee waivers or reductions for petitioners who demonstrate public-interest motivations or financial hardship.

Once a substantively reviewable petition is filed, the registry will not simply demand that the developer upload the underlying AI-related information to the public registry. Instead, the registry will partner with trusted, independent third-party organizations possessing the specialized technical and legal expertise required to conduct these substantive reviews. This delegation would prevent the governing administrative body from becoming overburdened while elevating the technical and legal rigor and overall efficiency of the review process. Specifically, the registry will request that the company securely transmit the registered information to the trusted third party through a protected channel and under a strict confidentiality regime. The trusted third party can then compare the received materials against the short descriptions, claimed boundaries, and hash values already recorded in the registry. This verification step ensures that the materials examined in the substantive review correspond to the information previously registered, while still avoiding the cybersecurity costs of routine centralized storage. After verification, this substantive review by the trusted third party focuses on two core issues: first, whether the registered AI components legally qualify as protectable trade secrets; and, second, whether their deployment harms the public, such as by infringing upon personal privacy or other legitimate interests, introducing systematic bias, or breaching existing laws and regulations. If deemed necessary, the third party may request further information and input from the registrant during the examination process.

Upon concluding the substantive review, the registry takes two primary actions. First, if any registered information fails to meet trade secret requirements, the registry will request the registrant to generate new hash values of the remaining AI secrets after unprotected portions have been removed. Once the revised hash values are submitted and verified, the registry will publish an amended record and issue an updated certificate, thereby revising the registered scope and effectively removing the non-qualifying information from the registry. As a result of this removal, AI developers are barred from asserting trade secret protection to shield that specific information from subsequent, potential transparency mandates. Second, regardless of whether the registered information

qualifies as trade secrets, if the review uncovers potential threats to the public interest or regulatory violations, the registry will notify the petitioning party of the identified issues and refer the matter to the appropriate regulatory bodies for subsequent actions.

The proposed AI secrets registry's substantive review mechanism draws robust comparative insights from the emerging E.U. data governance framework, specifically the E.U. Data Act ("DA") and the Digital Service Act ("DSA").[279] For instance, under Article 4 of the DA, if a manufacturer of connected devices refuses a user's data-sharing request citing the need to avoid serious economic damage from trade secret disclosure, the user may challenge this refusal before a national competent authority or a certified Dispute Settlement Body.[280] These independent entities are tasked with examining the data to assess whether the trade secret claim justifies the refusal.[281] Similarly, under Article 40 of the DSA, vetted researchers may request access to the internal data of very large online platforms ("VLOP") or very large online search engines ("VLOSE") to study systemic risks.[282] If a platform claims that such access would compromise its trade secrets, it may request an amendment to the data access request.[283] This claim is then reviewed by a third-party regulator, the Digital Services Coordinator ("DSC"), which evaluates the assertion and determines whether the amendment is permissible. [284] Therefore, the proposed registry in this Article represents an extension of these models—utilizing an independent, third-party review of trade secret claims to ameliorate the tension between AI secrets and public transparency, thereby operationalizing the preliminary suggestions advanced by Keller and Aplin.[285]

Meanwhile, some Chinese local data registration systems offer valuable comparative insights as well. Following a preliminary formality check, several of these regional systems designate independent, third-party service organizations to conduct a substantive examination to

279. *See* Commission Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), 2023 O.J. (L 2854) 44 - 46; Commission Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 82-85; Keller & Aplin, *supra* note 16, at 27-28.

280. *See* Council Regulation 2023/2854, *supra* note 279, at 45.

281. *See id.*; Tanya F. Aplin & Johnathon Liddicoat, *Mandatory Sharing of Trade Secrets: International Flexibilities and EU Models* 13-14 (Oct. 17, 2025), https://ssrn.com/abstract=5912322 [https://perma.cc/E3T5-V4ZD].

282. *See* Council Regulation 2022/2065, *supra* note 279, at 82-85.

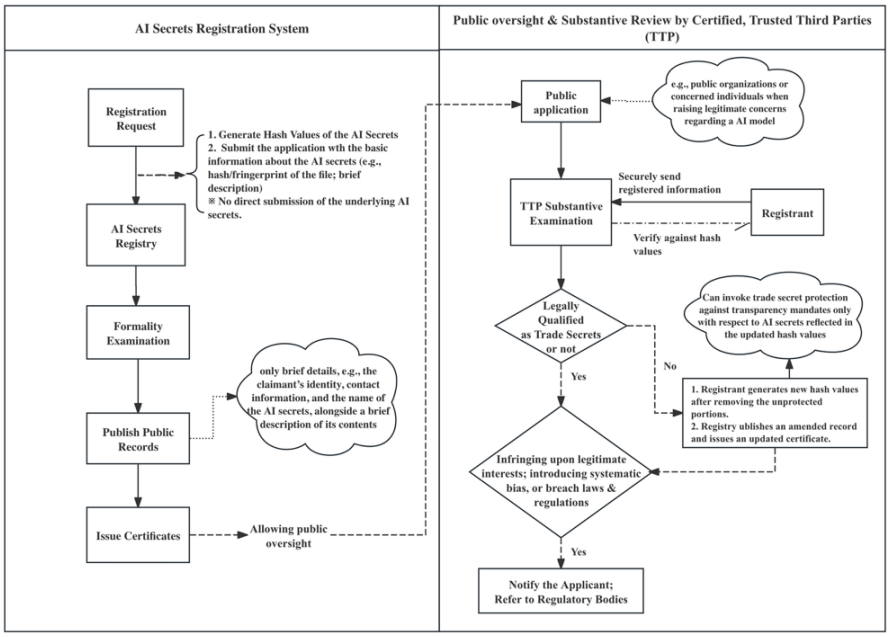
283. *See id.* at 83.

284. *See id*.; Keller & Aplin, *supra* note 16, at 28.

285. *See* Keller & Aplin, *supra* note 16, at 31-32.

ensure that the subject data meets the registration criteria and neither infringes upon individual rights nor contravenes applicable laws.[286]

Flowchart: The Proposed AI Registration Systems with Substantive Review by Certified, Trusted Third Parties.[287]



B. Addressing Structural Failures, Achieving Allied Benefits

The proposed registration system can remedy the inherent limitations of current mandated-disclosure approaches by addressing the structural failures of trade secret law within the AI secrets context. To recap, mandated-disclosure consistently struggles against the rampant overclaiming of trade secrets by AI developers.[288] This overclaiming is

286. *See* Chang-chun Municipal Data Property Rights Registration Management Measures, *supra* note 278, at art. 15; Interim Measures for the Administration of Data Property Rights Registration of Shenzhen Municipality, *supra* note 278, at art. 15; *Xiamen Shi Sjuju Zichan Dengji Guanli Zanxing Banfa* (厦门市数据资产登记管理暂行办法) [Interim Measures for the Administration of Data Asset Registration of Xiamen Municipality] (promulgated by Xiamen Mun. Data Admin. Bureau, July 12, 2024, effective July 12, 2024), art. 19, http://www.fjdjdq.com/content.asp?id=18763 [https://perma.cc/2QU9-M9RZ] (China) [hereinafter Interim Measures for the Administration of Data Asset Registration of Xiamen Municipality] (demonstrating substantive review by the third-party service organization before formality check by the registry).

287. This flowchart is adapted from an original version created by Gangjia Li, a student in my 2025 Chinese and Comparative Trade Secrets Law course, who utilized an initial draft of this Article for her group presentation. I am grateful to Gangjia for her consent to allow me to refine and incorporate this updated chart into the present work.

288. *See supra* notes 189-91 and accompanying text.

directly facilitated by the structural features of trade secret law, most notably, the absence of a pre-identification requirement and an inherently broad boundary and scope of protection, which ultimately frustrate regulatory demands for AI transparency.[289]

Under the proposed registry framework, AI developers' right to assert a trade secret defense against transparency mandates hinges entirely on prior registration.[290] As such, AI developers need to pre-identify the scope of their AI secrets *ex ante*. The developer must define the claimed boundary through generating their hash values for registration. The scope of the registration strictly governs the boundary of the AI secrets that can be shielded from future transparency mandates.[291] As a result, AI developers are bound by their original filings and can no longer strategically redefine their AI secrets *ex post* to avoid regulatory disclosure. Put differently, should any unregistered AI components or related system information fall within the scope of subsequent transparency mandates, developers are legally precluded from invoking trade secrecy to shield them from disclosure. For that information, the aforementioned obstacles to public transparency, caused by trade secret overclaiming under current mandated-disclosure approaches,[292] can be effectively alleviated.

Furthermore, the registry further mitigates the overclaiming issue of AI secrets by establishing mechanisms for public scrutiny and substantive review. Admittedly, developers may still attempt to overstate the scope of their AI secrets during the initial registration process, given that the registry defaults to a preliminary formality check. However, the threat of a substantive review initiated by the public, coupled with its attendant legal consequences, serves as a deterrent against the overclaiming. The reason is that if a review determines that components were overclaimed, the registry removes them from the record, legally precluding developers from using trade secrecy to shield those specific parts or information from future disclosure mandates. Therefore, that AI-related information is freed for further public scrutiny under other relevant regulatory transparency regimes. By shifting to a streamlined, request-driven administrative review, this approach avoids the lengthy and costly court battles traditionally associated with defending trade secrets against disclosure mandates,[293] ensuring that public transparency is achieved in a much more timely manner.

---

289. *See supra* Part III.B.
290. *See supra* Part IV.A.
291. *See supra* Part IV.A.
292. *See supra* notes 189-91 and accompanying text.
293. *See supra* notes 189-91 and accompanying text.

While its primary function is to resolve the structural failures of trade secret law to facilitate mandated AI transparency under the current mandated-disclosure approaches, the proposed registration framework yields several ancillary benefits that further justify its adoption. Foremost among these benefits is the registry's signaling function. Much like registration and recordation systems in other contexts, the official record and issued certification can lower the otherwise high information costs AI developers face during trade secret transactions. Furthermore, they signal the existence of valuable intangible assets, thereby elevating the company's market valuation.[294]

Transacting or licensing trade secrets normally entail high transaction costs, a phenomenon partially explained by "Arrow's Information Paradox."[295] A trade secret holder will naturally refuse to disclose confidential information to negotiate with potential counterparties absent an NDA. Conversely, counterparties may be reluctant to assume broad confidentiality duty without first knowing and valuing the concerned information.[296] For example, prospective licensees may fear that the disclosed information is already publicly available or readily ascertainable, yet signing an NDA may legally preclude them from using it should negotiations fail.[297] This dilemma significantly inflates transaction costs and may even disrupt socially desirable deals.[298]

In addition, unlike patent, which companies routinely use to signal R&D excellence and productivity and boost the outside value estimations,[299] trade secrets inherently lack this signaling function.[300] Because both the content and the very existence of a company's trade secrets are

---

294. *See* Vinizky, *supra* note 64, at 463-70 (examining trade secret transactions' high information costs); Clarisa Long, *Patent Signals*, 69 U. CHI. L. REV. 625, 643-55 (2002) (explaining that patent law reduces the high information costs in transactions); Honghong Shao (邵红红) [Shao Honghong], *Shuju Chanquan Dengji de Gongneng Dingwei, Moshi Xuanze yu Zhidu Wanshan—Yi Xinhao Lilun wei Qierudian* (*数据产权登记的功能定位、模式选择与制度完善——以信号理论为切入点*) [*The Functional Positioning, Model Selection, and System Improvement of Data Property Rights Registration: From the Perspective of Signaling Theory*], 2024 ZHISHI CHANQUAN 54, 54-55 (知识产权) [INTELL. PROP.], (China) (analyzing China's local data registration system via its signaling function).

295. *See* Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention*, *in* THE RATE AND DIRECTION OF INVENTIVE ACTIVITY 614-16 (1962); *see also* Bone, *supra* note 14, at 280; Vinizky, *supra* note 64, at 263. *But cf.* Lemley, *Surprising Virtues*, *supra* note 14, at 336-37 (arguing that trade secret law serves as a partial solution to Arrow's Information Paradox).

296. *See* Bone, *supra* note 14, at 280; Vinizky, *supra* note 64, at 463-64.

297. Currently, still some courts allow independent breach of contract cause of action to proceed even when the concerned information is not confidential at all. *See* Varadarajan, *supra* note 41, at 1566.

298. *See* Bone, *supra* note 14, at 280.

299. *See* Schwartz, *supra* note 199, at 641-42.

300. *See* Levine & Sichelman, *supra* note 204, at 773-74.

typically inaccessible, outsiders cannot factor it into the company's valuation. This lack of visibility prevents trade secrets from acting as market signals, ultimately hindering potential financing opportunities, particularly for start-ups.[301]

By providing a verifiable public record, the proposed registry effectively mitigates these transaction costs and serves as a vital signaling mechanism for AI developers. Upon successful registration, the system issues a formal certificate providing verifiable proof that claimed AI secrets exist, and that the registering entity is their legitimate owner. When an AI developer approaches a potential counterparty for licensing or collaboration, they can present this certification or registration record. At a minimum, the record confirms the existence of the secrets and provides high-level description, enabling the counterparty to make a better-informed decision about proceeding under an NDA. Likewise, the record signals the existence of AI secrets and their basic information to the broader market, serving as rough proxies for the company's technological capabilities and innovative output. Therefore, the registry, to some extent, elevates the firm's external valuation, remedying the inherent limits of traditional, completely opaque trade secret regime.

Moreover, if the registration record reflects that the AI secrets have survived a substantive review following a public request, the registry's signaling power is exponentially amplified. In this scenario, the record acts as an independent assurance that the subject matter constitutes a legitimate, protectable trade secret. This substantially diminishes the counterparty's perceived risk of being unfairly restricted by an NDA over unprotectable information. As such, it directly tackles Arrow's Information Paradox by allowing both parties to enter negotiations with greater trust and certainty, thereby reducing the transaction costs. In a similar vein, a substantiated record amplifies the value-signaling function of the registry to outside investors, ultimately unlocking enhanced financing and investment opportunities. After all, a post-review record provides robust market assurance that the registered AI secrets are highly likely to be genuinely protectable and valuable assets.

Another possible benefit of the proposed registration system lies in its enhanced notice function for employees. Current trade secret law relies heavily on the reasonable secrecy measures adopted by information holders, most notably NDAs, to notify employees who access the information about a proprietary claim.[302] However, without an understanding of the rough boundaries and attributes of protected trade

---

301. *See id*. at 766-67; *see also* Schwartz, *supra* note 199, at 653-54.

302. Varadarajan, *supra* note 57, at 384-85.

secrets, employees become overly cautious about switching jobs or launching startups, thereby chilling knowledge spillover and cumulative innovation. [303] Relying on secrecy measures deemed reasonable under current trade secret law to communicate these boundaries is largely ineffective. [304] The primary flaw lies in, again, the disproportionate weight courts give to overly broad NDAs when assessing reasonable measures.[305] Because sweeping NDAs fail to delineate the contours of claimed trade secrets, they fundamentally fail their notice function.[306]

By incentivizing AI developers to pre-identify the scope and boundaries of their AI secrets through generating hash values for registration purposes, the proposed registry may help employees who access these secrets internally under NDAs better understand and ascertain the potential proprietary claims of their employers. Once AI developers delineate the rough boundaries of their AI secrets, employees interacting with them can rely on the employer's own identification to grasp their defining attributes. Consequently, departing employees can more effectively navigate their future innovative endeavors, knowing how to better innovate around the secrets to avoid infringement. Meanwhile, even if the identified scope for registration does not govern trade secret identification in trade secret misappropriation litigation,[307] sued employees remain in a stronger position than under the traditional framework. By entering a dispute with prior knowledge of the claimed boundaries, employees possess a more solid foundation for framing their defenses, ultimately securing greater bargaining power during settlement negotiations with former employers. Accordingly, by prompting AI developers to pre-identify the boundaries of their AI secrets, the proposed registry preserves the socially beneficial knowledge spillover and cumulative innovation typically driven by employee mobility in the AI context.

C. Limitations and Future Directions

The proposal advanced in this Article has limitations. First, delineating every practical detail of a registration system for AI secrets falls beyond the scope of this work. Implementing such a system within any given jurisdiction requires a host of nuanced, highly specific operational rules. These mechanisms must be carefully tailored to accommodate a particular jurisdiction's unique legal and governmental frameworks,

303. *See id.* at 385-86.
304. *See id.* at 388, 390-92.
305. *See supra* notes 239-40 and accompanying text.
306. *See* Varadarajan, *supra* note 57, at 390-91.
307. *See supra* Part IV.A.3.

making a universal generalization impossible. Instead, the primary objective of this Article is to establish a foundational framework for an AI secrets registry.[308] This approach empowers individual jurisdictions to build upon this foundational model, designing and implementing a system customized to their specific legal and societal needs. Moreover, precisely because some features of this foundational framework draw comparative insights and models from existing registration, recordation, or third-party review systems of representative jurisdictions, jurisdictions may more easily implement the proposed registry by leveraging their prior practical experiences to address this transnational challenge. [309] That being told, future regional studies may continue exploring how the foundational framework proposed in this Article can be appropriately adopted, adapted, and implemented within specific jurisdictions.

Second, although this Article has explored the potential categories of AI secrets that AI developers might assert under current trade secret law, [310] predicting the sheer volume of AI information that would be submitted under the proposed system remains challenging. This raises a potential practical hurdle: the risk of an unmanageable quantity of registrations. For example, because AI model training inherently requires immense amounts of data,[311] the resulting proprietary datasets are massive in scale.[312] This prompts the question of whether registering such large-scale and numerous training datasets is practically feasible. However, given that the proposed system only requires hash-value recordation rather than actual contents registration, the registration of large-scale information is practically feasible. China's local data registration systems once again provide evidence supporting the capability of the registration system.[313] For instance, a company in Beijing successfully obtained registration for smart-city energy datasets comprising 250 million data points.[314] Moreover, the very existence of registry, particularly one incorporating a mechanism for substantive review, would naturally incentivize AI developers to prioritize and curate their submissions.

---

308. *See supra* Part IV.

309. *See supra* Part IV.A.

310. *See supra* Part I.B.

311. *See supra* note 79 and accompanying text.

312. Torrance & Tomlinson, *supra* note 79, at 242.

313. For examples of large-scale data registrations, see Zhongguo Zhishi Chanquan Bao (中国知识产权报) [China Intellectual Property News], *Shuju Zhishi Chanquan Dengji Shida Dianxing Anli Laile* (数据知识产权登记十大典型案例来了) [*Top Ten Typical Cases of Data Intellectual Property Registration Are Here*], SHOUDU ZHISHI CHANQUAN FUWUYE XIEHUI (首都知识产权服务业协会) [CAPITAL INTELL. PROP. SERVS. ASS'N] (May 28, 2024), https://capitalip.org/news/shownews.php?id=11995 [https://perma.cc/N7MN-3CEA].

314. *Id.*

Rather than registering vast amounts of raw information regarding their AI models, developers would be incentivized to selectively register only those AI secrets they genuinely deem valuable, thereby significantly alleviating potential administrative and practical burdens, if any.

Third, establishing and maintaining a formal registry is undeniably resource-intensive, requiring substantial societal and economic benefits to justify its implementation.[315] Though this Article outlines the prospective advantages of the proposed system, most notably its supplementary role in enhancing AI transparency alongside other ancillary benefits,[316] conducting a comprehensive cost-benefit analysis exceeds the scope of this Article. Ultimately, it falls to individual jurisdictions and their respective policymakers, who possess the localized information and institutional knowledge necessary, to perform the rigorous cost-benefit calculus required. These bodies are best positioned to determine whether implementing a customized registry, built upon this Article's foundational framework, represents an efficient policy choice. Furthermore, future studies dedicated to this framework could provide the extensive space required to conduct a more holistic and detailed cost-benefit analysis.

CONCLUSION

In an era where artificial intelligence systems are seamlessly integrated into daily life, AI transparency has emerged as a primary regulatory focus, presenting a transnational challenge shared across multiple jurisdictions. A major obstacle to achieving this transparency lies in the assertion of "AI secrets" by developers. By engaging with the most recent cases, regulations, and statutes, this Article maps how current trade secret law protects AI components and related information, illuminating the inherent conflict between these proprietary claims and public transparency demands.[317] Also, it highlights the limitations of the mandated-disclosure approaches currently favored by scholars and policymakers. This Article argues that these limitations stem from structural failures within trade secret law when applied to the AI context, necessitating a more robust, structural solution to supplement existing disclosure mandates.[318] Accordingly, this Article proposes a novel AI secrets registration system designed to rectify these structural failures while yielding

315. Varadarajan, *supra* note 57, at 387-88.
316. *See supra* Part III.
317. *See supra* Parts I–II.
318. *See supra* Part III.

ancillary benefits.[319] Although this proposal inherently possesses limitations,[320] establishing this foundational framework for a third-party registration and review system will ideally catalyze further scholarly inquiry and capture the attention of policymakers worldwide.

319. *See supra* Part IV.
320. *See supra* Part IV(C).