The Promise and Perils of Enterprise Data as Trade Secrets

Yang Chen*

29 STAN. TECH. L. REV. 1 (2026)

ABSTRACT

Various types of information exist as data, ready for collection and use by relevant actors. A broad distinction, however, may be drawn between personal data, derived from individuals, and enterprise data, which typically comprises large-scale collections generated or acquired by firms during business operations. Enterprise data may include proprietary business information as well as data collected from customers or the public. A growing body of literature explores legal frameworks for protecting enterprise data, though approaches vary. Jurisdictions worldwide have not reached a consensus on whether or how enterprise data may receive legal protection, despite vigorous debates. An emerging viewpoint across jurisdictions is to protect enterprise data as trade secrets, but this approach has not yet gained wide acceptance.

This Article engages with that debate and contributes to the current literature on enterprise data as trade secrets from three perspectives. First, it reiterates the potential promise of trade secret law by offering a doctrinal analysis showing how trade secret law can protect diverse forms of enterprise data in the data economy. These comprise three key categories: confidential enterprise data, private data compilations, and "semi-public" enterprise data compilations, where front-end data points are publicly accessible but back-end compilations are kept private. Second, the Article explores current cases, laws, and regulations in representative jurisdictions, the United States, China, and the EU, documenting the extent to which the concept of enterprise data as trade secrets has been recognized. This positive analysis highlights the status quo: the role of trade secret law in protecting the first two categories of enterprise data

---

* Ian Yang Chen, Assistant Professor, School of Law, City University of Hong Kong; S.J.D., LL.M., University of Pennsylvania Carey Law School. Thank you for the comments and suggestions from Gideon Parchomovsky, Hui Jing, Tan Cheng Han, Klaus Heine, Tan Zhong Xing, Jyh-An Lee, Guobin Cui, David Tan, Albert Wai-Kit Chan, Josje de Vogel, Yan Wang, Alexander Loke, Xingguang Zou, Linjun Gao, and other participants in the 2025 Meeting of the Private Law Consortium at Erasmus School of Law, Erasmus University Rotterdam; the 2025 IP Conference at the Chinese University of Hong Kong; and the 2025 Intellectual Property and Technology in the 21st Century: Challenges in the Next Decade conference at the National University of Singapore. Thanks for Yixuan Bai's excellent research assistance throughout. All errors are my own.

has gained growing and continuous recognition, but its application to "semi-public" enterprise data compilations remains limited. Third, based on the positive exploration, the Article unpacks the challenges and risks associated with applying trade secret law to "semi-public" enterprise data compilations, offering explanations for its limited acceptance compared to the other two types. It argues that protecting most "semi-public" data compilations as trade secrets does not serve the core theoretical aims of trade secret law. This is because extending protection to these compilations fails to yield the business efficiency necessary to justify the associated costs. Thus, normatively, the Article argues that trade secret law should only protect the type of "semi-public" data compilation whose front-end access is meaningfully restricted to a limited number of users. At the same time, trade secret law cannot be used to sanction data scraping activities that do not involve intrusion into a data holder's system or direct circumvention of genuine access restrictions.

TABLE OF CONTENTS

I. INTRODUCTION 4
II. THE PROMISE: AN EMERGING RECOGNITION OF ENTERPRISE DATA AS TRADE SECRETS 10
A. Modern Trade Secret Law in a Nutshell 10
B. The Resilience of Trade Secret Law in the Data Economy 13
III. ENTERPRISE DATA SECRETS: GROWING RECOGNITION WITHOUT WIDER APPLICATION 20
A. Private Data and Data Compilations: Consistent and Growing Recognition 21
B. "Semi-Public" Data Compilations: Limited Recognition Without Wider Application 26
IV. REASONS AND PERILS: THE LIMITS OF TRADE SECRET LAW 34
A. Revisiting the Secrecy of "Semi-Public" Data Compilations 35
B. Data Scraping, Improper Means to Acquire, and Reverse Engineering 48
C. No Trade Secrets Protection—Then What? 54
V. CONCLUSION 55

I. INTRODUCTION

In the era of digitalization, data seems to be omnipresent. Various types of information, whether possessing a physical presence or existing solely in the digital realm, can subsist in the form of data, ready to be collected and utilized by relevant parties.[1] There is no single definition of data, which is sometimes even used interchangeably with information.[2] However, a rough distinction may be made between personal data and enterprise data. The former refers to data consisting exclusively of personal information about identifiable individuals, while the latter typically concerns much larger-scale aggregations or collections of data that an enterprise generates or collects in the course of its business operations.[3] There are various types of enterprise data, including a firm's own business data as well as personal and non-personal information collected from external sources (e.g., customers or the public).[4]

There is immense value to be extracted from data, so much so that it is claimed to be the new oil of today's digital economy.[5] Ever since the transition to the so-called data economy, legal discussions related to data have abounded. Much scholarship has analyzed laws and regulations governing data scraping and relevant causes of action.[6] Many scholars are investigating data

---

[1] *See, e.g.*, Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE. L.J. 1460, 1462–63 (2020); Tanya Aplin et al., *The Role of EU Trade Secret Law in the Data Economy: An Empirical Analysis*, 54 INT'L REV. INTELL. PROP. COMPETITION L. 826, 827 (2023).

[2] *See* Herbert Zech, *A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data*, 11 J. INTELL. PROP. L. & PRAC. 460, 462–63 (2016); Josef Drexl, *Designing Competitive Markets for Industrial Data: Between Propertisation and Access*, 8 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 257, 263–65 (2017).

[3] Cui Guobin (崔国斌), *Xinjiu Ru Jiuping: Qiye Shuju Baohu de Shangye Mimi Lujing* (新酒入旧瓶：企业数据保护的商业秘密路径) [*New Wine in Old Bottles: The Trade Secret Path for Enterprise Data Protection*], ZHENGZHI YU FALÜ (政治与法律 [POL. SCI. & L.] no. 11, 2023, at 3; *see also* Drexl, *supra* note 2, at 264 ("industrial data"). Enterprise data is synonymous with platform data or data owned by data producers. See Niva Elkin-Koren, Maayan Perel & Ohad Somech, *Unlocking Platform Data for Research*, 100 IND. L.J. 1479, 1487–89 (2025) ("platform data"); Peter K. Yu, *Data Producer's Right and the Protection of Machine-Generated Data*, 93 TUL. L. REV. 859, 863–64 (2019) (discussing data producers' rights in data they generate and collect).

[4] *See* Elkin-Koren, Perel & Somech, *supra* note 3, at 1486–89.

[5] *See* Yu, *supra* note 3, at 860; *see generally* Jathan Sadowski, *When Data Is Capital: Datafication, Accumulation, and Extraction*, BIG DATA & SOC'Y, Jan.–June 2019, at 1, 1–2 (exploring the notion of data as capital).

[6] See, e.g., Han-Wei Liu, *Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and Its Open Banking Watershed Moment*, 30 WASH. INT'L L.J. 28, 32–53 (2020); Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 372–81 (2018); Ugo Pagallo & Jacopo Ciani Sciolla, *Anatomy of Web Data Scraping: Ethics, Standards, and the Troubles of the Law*, EUR. J. PRIV. L. & TECHS., no. 2, 2023, at 1, 5–13.

transparency issues, highlighting the growing tension between corporate control over data and the public's need for transparency.[7] The importance of data has become even more pronounced with the advent of generative artificial intelligence (AI) and has sparked discussions on a range of new legal issues.[8] For example, there has been increasing attention on potential infringement arising from using others' copyrighted materials as AI training data.[9] The legal dispute between The New York Times and OpenAI is one such example.[10]

In contrast, another line of scholarship focuses on the legal protections that may be afforded to data. Early papers have explored whether individuals have any property-like rights concerning their personal data, beyond traditional rights to privacy or personal information.[11] Many studies, particularly those concerning the European Union's General Data Protection Regulation (GDPR), have analyzed how data collection, processing, and transfer may be more

---

[7] *See, e.g.*, Amy Kapczynski, *The Public History of Trade Secrets*, 55 U.C. DAVIS L. REV. 1367, 1369–77 (2022); Sonia Katyal & Charles Graves, *From Trade Secrecy to Seclusion*, 109 GEO. L.J. 1337, 1351–97 (2021) (describing different types of data claimed as trade secrets).

[8] *See, e.g.*, John G. Sprankling, *Trade Secrets in the Artificial Intelligence Era*, 76 S.C.L. REV. 181, 209–10 (2024); Hannah Bloch-Wehba*, Access to Algorithms,* 88 FORDHAM L. REV. 1265, 1266–73 (2020) (explaining data transparency issues in automated decision-making); Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 56–62 (2019) (similar discussion of data transparency in the AI era). For other prominent AI-related legal issues, *see, e.g.*, Edward Lee & Andrew Moshirnia, *The AI Penalty: Is There a Bias Against AI-Generated Works?*, MICH. ST. L. REV. (forthcoming 2024) (manuscript at 3–5) (an empirical study on AI-generated work); Matthew Sag & Peter K. Yu, *The Globalization of Copyright Exceptions for AI Training*, 74 EMORY L.J. 1163, 1166–68 (2025) (copyright issues related to AI training); 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, 262–65 (2024) (AI and personality rights); Amanda Levendowski, *How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem*, 93 WASH. L. REV. 579, 580–90 (2018); Yang Chen, *Two Roads Diverge and Converge in the AI Era: Computer-Generated Works as an Exception for Human Authorship?*, 36 COLUM. J. ASIAN L. (forthcoming) (manuscript at 3–5) (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, 584–85 (2025) (AI copyrightability issues in Hong Kong).

[9] *See, e.g.*, Sag & Yu, *supra* note 8, at 1167-68; Robert Brauneis, *Copyright and the Training of Human Authors and Generative Machines*, 48 COLUM. J.L. & ARTS 1, 3–4 (2025); 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 101, 191–97 (2025).

[10] *See* Audrey Pope, *NYT v. OpenAI: The Times's About-Face*, HARV. L. REV. BLOG (Apr. 10, 2024), https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-timess-about-face/ [https://perma.cc/Q7B3-LB5C].

[11] *See, e.g.*, Pamela Samuelson, *Privacy as Intellectual Property?,* 52 STAN. L. REV. 1125, 1130–51 (2000); Mark A. Lemley, *Private Property*, 52 STAN. L. REV. 1545, 1545–57 (2000).

efficiently and effectively regulated.[12] An equally heated debate is whether enterprise data is entitled to legal protection,[13] and this Article joins that discussion.

There is abundant scholarship on the protection of enterprise data, but the approaches explored and proposed differ. For instance, we might ask whether copyright law can protect some enterprise data as compilation works.[14] However, compilation works are protectable only when the selection and arrangement of data is somehow creative, and protection only extends to the selection and arrangement itself, not to the underlying data.[15] The "incompetence" of copyright law to offer "adequate" enterprise data protection prompted the EU to take the lead in granting a sui generis database right to enterprise data to preserve the effort and investment of companies in producing and aggregating data.[16] Extensive scholarship has examined the justifications and challenges concerning the EU's sui generis protection regime, as well as whether alternative models may be more appropriate.[17] For example, there was intensive EU debate over the merits of a novel data producer right for enterprise data protection.[18]

---

[12] *See, e.g.*, W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASH. INT'L L.J. 485, 485–87 (2020); Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 94–97 (2021); Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means,* 28 INFO. & COMM. TECH. L. 65, 65–67 (2019).

[13] *See*, e.g., Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 3–5 (2019); Jie (Jeanne) Huang, *The Rise of Data Property Rights in China: How Does It Compare with the EU Data Act and What Does It Mean for Digital Trade with China?*, 27 J. INT'L ECON. L. 462, 462–64 (2024); Cui, *supra* note 3, at 15.

[14] *See* Determann, *supra* note 13, at 18–20.

[15] *See id.*

[16] *See* Yu, *supra* note 3, at 867–68; Matthias Leistner, *The Existing European IP Rights System and the Data Economy – An Overview with Particular Focus on Data Access and Portability*, *in* DATA ACCESS, CONSUMER INTERESTS AND PUBLIC WELFARE 209, 223–232 (Sebastian Lohsse, Reiner Schulze & Dirk Staudenmayer eds., 2020).

[17] *See, e.g.*, Yu, *supra* note 3, at 873–79 (discussing problems with the EU database right that pushed the United States not to follow suit); Leistner, *supra* note 16, at 227–31 (discussing problems with the EU database right).

[18] *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building a European Data Economy*, at 13, COM (2017) 9 final (Oct. 1, 2017), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0009 [https://perma.cc/5GCU-BZQP] (proposing a new data producer right to protect enterprise data in the EU). For scholar discussions, *see*, *e.g.*, Yu, *supra* note 3, at 884–96 (arguing against such a new data producer right); Ivan Stepanov, *Introducing a Property Right over Data in the EU: The Data Producer's Right—An Evaluation*, 33 INT'L REV. L. COMPUT. & TECH. 65, 74–75 (2019) (evaluating the proposed EU data producer right).

Most scholarship on U.S. law adopts a more "conservative" stance toward enterprise data protection, primarily focusing on sanctions for data misappropriation, because U.S. law does not directly protect data aggregations.[19] Only a few scholars have examined the possibility of direct legal protection for data, but they nonetheless argue—and ultimately conclude—that no new property right should be created.[20]

Most discussions of Chinese law take a different approach. Assuming that a property-like right to enterprise data is normatively justified, Chinese scholarship focuses instead on how such a right should be designed.[21] Correspondingly—or perhaps as a direct result—in 2022, the Chinese central government issued a national policy document that explicitly adopted the term "data property rights system," sending a strong signal that enterprise data may be granted legal protection.[22] However, the document did not clarify whether it establishes a new property right, and if so, what that right would entail.[23]

Despite vigorous debates, jurisdictions worldwide have not reached consensus on whether or how enterprise data may receive legal protection. Amid the fragmented exploration of enterprise data protection, an emerging viewpoint across jurisdictions is the protection of enterprise data as trade

---

[19] *See, e.g.*, Liu, *supra* note 6, at 32–44 (discussing causes of action for misappropriating other enterprises' data in the United States); Geoffrey Xiao, *Data Misappropriation: A Trade Secret Cause of Action for Data Scraping and a New Paradigm for Database Protection*, 24 COLUM. SCI. & TECH. L. REV. 125, 129–41 (2022) (same).

[20] *See generally* Determann, *supra* note 13 (discussing potential legal protections offered to data in the United States and concluding that no new property rights should be created for data).

[21] *See, e.g.*, Bingwan Xiong, Jiangqiu Ge & Li Chen, *Unpacking Data: China's 'Bundle of Rights' Approach to the Commercialization of Data*, 13 INT'L DATA PRIV. L. 93, 96–99 (2023) (discussing the different bundle of rights attaching to data under the current Chinese legal framework); Cui Guobin (崔国斌), *Gongkai Shuju Jihe Falü Baohu de Ketai Yaojian* (公开数据集合法律保护的客体要件) [*Legal Protection of Public Data Sets: Object Requirements*], ZHISHI CHANQUAN (知识产权) [INTELL. PROP.], no. 4, 2022, at 18, http://zyzk.jcrb.com/flqk/content.html?gid=F786366&libid=all [https://perma.cc/B99W-J39Z] (proposing a new property right for enterprise data when it cannot receive protection from other laws such as copyright and trade secrets).

[22] *See* ZHONGGONG ZHONGYANG GUOWUYUAN (中共中央国务院) [CENTRAL COMMITTEE OF THE COMMUNIST PARTY OF CHINA AND THE STATE COUNCIL], *Guanyu Goujian Shuju Jichu Zhidu Genghao Fahui Shuju Yaosu Zuoyong de Yijian* (关于构建数据基础制度更好发挥数据要素作用的意见) [*Opinions on Building a Basic Data System to Better Leverage the Role of Data Elements*] (Dec. 2, 2022), http://www.gov.cn/zhengce/2022-12/19/content_5732695.htm [https://perma.cc/D7HT-FNXZ].

[23] This is why some scholars still consider the new property right system to actually be a new intellectual property right system. *See* Huang, *supra* note 13, at 473.

secrets.[24] In the U.S. case *Compulife Software, Inc. v. Newman*, the Eleventh Circuit did not question the notion that trade secret law could protect the plaintiff's secret data compilations, even though each data point within could be obtained by the public through legitimate means.[25] The case highlights the possibility of protecting enterprise data as trade secrets in the United States rather than relying on other causes of action, such as breach of contract and violations of the Computer Fraud and Abuse Act (CFAA), that target data scraping behaviors rather than offering direct protection to data itself.[26] Similarly, while the Chinese central government has not classified the new data property rights, many local governments are adopting a trade secret-like protection model for enterprise data: many data registration systems developed by local governments require data to be secret for it to be registrable.[27] Along the same lines, the new EU Data Act, by regulating the intricate relationship between data sharing and trade secrets protection, appears to introduce a new sub-category of trade secrets—data secrets—which echoes the emerging concept of enterprise data as trade secrets.[28] Thus, protecting enterprise data as trade secrets has attracted attention not only in academic work but also in practice across jurisdictions.

However, this growing recognition has yet to produce a transnational consensus, and the extent to which trade secret law can protect enterprise data remains uncertain. This raises four interrelated and critical questions: (1) how resilient trade secret law is within the context of the data economy, (2) what the status quo is regarding the protection of enterprise data as trade secrets, (3) why broader acceptance of its role has not yet emerged, and (4) whether such broader acceptance is desirable. This Article addresses these questions and contributes to the current literature on enterprise data as trade secrets from three perspectives.

---

[24] *See, e.g.*, Xiao, *supra* note 19, at 141–67 (advocating for treating enterprise data as trade secrets in the United States); Cui, *supra* note 3, (arguing that trade secret law can protect most enterprise data in China); Aplin et al., *supra* note 1, at 828 (discussing how the EU Trade Secrets Directive can protect enterprise data).

[25] Compulife Software, Inc. v. Newman, 959 F.3d 1288, 1310–14 (11th Cir. 2020); Compulife Software, Inc. v. Newman, 111 F.4th 1147, 1160–63 (11th Cir. 2024).

[26] *See* Xiao, *supra* note 19, at 141; Elkin-Koren, Perel & Somech, *supra* note 3, at 1512–14.

[27] *See* Lü Bingbin (吕炳斌), *Shuju Zhishi Chanquan Dengji: Shangye Mimi Moshi Yihuo Shujuku Moshi* (数据知识产权登记：商业秘密模式抑或数据库模式) [*Registration of Data Intellectual Property: Trade Secret Model or Database Model*], ZHISHI CHANQUAN (知识产权) [INTELL. PROP.], no. 6, 2024, at 63.

[28] *See* Aplin et al., *supra* note 1, at 835 (describing the application of trade secret law in the digital economy as an emerging area of scholarship).

First, it reiterates the promise of trade secret law in protecting enterprise data. Drawing from the current literature, the Article offers a doctrinal analysis showing that trade secret law can be adapted to protect diverse forms of enterprise data in the data economy, including purely confidential enterprise data, private data compilations, and "semi-public" enterprise data compilations.[29]

Second, the Article explores caselaw, statutes, and regulations in representative jurisdictions, including the United States, China, and EU, documenting the extent to which the concept of enterprise data as trade secrets has been recognized. This Article focuses on these three jurisdictions because they are potential regulatory leaders of the digital economy worldwide.[30] The three jurisdictions, despite their different legal systems, can serve as representative examples for examining the role of trade secrets in the data economy. This analysis fills a gap in the current literature, as no prior study has systematically explored the application of the concept of enterprise data as trade secrets across these jurisdictions. Through the analysis, this Article highlights the status quo: while trade secret law's role in protecting the first two categories of enterprise data has gained growing and continuous recognition, its application to "semi-public" enterprise data compilations remains limited.

Third, based on the positive accounts, the Article then unpacks the challenges and risks associated with applying trade secret law to "semi-public" enterprise data compilations, offering explanations for its limited acceptance. It argues that protecting most "semi-public" data compilations as trade secrets does not serve the core theoretical aims of trade secret law. This is because extending protection to these compilations fails to yield the business efficiency necessary to justify the associated costs. Thus, normatively, the Article argues that trade secret law should only protect the type of "semi-public" data compilation whose front-end access is meaningfully restricted to a limited number of users. At the same time, trade secret law cannot be used to sanction data scraping activities that do not involve intrusion into a data holder's system or direct circumvention of genuine access restrictions.

---

[29] For definitions of the three types of enterprise data, *see infra* Part II.

[30] *See generally* ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY (Oxford Univ. Press 2023) (construing China, the United States, and the EU as three "digital empires" competing to promulgate regulatory frameworks that shape other jurisdictions).

II. THE PROMISE: AN EMERGING RECOGNITION OF ENTERPRISE DATA AS TRADE SECRETS

A. Modern Trade Secret Law in a Nutshell

Trade secret law has a long history.[31] In the United States, it originated in common law contractual protections during the nineteenth century that gradually developed into torts under state common law. It then evolved into its modern protection model through various state law harmonization efforts, leading to the promulgation and widespread adoption of the Uniform Trade Secrets Act (UTSA) by most states in the twentieth century.[32] Despite this long history, federal trade secret protection only began receiving attention from policymakers and stakeholders in the twenty-first century.[33] This interest culminated in the enactment of the Defend Trade Secrets Act (DTSA) in 2016.[34] In the same year, the EU promulgated the Trade Secrets Directive (TSD), aiming to harmonize the trade secrets protections across its member states.[35] Major developments in Chinese trade secret law occurred during the same period.[36]

---

[31] *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, 498–502 (2010) (summarizing the common-law history of trade secrets in the United States); Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317, 322–38 (2015) (recounting the history of U.S. trade secret law before the federal Defend Trade Secrets Act).

[32] *See* Seaman, *supra* note 31, at 322–30.

[33] Federal attention to trade secret protection spiked in 2013. *See* EXEC. OFF. OF THE PRESIDENT OF THE U.S., ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS (Feb. 2013), https://www.justice.gov/criminal-ccips/file/938321/download [https://perma.cc/VUQ2-P5HH]. The history of Chinese trade secret law began much more recently, starting roughly from 1993. *See* Yang Chen, *Development of China's Trade Secret Law in the US' Shadow: Negative Consequences for China and Suggestions*, 17 U. PA. ASIAN L. REV. 138, 148–68 (2022).

[34] *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, 113–120 (2018).

[35] Directive 2016/943, of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, 2016 O.J. (L 157) 1 [hereinafter EU TSD]; Aplin et al., *supra* note 1, at 828.

[36] Primarily from 2017 to 2020. *See* Chen, *supra* note 33, at 156–68; 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, 830 (2023) (explaining that burden-shifting clauses were added to China's trade secret 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, 70 (2025) (noting that preliminary injunctions became available in trade secrets cases in 2018).

This helps explain why our understanding of trade secret law's role in the data economy emerged much later—and why it remains relatively new.[37]

Yet the importance of trade secret law is being increasingly recognized across the globe. Enterprises are actively utilizing trade secret law to protect business information as well as a wide range of technical information, regardless of patentability.[38]A common business strategy is to combine trade secret law and patent law protection by patenting the components of an invention that satisfy the enabling disclosure requirement, while preserving other critical aspects or the improvements to the invention as secrets.[39] The rising popularity of trade secret law among enterprises is reflected to an extent in litigation statistics across different jurisdictions.[40]

There were some historical requirements pertaining to trade secrets protection,[41] but modern trade secret law stipulates only three requirements, which are shared across jurisdictions and the international protection

---

[37] As compared to copyright law and related rights systems, such as the EU's sui generis database right. *See* Yu, *supra* note 3 (mainly discussing the database right and the then-newly proposed data producer rights); *cf.* Peter K. Yu, *Fitting Machine-Generated Data into Trade Regulatory Holes*, *in* TRADE IN KNOWLEDGE: INTELLECTUAL PROPERTY, TRADE AND DEVELOPMENT IN A TRANSFORMED GLOBAL ECONOMY 738, 741–43 (Antony Taubman & Jayashree Watal eds., 2022) (exploring the trade secrets model for enterprise data protection).

[38] *See* Chen, *supra* note 33, at 140–41; Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 338–41 (2008); *see generally* Andrew Beckerman-Rodau, *The Choice Between Patent Protection and Trade Secret Protection: A Legal and Business Decision*, 84 J. PAT. & TRADEMARK OFF. SOC'Y 371 (2002) (discussing the business considerations involved in choosing between patent and trade secret protections).

[39] *See* W. Nicholson Price II, *Expired Patents, Trade Secrets, and Stymied Competition*, 92 NOTRE DAME L. REV. 1611, 1617–18 (2017).

[40] For U.S. statistics, *see Lex Machina Releases 2024 Trade Secret Litigation Report*, LEXISNEXIS (Sep. 12, 2024), https://www.lexisnexis.com/community/pressroom/b/news/posts/lex-machina-releases-2024-trade-secret-litigation-report [https://perma.cc/FS8P-TQZ4]; David S. Almeling, Darin W. Snyder & Michael Sapoznikow*, A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 301–02 (2009) [hereinafter Almeling (Federal)]; David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 66–68 (2010) [hereinafter Almeling (State)]. For China statistics, *see* Yang Chen, *Demystifying China's Trade Secret Law in Action: A Statistical Analysis*, 13 QUEEN MARY J. INTELL. PROP. 198, 206–08 (2023); Jyh-An Lee, Jingwen Liu & Haifeng Huang, *Uncovering Trade Secrets in China: An Empirical Study of Civil Litigation from 2010 to 2020*, 17 J. INTELL. PROP. L. & PRAC. 761, 763–74 (2022). For EU statistics, *see* EUR. UNION INTELL. PROP. OFF., TRADE SECRETS LITIGATION TRENDS IN THE EU 19–22 (2023), https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2023_Trade_Secrets_Litigation_Trends_in_the_EU/2023_Trade_Secrets_Litigation_Trends_Study_FullR_en.pdf [https://perma.cc/4G9U-MNAS].

[41] *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); Joseph Fishman & Deepa Varadarajan, *Earning Trade Secrets*, 109 CORNELL L. REV. 1381, 1385 (2024) (explaining the common-law original acquisition or investment requirement).

framework.[42] First, the information should be kept secret, meaning that it cannot be publicly known or readily ascertainable.[43] The law, however, does not demand absolute secrecy—maintaining secrecy in the relevant industry or business suffices.[44] In fact, one of the theoretical justifications for trade secret law is to promote disclosure to internal and certain external parties that would allow more efficient use of the information.[45] Second, the information's value should derive, at least partly, from its secrecy.[46] Finally, there should be reasonable efforts—such as physical, technical, or contractual measures—to maintain the secrecy of information claimed as trade secrets.[47] The theoretical rationale for reasonable secrecy measures centers on notice to recipients of the information's secret nature, thereby enabling them to more appropriately structure their conduct.[48]

Information satisfying the three requirements can receive trade secrets protection without registration, which is required for patent and trademark protections.[49] However, trade secrets liability only attaches when there is misappropriation. Misappropriation conduct includes the acquisition of trade secrets through improper means—such as theft, cyber espionage, bribery, or

---

[42] *See* Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 316–17 [hereinafter TRIPS Agreement]; Sharon K. Sandeen & Tanya Aplin, *Trade Secrecy, Factual Secrecy and the Hype Surrounding AI*, *in* RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND ARTIFICIAL INTELLIGENCE 443, 452 (Ryan Abbott ed., 2022); Chen, *supra* note 33, at 144.

[43] *See* UNIF. TRADE SECRETS ACT § 1(4)(I) (UNIF. LAW COMM'N 1979) (amended 1985) [hereinafter UTSA]; EU TSD, *supra* note 35, at art. 2(1)(b); Fan Buzhengdang Jingzheng Fa (反不正当竞争法) [Anti-Unfair Competition Law] (promulgated by the Standing Comm. Nat'l People's Cong., Sep. 2, 1993, effective Dec. 1, 1993; rev'd by the Standing Comm. Nat'l People's Cong., June 27, 2025), art. 10, CLI.1.5299169(EN) (Lawinfochina) [hereinafter 2025 AUCL].

[44] *See* Sandeen & Aplin, *supra* note 42, at 452.

[45] *See* Lemley, *supra* note 38, at 332–37.

[46] UTSA, *supra* note 43, at § 1(4)(I) ; EU TSD, *supra* note 35, at art. 2(1)(a); 2025 AUCL, *supra* note 43, at art. 10.

[47] *See* UTSA, *supra* note 43, at § 1(4)(II); EU TSD, *supra* note 35, at art. 2(1)(c); 2025 AUCL, *supra* note 43, at art. 10. China's judicial interpretation on trade secret law provides some examples. *See* Zuigao Renmin Fayuan Guanyu Shenli Qinfan Shangye Mimi Minshi Anjian Shiyong Falü Ruogan Wenti de Guiding, Fashi [2020] 7 Hao (最高人民法院关于审理侵 犯商业秘密民事案件适用法律若干问题的规定, 法释 [2020] 7 号) [Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Cases Involving Infringements upon Trade Secrets No. 7 [2020]] (promulgated by Sup. People's Ct., Sep. 10, 2020, effective Sep. 12, 2020), CLI.3.345991(EN) (Lawinfochina), at art. 6 [hereinafter 2020 Judicial Interpretation].

[48] *See* Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357, 361–62 (2017).

[49] *See* Deepa Varadarajan, *The Trade Secret-Contract Interface*, 103 IOWA L. REV. 1543, 1552 (2018).

other behaviors deemed contrary to business ethics—as well as the disclosure and use of trade secrets in breach of a duty of confidence.[50] Reverse engineering and independent development are legitimate means to acquire trade secrets.[51] A key feature that distinguishes trade secret law from contract law is that its enables plaintiffs to impose liability on third-parties who disclose or use trade secrets with the requisite knowledge of their improper acquisition or disclosure.[52] A successful trade secret claim can provide plaintiffs with various remedies—including compensatory damage awards, disgorgement, punitive damage awards, and injunctions—which go beyond typical contract law remedies.[53] Although the debate on the theoretical foundations of trade secret law persists, the emerging approach is to treat trade secrets as a type of intellectual property (IP) right.[54] But that issue is not the focus of this Article and does not influence its analysis.

B. The Resilience of Trade Secret Law in the Data Economy

Trade secret law, similar to other areas of IP doctrine, is a product of the traditional economy. However, it has demonstrated surprising resilience in

---

[50] *See* UTSA, *supra* note 43, § 1 cmt. 1; EU TSD, *supra* note 35, art. 4; 2025 AUCL, *supra* note 43, art. 10.

[51] *See* UTSA, *supra* note 43, § 1 cmt. 1; EU TSD, *supra* note 35, art. 3; 2020 Judicial Interpretation, *supra* note 47, at art. 14. It remains unclear, however, whether anti-reverse engineering clauses would turn otherwise legitimate reverse engineering conduct into improper means of acquisition. *See generally* Camilla Alexandra Hrdy, *Keeping ChatGPT a Trade Secret While Selling It Too*, 40 BERKELEY TECH. L.J. 75 (2025) (discussing the enforceability of anti-reverse engineering clauses in the United States); Yang Chen, *Enforceability of Anti-Reverse Engineering Clauses in Software Licensing Agreements: The Chinese Position and Lessons from the United States and European Union's Laws*, 43 U. PA. J. INT'L L. 783 (2022) (discussing the enforceability of anti-reverse engineering clauses in the United States, EU, and China).

[52] *See* UTSA, *supra* note 43, § 1(2); EU TSD, *supra* note 35, art. 4; 2025 AUCL, *supra* note 43, art. 10.

[53] *See* Varadarajan, *supra* note 49, at 1553; UTSA, *supra* note 43, at §§ 2–3; *cf.* Xingguang Zou & Yang Chen, *Unveiling the Mysterious Role of Contractual Disgorgement: A Comparative and Functional Approach*, 27 U. PA. J. BUS. L. 377, 390–405 (2025) (explaining that disgorgement is also available for some contract claims).

[54] For theoretical debates, *compare* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241 (1998) (questioning trade secrets' IP nature), *and* Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803 (2014) (same), *with* Lemley, *supra* note 38 (justifying trade secrets as IP rights), and Varadarajan, *supra* note 49, at 1550 ("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, *supra* note 33, at 190.

addressing issues that arise in the data economy.[55] Traditionally, trade secret law has applied primarily to business and technological information, such as formulas, methods, customer lists, techniques, and mechanical processes.[56] These examples represent the focal points of historical trade secrets cases centering on the "protection of competitive information that businesses use to advance their marketplace positions."[57] It is not intuitively apparent that it can encompass enterprise data, a relatively new concept emerging from the data economy. However, the subject matter of trade secret law, particularly in today's world, is extremely broad and arguably all-encompassing.[58] Some texts have documented the open-ended nature of trade secret law, which has extended to many novel types of information, including healthcare safety information (clinical research results), environmental information, algorithms underlying automated public decision-making processes, and "sensitive" employee-related information.[59]

Compared to these non-traditional, non-competitive types of information, enterprise data—which is more directly tied to a firm's market competitiveness—is even more likely to fall within the scope of trade secrets protection. The open-ended nature of trade secrets subject matter, which may suitably cover enterprise data, can be seen in modern understandings of trade secret laws shared among jurisdictions. For instance, the U.S.-China Economic and Trade Agreement (Phase One) adopts a broad definition of trade secrets covering any information of commercial value.[60] This Agreement demonstrates

---

[55] Discussions on *how* other IP laws can adapt to solve issues in the new economy abound. *See, e.g.*, *supra* notes 8–9. For discussions on right of personality and trademarks, see Jennifer E. Rothman, *Navigating the Identity Thicket: Trademark's Lost Theory of Personality, the Right of Publicity, and Preemption*, 135 HARV. L. REV. 1271, 1273–78 (2022); Yang Chen, *Navigating the Identity Thicket in China from a Comparative Lens: Conflicting Control Rights over a Person's Name*, 53 H.K.L.J. 843, 843–46 (2023).

[56] *See* Varadarajan, *supra* note 49, at 1548; Eric E. Johnson, *Trade Secret Subject Matter*, 33 HAMLINE L. REV. 545, 546 (2010).

[57] Charles Tait Graves & Sonia K. Katyal, *From Trade Secrecy to Seclusion*, 109 GEO. L.J. 1331, 1346 (2021).

[58] *See* JAMES POOLEY, TRADE SECRETS § 1.01 (L.J. Press ed. 2019) ("Virtually any useful information can qualify as a trade secret."); Varadarajan, *supra* note 49, at 1551; Graves & Katyal, *supra* note 57, at 1350; Deepa Varadarajan, *Business Secrecy Expansion and FOIA*, 68 UCLA L. REV. 462, 471 (2021).

[59] *See* Graves & Katyal, *supra* note 57, at 1352–53, 1368–70, 1385–86; Varadarajan, *supra* note 58, at 480–83.

[60] *See* Economic and Trade Agreement Between the Government of the United States of America and the Government of the People's Republic of China, PRC-U.S., sec. B, Jan. 15, 2020, Off. of the U.S. Trade Representative, https://ustr.gov/countries-regions/china-mongolia-taiwan/peoples-republic-china/phase-one-trade-agreement/text [https://perma.cc/63E7-AQUK] [hereinafter Phase One Agreement].

that, as long as enterprise data can bring potential or actual economic value to holders, it may be granted trade secrets protection—a point that this Article will discuss.[61] UTSA does not clearly cover enterprise data, but it does cover compilation as a type of trade secret, which can be inferred to extend to data compilations.[62] New Jersey's trade secrets statute, based on the UTSA, cites business data compilation as an example of trade secrets.[63] China's laws even more explicitly include data as a type of trade secret, further strengthening the possibility of including enterprise data within the trade secrets domain. Although China's statute defines trade secrets narrowly as only business and technological information, the 2020 judicial interpretation expands this scope by listing novel types of information—such as algorithms, *technical or business data*, computer software, and related documents—as potential candidates for trade secrets.[64] As Aplin et al. succinctly state, "there is nothing that *prima facie* precludes data . . . from being protected."[65]

Applying trade secret law to present-day enterprise data—including large-scale data aggregations or compilations—presents few difficulties, provided that the three core requirements discussed earlier are met. First, most enterprise data can easily satisfy the independent economic value requirement. Individual data points would not be expected to provide the required value, but it is well-established that data aggregations can provide a competitive edge.[66] Enterprise data generated through the collection and aggregation of individual data points can generate substantial value for further development and innovation.[67] The existence of well-developed markets for enterprise data further demonstrates the significant economic value that such data can hold, particularly when firms are among the few within a market possessing a specific type of aggregated data.[68] The European Data Market Study 2021-2023

---

[61] *See infra* notes 66–75 and accompanying text.

[62] *See* UTSA, *supra* note 43, § 1(4).

[63] N.J. STAT. ANN. § 56:15-2 (West 2020); *see* Graves & Katyal, *supra* note 57, at 1349.

[64] *See* 2020 Judicial Interpretation, *supra* note 47, art. 1. *Cf*. 2025 AUCL, *supra* note 43, at art. 10.

[65] Aplin et al., *supra* note 1, at 836.

[66] *See id.* at 841–42.

[67] *See* Drexl, *supra* note 2, at 262–63; Sadowski, *supra* note 5, at 6–8.

[68] *See* Aplin et al., *supra* note 1, at 842; *Commission Staff Working Document Accompanying the Communication "Building a European Data Economy*," at 13, SWD (2017) 2 final (Jan. 10, 2017), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002 [https://perma.cc/NV4T-4XA2]; Cem Dilmegani, *Data Marketplaces: What It Means and Types in 2025*, AI MULTIPLE (Mar. 11, 2025), https://research.aimultiple.com/data-marketplace/ [https://perma.cc/YNU6-L38H] (describing different types of current data marketplaces).

estimates that by 2030, data monetization could generate up to €42 billion in additional spending in the EU data economy—accounting for as much as 36% of new economic activity in the sector.[69] According to the Chinese government, the Chinese national data market had exceeded 160 billion RMB in transaction volume in 2024.[70] These figures underscore how enterprise data is increasingly becoming a valuable asset capable of driving substantial economic returns for those who own it.

Different types of enterprise data may generate varying levels of economic value, depending on the nature of the data and method of use.[71] This, however, does not challenge the proposition that enterprise data satisfies the independent economic value requirement. The threshold for satisfying the value requirement under trade secret law is relatively low, as the value can be actual or potential.[72] This means that firms need only demonstrate the potential economic value or competitive advantage that enterprise data may confer, without having to show any actual benefits derived. Scholars often call for strengthening the commercial value requirement by emphasizing the sub-requirement that value should derive from the secrecy of information,[73] but trade secret holders typically have little difficulty demonstrating that the information provides them with commercial value because of its secrecy.[74] Firms can readily convince courts that their confidential enterprise data may confer at least a modest competitive edge over competitors lacking access to that data, thereby satisfying the independent economic value requirement.[75]

---

[69] INT'L DATA CORP. & LISBON COUNCIL, EUR. COMM'N, EUROPEAN DATA MARKET STUDY 2021–2023, DIGITAL STRATEGY 42 (2024), https://digital-strategy.ec.europa.eu/en/library/results-european-data-market-study-2021-2023 [https://perma.cc/UL4A-U4ZV].

[70] *Tubiao: 2024 Nian Quanguo Shuju Shichang Jiaoyi Guimo Tongi Zengzhang Chao 30%* (图表：2024 年全国数据市场交易规模同比增长超 30%) [*Chart: Nationwide Data Market Transaction Volume in 2024 up by More Than 30%*], ZHONGHUA RENMIN GUOHEGUO ZHONGYANG RENMIN ZHENGFU (中华人民共和国中央人民政府) [THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA] (Apr. 4, 2025), https://www.gov.cn/zhengce/jiedu/tujie/202504/content_7017217.htm [https://perma.cc/QVU5-JPNQ].

[71] For various methods of use, see Sadowski, *supra* note 5, at 5–6.

[72] *See* Camilla A. Hrdy, *The Value in Secrecy*, 91 FORDHAM L. REV. 557, 570–73 (2022).

[73] *See id.* at 590–91; Aplin et al., *supra* note 1, at 842.

[74] *See* Almeling (Federal), *supra* note 40, at 319–20 (showing that during the studied period, only a few U.S. federal courts addressed the value element, and only a few of those courts held that the element was not satisfied); Almeling (State), *supra* note 40, at 92 (the statistics of U.S. state courts indicate the same); Chen, *supra* note 40, at 215–16 (China's statistics also show the same).

[75] *See* POOLEY, *supra* note 58, § 4.05 (1) ("[T]he incremental value of the secret need not be great, just not trivial.").

Enterprise data does not intuitively fulfill the secrecy requirement, which is often cited as one of the limits of trade secret law in the data economy.[76] There are straightforward scenarios, such as when the enterprise data claimed as a trade secret is purely private and confidential, where there is little doubt that enterprise data can receive trade secrets protection.[77] As explained above,[78] sharing enterprise data with internal employees or business partners does not necessarily destroy its secret nature, so long as reasonable efforts are made to maintain its confidentiality.[79]

A more complex question arises in situations when the enterprise data contains not only private data but also publicly accessible information. This type of compilation falls into a preexisting doctrine in trade secret law: combination trade secrets.[80] A combination trade secret refers to a compilation of components, each of which is individually in the public domain and thus unprotectable, but whose synthesis can be legally protected via trade secret law.[81] In *AirFacts, Inc. v. de Amezaga*, the Fourth Circuit, applying Maryland's trade secret statute, reaffirmed that:

> "a trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process, design and operation of which, in unique combination, affords a competitive advantage and is a protectable secret."[82]

---

[76] For this peril and alleged issues with trade secret law in the data economy, see *infra* Part III.

[77] *See* Elkin-Koren, Perel & Somech, *supra* note 3, at 1490–91; Leistner, *supra* note 16, at 235; Cui, *supra* note 3, at 11.

[78] *See supra* notes 44–45 and accompanying text.

[79] *See* POOLEY, *supra* note 58, § 4.04(2)(a).

[80] *See* PETER S. MENELL ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE: VOLUME I—PERSPECTIVES, TRADE SECRETS & PATENTS 60, 62 (Clause 8 Publ'g 2023).

[81] Tait Graves & Alexander Macgillivray, *Combination Trade Secrets and the Logic of Intellectual Property*, 20 SANTA CLARA HIGH TECH. L.J. 261, 266 (2004).

[82] 909 F.3d 84 (4th Cir. 2018) (citing Imperial Chem. Indus. v. Nat'l Distillers & Chem. Corp., 342 F.2d 737, 742 (2d Cir. 1965)). The doctrine is also widely accepted in other states. *See, e.g.*, Sutra, Inc. v. Iceland Exp., No. CIV.A. 04-11360, 2008 WL 2705580, at *4 (D. Mass. July 10, 2008) (Massachusetts); Mike's Train House, Inc. v. Lionel LLC, 472 F.3d 398, 411 (6th Cir. 2006) (Michigan); VFD Consulting, Inc. v. 21st Servs., 425 F. Supp. 2d 1037, 1049 (N.D. Cal. 2006) (Minnesota); Integrated Cash Mgmt. Servs., Inc. v. Digital Transactions, Inc., 920 F.2d 171, 174 (2d Cir. 1990) (New York); Glaxo, Inc. v. Novopharm Ltd., 931 F. Supp. 1280, 1300 (E.D.N.C. 1996), *aff'd*, 110 F.3d 1562 (Fed. Cir. 1997) (North Carolina); San Jose Constr., Inc. v. S.B.C.C., Inc., 67 Cal. Rptr. 3d 54, 63 (Cal. Ct. App. 2007) (California). For other states, *see generally* BRIAN M. MALSBERGER ET AL., TRADE SECRETS: A STATE-BY-STATE SURVEY (7th ed. 2020) (providing a comprehensive guide to how each U.S. state approaches the major trade secret doctrines).

The secrecy and commercial value reside in the combination itself, not in the individual publicly available elements, so only the combination qualifies for trade secret protection.[83] The analogy used by the Northern District of Illinois in *Allstate Ins. Co. v. Ameriprise Fin. Servs*. is illustrative. The case involved customer lists, and the court analogized customer information to the ingredients of a recipe.[84] While the individual ingredients may lack the requisite value due to their public nature, the recipe—that is, the specific way in which those ingredients are combined and arranged—is not accessible to competitors and possesses independent economic value.[85] Applying the combination trade secrets doctrine, enterprise data can warrant legal protection even when some or most data points are public, as long as the combination as a whole is secret. Accordingly, there is no significant doctrinal difficulty in applying trade secret law to private data compilations.

The most challenging type of enterprise data is what this Article terms "semi-public" data compilations. In these scenarios, companies—due to the nature of their business models—must make some or most of the data points within their data aggregations publicly accessible at the front-end, while keeping the compilation as a whole unpublished at the back-end. The enterprise data at issue in *Compulife* exemplifies this category. The plaintiff, Compulife, owned a data aggregation consisting of millions of insurance quotes calculated based on data provided by potential consumers.[86] When a potential customer entered their personal details into Compulife's public website, the system generated and displayed several insurance quotes for the customer to view.[87] Compulife's business model made most of the data points (i.e., the insurance quotes) readily ascertainable by the public through basic data entry.[88] However, the aggregation of all data points was not made publicly available. Accessing the whole data aggregation required direct purchase from

---

[83] Thermodyne Food Serv. Prods., Inc. v. McDonald's Corp., 940 F. Supp. 1300, 1304–05 (N.D. Ill. 1996) (involving a claim of a "combination" trade secret, the value of which inhered in the "interrelationship" of its component parts rather than in the parts themselves); POOLEY, *supra* note 58, at § 11.02 (2)(a) n.13.

[84] Allstate Ins. Co. v. Ameriprise Fin. Servs., Inc., No. 17-CV-5826, 2023 WL 5334638, at *18 (N.D. Ill. Aug. 18, 2023).

[85] *Id.*

[86] Compulife Software, Inc. v. Newman, 959 F.3d 1288, 1296–97 (11th Cir. 2020).

[87] *Id.*

[88] *Id.*

Compulife.[89] The *Compulife* case exemplifies scenarios where data points are publicly available at the front-end but a full aggregated database is not.[90]

From a doctrinal perspective, it appears that the combination trade secrets doctrine can also apply to "semi-public" data compilations.[91] After all, the back-end database is not publicly disclosed, and the public availability of some data points at the front-end does not necessarily harm the secrecy of the data compilation itself. The application is thus premised on the fact that the public cannot easily reproduce the whole data aggregation by independently compiling the front-end data points.[92] Under this condition, the back-end enterprise data is not readily ascertainable and thus protectable as trade secrets.[93]

Finally, trade secrets derive their secrecy from the reasonable measures taken by information holders to maintain confidentiality. This requirement generally calls for trade secret holders to adopt precautions that are proportionate to the value and nature of the trade secret at issue.[94] Despite the variation in requisite measures across individual trade secret cases, certain common practices—whether adopted individually or in combination—can typically help satisfy the reasonableness standard. Typical measures include confidentiality agreements signed by employees or business partners; and technical and physical protections that restrict access to certain persons.[95] Secrecy measures that typically satisfy the reasonableness standard are aligned with practices already implemented by many enterprise data holders. An empirical study on data sharing in the EU shows that the main protection measures taken by companies sharing their confidential and commercial data with others are contracts (e.g., non-disclosure agreements) and technical measures to restrict access.[96] These closely resemble the standard secrecy

---

[89] *Id.*

[90] Some scholars argue that even in *Compulife*, the data aggregation itself was readily ascertainable because there were no measures taken to restrict public access to data points. *See, e.g.*, Cui, *supra* note 3, at 18. This Article will explore and discuss that argument in detail. *See infra* Part III.

[91] *See, e.g.*, Cui, *supra* note 3, at 15–18. This Article, however, respectfully disagrees with this position for normative reasons detailed in Part III.

[92] *See* Cui, *supra* note 3, at 17.

[93] *See id.* at 10–12, 15–18.

[94] *See* POOLEY, *supra* note 58, § 4.04 (2)(b); Aplin et al., *supra* note 1, at 844.

[95] *See* Almeling (Federal), *supra* note 40, at 322–23; Almeling (State), *supra* note 40, at 80–81; Chen, *supra* note 40, at 220, 237.

[96] *See* ALFRED RADAUER ET AL., EUR. COMM'N, STUDY ON THE LEGAL PROTECTION OF TRADE SECRETS IN THE CONTEXT OF THE DATA ECONOMY: FINAL REPORT 58–60 (2022),

practices already recognized under existing trade secret laws.[97] Thus, there is no additional step for firms to take in order to satisfy the reasonable secrecy measure requirement. This highlights a critical aspect of treating enterprise data, particularly private data and data compilations, as trade secrets: it is a protection approach that aligns very closely to the current market practice.[98]

It seems that doctrinally, enterprise data can be treated as trade secrets. The existing doctrines of trade secret law are sufficiently flexible to extend protection to private and confidential enterprise data and data compilations—provided that they meet the three core requirements for trade secret protection. As the current literature argues, the combination trade secrets doctrine may even extend to "semi-public" data compilations under sufficient secrecy measures, a point that this Article will revisit after examining recent cases.[99] At this point, an interim conclusion can be drawn: trade secret law *may* have a promising role to play in the data economy because of its resilience. Putting the doctrinal analysis aside, there is value in exploring how current law and practice have recognized the role of trade secret law in the data economy.

III. ENTERPRISE DATA SECRETS: GROWING RECOGNITION WITHOUT WIDER APPLICATION

No other study has documented in detail how the concept of enterprise data as trade secrets has been recognized in practice, despite emerging scholarly discussions. As such, this Part serves as the first attempt to examine how the three jurisdictions have applied trade secret law to protect enterprise data, thereby highlighting the *status quo*. It begins with a positive account of private data and data compilations, the first two types of enterprise data, followed by an analysis of "semi-public" data compilations.

---

https://op.europa.eu/en/publication-detail/-/publication/c0335fd8-33db-11ed-8b77-01aa75ed71a1/language-en [https://doi.org/10.2826/021443].

[97] For example, training, guidelines, or policies for employees; specific clearing process during staff recruitment; and actions targeted toward departing staff to ensure post-employment confidentiality. *See id.* at 59. *Cf.* 2020 Judicial Interpretation, *supra* note 47, art. 6 (written policies and requests for post-employment confidentiality); Almeling (State), *supra* note 40, at 81 (education of employees about secrecy, written policies, and interviews); Chen, *supra* note 40, at 237 (written policies, entrance and exit interviews, and requirement for the return of work materials and products upon separation).

[98] *See* Lü, *supra* note 27, at 66–67. For discussions on the measures taken by data holders in the context of "semi-public" data compilations and whether these measures are sufficient to maintain secrecy, see *infra* Part III.

[99] *See infra* Part III.

A. Private Data and Data Compilations: Consistent and Growing Recognition

With respect to scenarios in which most of the underlying data points are private and confidential—circumstances that, as previously noted, present no barrier to the direct application of trade secret law—courts have consistently upheld trade secret claims in the data economy.[100]

U.S. courts began recognizing confidential enterprise data as trade secrets at an early stage.[101] For example, in *P.C. of Yonkers, Inc. v. Celebrations! The Party & Seasonal Superstore, L.L.C.*, the District Court for the District of New Jersey held that a comprehensive database containing franchisee sales and revenue data, customer data, merchandise data, and vendor information constituted protectable common law trade secrets.[102] The court applied trade secret law in a straightforward way. This data, after being compiled by and for use in the plaintiff's business and subject to several measures to restrict its dissemination, constituted a trade secret.[103] Other U.S. courts have reached similar results.[104] This approach of using trade secret law to protect confidential data remains unchanged after the promulgation of the federal DTSA.[105]

Courts have also recognized the potential of trade secret law to protect enterprise data compilations—which remain secret even when some individual data points are publicly accessible—in the data economy. For example, the court in *DiscoverOrg Data, LLC v. ThisWay Global, LLC* rejected the defendant's argument that the plaintiff needed to plead that all subsets of its data

---

[100] *See supra* notes 82–84 and accompanying text.

[101] Although courts recognized confidential enterprise data early on, they usually did so under the doctrinal label of trade secret protection for databases or compilations, rather than as a separate category of "enterprise data." *See* Miriam Bitton, *A New Outlook on the Economic Dimension of the Database Protection Debate*, 47 IDEA, no. 2, 2006, at 156–57.

[102] No. CIV.A.04-4554, 2007 WL 708978, at *10–11 (D.N.J. Mar. 5, 2007).

[103] *Id.*

[104] *See generally*, QSRSoft, Inc. v. Rest. Tech., Inc., No. 06 C 2734, 2006 WL 2990432 (N.D. Ill. Oct. 19, 2006) (holding that a similar compilation of franchisee data was a trade secret under the Illinois Trade Secrets Act); E. Point Sys., Inc. v. Maxim, No. 3:13-CV-00215 (VAB), 2016 WL 1169553 (D. Conn. Mar. 22, 2016) (holding that the plaintiff's private database was accessible to users as a trade secret under Connecticut's UTSA equivalent).

[105] *See, e.g.*, Primacy Eng'g, Inc. v. SAN Eng'g, No. 1:18-CV-129-RP, 2018 WL 3520143, at *2 (W.D. Tex. July 20, 2018) (holding that the plaintiff had plausibly alleged trade secret claims under the DTSA and Texas UTSA, as the plaintiff's technical data package could qualify as a protectable trade secret); KPM Analytics N. Am. Corp. v. Blue Sun Sci., LLC, No. 4:21-CV-10572, 2021 WL 2982866, at *13 (D. Mass. July 15, 2021) (holding that non-publicly available database of customer-contributed information constituted trade secrets under the Massachusetts UTSA and DTSA).

compilations were trade secrets to survive the motion to dismiss.[106] It would be sufficient for the plaintiff to plead the proprietary nature of only the full compilation.[107] Similarly, in *Prysmian Cables & Systems USA, LLC v. Szymanski*, the court considered trade secrets protection for compilations of data as well-established law, and rejected the defendant's argument that the public availability of some portions of the plaintiff's technical data package undermined its secrecy.[108] Another district court, applying the DTSA and Illinois' UTSA equivalent, neatly stated that "a compilation of data, even if the component parts are in the public domain, may be protectable as a trade secret if it would require substantial time, effort, and expense to recreate the compilation."[109] Other district and circuit courts have ruled similarly.[110]

China's awareness of enterprise data secrets is also on the rise. An increasing number of Chinese scholars have begun to explore the feasibility of using trade secret law to protect enterprise data.[111] This approach is also receiving much more attention from Chinese courts.[112]

It is not novel for Chinese courts to apply trade secret law to protect business data when the asserted data was purely confidential. For example, the Supreme People's Court (SPC) once held that the whole data package

---

[106] No. A-20-CV-91, 2020 WL 10054509, at *2 (W.D. Tex. Dec. 1, 2020).

[107] *Id.* at *2.

[108] *See* Prysmian Cables & Sys. USA, LLC v. Szymanski, 573 F. Supp. 3d 1021, 1043 (D.S.C. 2021).

[109] *See* Abrasic 90 Inc. v. Weldcot Metals, Inc., 364 F. Supp. 3d 888, 897 (N.D. Ill. 2019).

[110] *See, e.g.*, Zvelo, Inc. v. Akamai Techs., Inc., No. 19-CV-00097, 2019 WL 4751809, at *7–8 (D. Colo. Sep. 30, 2019) (holding that a data compilation containing many publicly available URLs was a trade secret under the Colorado UTSA and the DTSA); AirFacts, Inc. v. De Amezaga, 909 F.3d 84, 95–97 (4th Cir. 2018) (concluding that flowcharts compiling public airline ticket data were trade secrets under the Maryland UTSA); United States v. Nosal, 844 F.3d 1024, 1042–43 (9th Cir. 2016) (holding a compiled database of a secret combination of public and private data to be trade secrets under the Economic Espionage Act); Allstate Ins. Co. v. Fougere, 79 F.4th 172, 189 (1st Cir. 2023) (determining that a compilation of some publicly available data, such as data obtainable from governmental registry and third-party websites, was a trade secret under the DTSA and the Massachusetts UTSA equivalent because the compilation itself is difficult to replicate). *But see* Citizens Info. Assocs., LLC v. JustMugshots.com, No. 1-12-CV-573, 2013 WL 12076563, at *3 (W.D. Tex. Feb. 26, 2013) (dismissing a trade secrets claim because all data comprising the compilation was public domain information, even though the defendant had scraped and copied essentially all of it).

[111] *See, e.g.*, Cui, *supra* note 3 (advocating strongly in favor of treating most enterprise data as trade secrets); Lü, *supra* note 27, at 65–68 (discussing the possibility and resilience of trade secrets protection on enterprise data while also highlighting the negative consequences); Lu Chunxin (卢纯昕), *Shuju Baohu de Lei Shangye Mimi Lujing Jiangou* (数据保护的类商业秘密路径建构) [*Constructing a Trade Secret-Like Path for Data Protection*], ZHISHI CHANQUAN (知识产权) [INTELL. PROP.], no. 3, 2024, at 91 (arguing that trade secret law offers protection for confidential data).

[112] *See infra* notes 113–119 and accompanying text.

containing the data resources of a particular technology was a protectable trade secret.[113] A Chongqing court once protected an enterprise's business data package containing confidential information about competitors' products as a trade secret.[114]

In addition to these conventional circumstances, Chinese courts are increasingly applying trade secret law to protect private enterprise data in the big data era, even when the data is more dynamic, large-scale, and complex. For instance, the Hangzhou Intermediate People's Court had no difficulty recognizing password-protected back-end data as trade secrets.[115] The court held that the defendant had misappropriated those trade secrets by using the back-end data to predict livestream lottery odds without authorization.[116] A recent decision by a Zhejiang Intermediate Court further concluded that confidential enterprise data products can be protected as trade secrets.[117] In that case, the court held that enterprise data comprising both publicly available information and derivative data generated through analysis of raw data—such as business forecasting, performance metrics, and data analytics—are protectable as trade secrets.[118] In another case decided by the Beijing courts,

---

[113] Dalian Beitong Shuju Pingtai Guanli Zhongxin Su Cui Mouji (大连倍通数据平台管理中心诉崔某吉) [Dalian Beitong Data Platform Mgmt. Ctr. v. Cui Mouji], (2021) Sup. People's Ct. Intell. Prop. Civ. Final Judgment No. 1687 (Sup. People's Ct. Mar. 14, 2022) (China).

[114] Chongqing Guangmou Motuoche Zhizao Youxian Gongsi Su Guangzhou Sanmou Motuoche Youxian Gongsi (重庆光某摩托车制造有限公司诉广州三某摩托车有限公司)[Chongqing Guangmou Motorcycle Mfg. Co., Ltd. v. Guangzhou Sanmou Motorcycles Co., Ltd.], (2022) Civ. First-Instance Judgment No. 8589 (Chongqing Free Trade Zone No. 192 People's Ct. Aug. 2023) (China).

[115] Hangzhou Mou Keji Gongsi Yu Wang Mou (杭州某科技公司与汪某) [Hangzhou X Tech. Co. Ltd v. Wang], (2021) Civ. Second-Instance Judgment No. 11274 (Hangzhou Intermediate People's Ct. 2021) (China).

[116] *Id.*

[117] Miao Moumou Su Hangzhou Shi Yuhang Qu Shichang Jiandu Guanli Ju, Hangzhou Shi Yuhang Qu Renmin Zhengfu & Mou (Zhongguo) Ruanjian Youxian Gongsi (缪某某诉杭州市余杭区市场监督管理局、杭州市余杭区人民政府、某（中国）软件有限公司行政处罚及行政复议纠纷案) [Miao Moumou v. Yuhang Dist. Mkt. Supervision Admin. of Hangzhou, Yuhang Dist. People's Gov't of Hangzhou & Mou (China) Software Co., Ltd.], (2024) Zhejiang Intermediate People's Ct. Admin. First-Instance Judgment No. 89 (Hangzhou Intermediate People's Ct. Aug. 29, 2024) (China).

[118] *See* Chen Chao (陈超), *Shangye Mimi Baohu Anli | Quanguo Shouli, Hangzhou Hulian Dachang de "Shengyi Canmou" Shuju Chanpin, Bei Rending Wei Shangye Mimi Yuyi Baohu* (商业秘密保护案例｜全国首例，杭州互联大厂的"生意参谋"数据产品，被认定为商业秘密予以保护) [*Trade Secret Protection Case | First Case Nationwide: Hangzhou Internet Giant's "Business Advisor" Data Product Recognized and Protected as a Trade Secret*], WANGLUO SHUJU FA (网络数据法) [CYBER DATA L.] (Sep. 9, 2024), https://mp.weixin.qq.com/s/cVhsVBebFpRRB9yeu9UJ6g [https://perma.cc/7B6B-EBS3].

the first instance court found that 1,505 hours of collected voice data was a trade secret.[119]

Some Chinese local governments, when designing supplementary measures (such as a data property registration system) to implement the "data property rights system" promoted by the central government, have adopted the concept of enterprise data as trade secrets. Under the Provisional Measures for the Registration of Data Intellectual Property Rights adopted in Beijing, Tianjin and Shandong, registrable enterprise data must be: (1) non-public, (2) obtained through legitimate means, (3) processed or transformed according to specific rules or algorithms, and (4) possess commercial value.[120] While registration does not create rights, it does serve as prima facie evidence of their existence.[121] Therefore, governmental registration of enterprise nonetheless provides support for the existence of protectable trade secrets.[122]

The concept of confidential enterprise data as trade secrets has received growing support in another digital empire—the EU. The results of the EU's

---

[119] On appeal, however, the Beijing intellectual property court determined that the enterprise data at issue was a 200-hour subset of the secret 1,505-hour voice data collection and held that this subset did not qualify as a trade secret because it had been voluntarily disclosed. Shumou (Beijing) Keji Gufen Youxian Gongsi Su Yinmou (Shanghai) Keji Youxian Gongsi (数某（北京）科技股份有限公司诉隐某（上海）科技有限公司) [Shumou (Beijing) Tech. Co. Ltd. v. Yinmou (Shanghai) Tech. Co. Ltd.], (2024) Civ. Second-Instance Judgment No. 546 (Beijing No. 3 Intermediate People's Ct. 2024) (China).

[120] 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), art. 6, Tianjin Intell. Prop. Examination & Approval No. 2, 2024, https://zscq.tj.gov.cn/zwgk/zcwj/zscqwj/202402/t20240227_6545482.html [https://perma.cc/96GU-QX4H]; 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 of Beijing (Trial)] (promulgated by Beijing Intell. Prop. Off., May 30, 2023, effective June 19, 2023), art. 2, THE PEOPLE'S GOV'T. OF BEIJING MUN., https://www.beijing.gov.cn/zhengce/zhengcefagui/202311/t20231115_3301983.html [https://perma.cc/HE6C-F6CS]; 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), art. 3. It is argued that Fujian's data registration follows the same non-public requirement. *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*], HUADONG ZHENGFA DAXUE XUEBAO (华东政法大学学报) [J.E. CHINA U. POL. SCI. & L.], no. 6, 2024, at 85.

[121] *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*], ZHISHI CHANQUAN (知识产权) [INTELL. PROP.], no. 3, 2024, at 36–39 (China).

[122] *See* Lü, *supra* note 27, at 63–65.

"Public Consultation on the Data Act" in 2021 indicated that the majority of respondents (58% of 336) rely on trade secrets protection when sharing data with business partners.[123] In particular, sectors such as finance (90%), agriculture (85%), and telecommunication (77%) relied heavily on trade secrets protection in business data-sharing scenarios.[124] The subsequent "Study on the Legal Protection of Trade Secrets in the Context of the Data Economy" continued to explore the feasibility, possibility and current status of protecting enterprise data as trade secrets.[125] Its survey of empirical evidence showed that 68% of firms who are at least somewhat familiar with trade secrets believe that trade secret law is being or could be used to protect their confidential and commercially valuable data shared with others.[126] Moreover, 71% of firms believed that trade secret law is at least "rather appropriate" to protect shared confidential and commercially valuable data.[127] The same scholars also conducted a doctrinal analysis affirming their confidence in EU trade secret law's capacity to protect confidential and commercially valuable enterprise data.[128]

In addition, courts in several EU member states have recognized that trade secret law may protect confidential data or data compilations, provided the requirements are met. For instance, in a landmark case decided by the Court of Appeal of Montpellier in France, a database containing years of research and trial data on new insecticidal nets received trade secrets protection.[129] Similarly, in Italy, the Court of Milan held that a database could simultaneously

---

[123] EUR. COMM'N, PUBLIC CONSULTATION ON THE DATA ACT: SUMMARY REPORT 5 (2021), https://digital-strategy.ec.europa.eu/en/public-consultation-data-act-summary-report [https://perma.cc/5W6R-FQMM].

[124] *Id.* at 5.

[125] *See generally* RADAUER ET AL., *supra* note 96 (examining the role of enterprise data in the EU, assessing when such data can qualify as trade secrets, and evaluating the feasibility and policy implications of relying on trade secret law to protect industrial and machine-generated data).

[126] *Id.* at 64–65.

[127] *Id.* at 66.

[128] *See* Aplin et al., *supra* note 1, at 839–46.

[129] Cour d'appel [CA] [regional court of appeal] Montpellier, 2e ch., May 14, 2019, 15/07646 (Fr.), *see* JONES DAY, 2021 MID-YEAR REVIEW: KEY GLOBAL TRADE SECRET DEVELOPMENTS 1, 7–8 (Aug. 2021), https://www.jonesday.com/-/media/files/publications/2021/08/2021-midyear-review-key-global-trade-secret-developments/files/2021-global-trade-secrets-midyear-review/fileattachment/2021-global-trade-secrets-midyear-review.pdf [https://perma.cc/F44K-AEJM].

enjoy sui generis protection and trade secrets protection, provided it was kept secret by adequate measures.[130]

The EU Data Act, effective since January 2024, also partially echoes the concept of enterprise data as trade secrets. The Data Act mainly aims to harmonize rules regarding data access within the EU, but also acknowledges that requiring the disclosure of some data may jeopardize data holders' trade secrets.[131] Thus, it explicitly affirms the proposition that certain enterprise data, if confidential, may be protected as trade secrets under the EU TSD even when such data is subject to disclosure obligations under the Data Act.[132] When dealing with access to or disclosure of data that amounts to trade secrets, the Data Act requires that necessary measures be taken to preserve the confidentiality and trade secret status of the shared data.[133] The Act highlights a subcategory of trade secrets under the TSD: data secrets.[134]

Overall, the concept of confidential enterprise data—or secret compilations thereof—as trade secrets has been gaining consistent and increasing recognition across the three digital empires. This is evidenced by a growing number of affirmative judicial decisions, legislative developments, governmental regulations, and rising practical and scholarly awareness.

B. "Semi-Public" Data Compilations: Limited Recognition Without Wider Application

Much like Compulife, many companies in the data economy structure their business models to allow public access to enterprise data points at the front-end while keeping the entire data compilation secret at the back-end.[135] However, the real-world application of trade secret law in this context remains limited. *Compulife* continues to stand as one of the few cases where trade

---

[130] Tribunale di Milano [Court of Milan], 9 Oct. 2020, No. 6142/2020 (It.); *see Case Law on Trade Secrets in Italy*, CMS LEGAL (Feb. 21, 2023), https://cms.law/en/int/expert-guides/trade-secrets-case-law/italy#:~:text=,corporate%20matters%2C%2009%20October%202020 [https://perma.cc/NV4L-J5A5].

[131] Regulation 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonized Rules on Fair Access to and Use of Data (Data Act), 2023 O.J. (L 2023/2854) 1, recitals 1–5, 31, arts. 4(6), 5(9), 17(2)(d), 19(3), 21(3).

[132] *See id.*

[133] *See id.*

[134] *See* Ella De Noyette, Leander Stähler & Thomas Margoni, *Data Secrets: The Data Act's New Trade Secrets Framework*, 56 INT'L REV. INTELL. PROP. & COMPETITION L. 984, 986 (2025).

[135] *See* Cui, *supra* note 3, at 16.

secret law has been used to protect "semi-public" enterprise data compilations.[136]

Again, *Compulife* involved a data aggregation comprising millions of individual insurance quotes that were publicly accessible through customer queries.[137] One aspect that distinguished *Compulife* from previous cases was that the data points within the plaintiff's aggregation were voluntarily made more accessible at the front-end due to business needs.[138] Customers could simply input information into the website to retrieve relevant insurance quotes. Neither terms of service restrictions nor technological barriers limited access to the front-end data.[139] *Compulife* is also notable for departing from the typical fact pattern of trade secret misappropriation based on unauthorized use or disclosure in breach of a duty of confidence, as seen in cases discussed above.[140] Instead, the case was concerned with the defendant's use of modern technology—a data scraping bot—to send different input data to the website to scrape more than forty-three million quotes, amounting to a significant portion of the plaintiff's data aggregation.[141] It took the defendant only four days to replicate the data using the scraping bot, which "required hundreds of thousands of queries and would have required thousands of man-hours if performed by humans."[142] Whether the defendant's data scraping amounted to trade secrets misappropriation was one of the issues before the court.[143] The critical aspects of *Compulife* lead a scholar to view it as the first case to use trade secret law to protect "publicly available (and hence scrape-able) databases."[144]

The status of the data aggregation as a trade secret was not contested on appeal,[145] but the Eleventh Circuit, in addressing the misappropriation element, reasoned as follows. Even though the individual quotes within the plaintiff's data aggregation were publicly available and thus not protectable on their own,

---

[136] *See* Xiao, *supra* note 19, at 128–29. Case searches do not return any other circuit court decisions reaching a similar result.

[137] *See supra* notes 86–90 and accompanying text.

[138] Unlike the other previously mentioned cases, the data compilations include some publicly available data but impose more public access limitations after compilation. *See supra* notes 106–110.

[139] *See* Xiao, *supra* note 19, at 141–44.

[140] *See supra* notes 106–110.

[141] Compulife Software, Inc. v. Newman, 959 F.3d 1288, 1299–1300 (11th Cir. 2020).

[142] *Id.*

[143] *Id*. at 1300.

[144] Xiao, *supra* note 19, at 128–29.

[145] *Compulife*, 959 F.3d at 1310.

acquiring all or a substantial portion of the aggregation through improper means could still constitute misappropriation of a protectable trade secret.[146] The court affirmed its own determination upon a second appeal, holding that the whole compilation of otherwise publicly individual quotes can still be a trade secret under the DTSA and Florida's UTSA equivalent because it "would be nearly impossible for a human to obtain through the website without scraping."[147] Thus, *Compulife* sent a strong signal to stakeholders that trade secret law can be a feasible avenue of enterprise data protection, even if their business models require the publication of some or most of the data points, when others use modern technology to scrape large portions of their data compilations.[148]

Although *Compulife* sparked heated discussions about the future role of trade secret law in protecting enterprise data against data scraping,[149] subsequent decisions involving similar "semi-public" data compilations have not relied on trade secret law to the extent argued by some scholars.[150] After *Compulife*, there have been comparable cases where plaintiffs sought to invoke trade secret law to protect their back-end enterprise data against third-party data scraping activities. For example, in *UAB "Planner5D" v. Facebook, Inc.*, the plaintiff survived a motion to dismiss its trade secrets claims based on the compilation of object and scene data files underlying the images shown to users.[151] Users could view and control the images on their screens, but the underlying object and scene data files were stored at secret internet addresses not directly accessible without circumventing the Planner5D software.[152] When the defendant used data scraping techniques to retrieve and replicate the

---

[146] *Id.* at 1313–14.

[147] Compulife Software, Inc. v. Newman, 111 F.4th 1147, 1161 (11th Cir. 2024).

[148] *See* Xiao, *supra* note 19, at 146–48.

[149] *See*, e.g., Peter J. Toren, *A Dubious Decision: Eleventh Circuit Finds Scraping of Data from a Public Website Can Constitute Theft of Trade Secrets (Part I)*, IPWATCHDOG (Jul. 2, 2020, at 16:15 PST), https://ipwatchdog.com/2020/07/02/dubious-decision-eleventh-circuit-finds-scraping-data-public-website-can-constitute-theft-trade-secrets-part/id=123029/ [https://perma.cc/NS2X-FP8M] [hereinafter Toren (Part I)]; Peter J. Toren, *Improper Means? The Eleventh Circuit's Dubious Trade Secrets Decision in Compulife Software v. Newman (Part II)*, IPWATCHDOG (July 14, 2020 at 12:15 PST), https://ipwatchdog.com/2020/07/14/improper-means-eleventh-circuits-dubious-trade-secrets-decision-compulife-software-v-newman-part-ii/id=123265/ [https://perma.cc/E9SZ-7M7Z] (expressing deep concern about the future wider application of *Compulife* in similar cases) [hereinafter Toren (Part II)].

[150] *See* Xiao, *supra* note 19, at 172.

[151] UAB "Planner5D" v. Facebook, Inc., No. 19-CV-03132-WHO, 2020 WL 4260733, at *6–9 (N.D. Cal. July 24, 2020).

[152] *Id.* at *7.

compilation of these hidden data files, they potentially acquired protectable trade secrets through improper means.[153] This case highlights a scenario in which enterprise data at the back-end might still be a protectable trade secret when aspects of its content are publicly viewable at the front-end, as long as the compilation of underlying data files remains confidential. Note, however, that *UAB "Planner5D"* differs from *Compulife* in that users were not given direct access to any underlying data files themselves, only to visual representations (images) derived from them.

In *Software Automation Holdings, Inc. v. Ins. Toolkits, LLC*, the plaintiff invoked trade secret law under the DTSA and North Carolina law to protect its enterprise data—a compilation of insurance industry data developed for its "Best Plan Pro" (BPP) software that was only accessible to paid users.[154] The complaint alleged that defendants created numerous fictitious user accounts (for instance, by using gift cards with insufficient funds) to gain unauthorized access to the BPP system and scrape its data, which was used in developing their competing insurance software.[155] In an early ruling, the court refused to dismiss the trade secret misappropriation claims, indicating its willingness to treat the compiled insurance data as a potentially protectable trade secret pending further proceedings.[156] In *DHI Grp., Inc. v. Kent*, the Fifth Circuit found a database compiling a massive number of resumes to be a protectable trade secret under the Texas UTSA.[157] Paid subscribers could access the resumes at the front-end, but the resume collection as a whole was kept secret and remained unpublished.[158] By hacking into the system and copying hundreds of thousands of resumes, the defendant misappropriated trade secrets.[159]

In a similar vein, in China, an intermediate court in Jiangsu applied trade secret law to protect a data product called "Business Advisor." Developed by the large online shopping platform Taobao, the product consisted of various types of information derived from analyzing the massive data collected from platform stores and users.[160] The data primarily included predictive,

---

[153] *Id.* at *8–9.

[154] Software Automation Holdings, Inc. v. Insurance Toolkits, LLC, No. 5:23-CV-140-D, 2024 WL 3297138, at *1–2 (E.D.N.C. July 3, 2024).

[155] *Id.* at *2.

[156] *Id.* at *1.

[157] No. 21-20274, 2022 WL 3755782, at *7–10 (5th Cir. Aug. 30, 2022).

[158] *Id.*

[159] *Id.* at *2.

[160] Zhejiang Taobao Wangluo Youxian Gongsi Su Moumou Taoshu Youxian Gongsi (浙江淘宝

index-based, and statistical information, displayed in the form of trend charts, rankings, proportion graphs, and similar formats, which may be useful for its platform stores.[161] Taobao offered multiple tiers of access to the data points in the product. Subscribers to the basic version could access standard categories of the data. Alternatively, they could opt for the professional version, which included both the basic and all professional-level categories. Users could also subscribe to the basic version and pay an additional fee to access specific professional categories deemed necessary for their business.[162] The court held that the defendant misappropriated protectable trade secrets by employing technical means to acquire a substantial portion of data from the "Business Advisor."[163]

These cases do not mirror the extreme scenario in *Compulife*, where most data points underlying the insurance website were much more easily accessible. However, all of them concern the acquisition of the whole or a substantial part of a data compilation at the back-end despite the accessibility of certain front-end data points to customers.[164] And in all of them, courts acknowledged the application of trade secret law to protect "semi-public" data compilations.

However, in several U.S. disputes with fact patterns more closely resembling that of *Compulife*, trade secret law claims were not raised by

---

网络有限公司诉某某淘数有限公司) [Zhejiang Taobao Network Co., Ltd. v. Moumou Taoshu Co., Ltd.], (2023) Su 01 Civ. First-Instance Judgment No. 4082 (Nanjing Intermediate People's Ct., Jiangsu June 12, 2025) (China) [hereinafter "2023 Jiangsu Case on Business Advisor"]; *see Taobao "Shengyi Canmou" Shuju An Pan Pei 3000 Wan* (淘宝"生意参谋"数据案判赔 3000 万) [*Taobao "Business Advisor" Data Lawsuit Results in 30 Million Yuan in Damages*], ZHI CHAN KU (知产库) [IPCODE] (June 23, 2025), https://mp.weixin.qq.com/s/m_Djj-WTzy7PM83k2R-dEg [https://perma.cc/VSK8-8ERN]. A Zhejiang intermediate court also held the data product as trade secrets albeit in an administrative case. *See* Miao Moumou Su Hangzhou Shi Yuhang Qu Shichang Jiandu Guanli Ju (缪某某诉杭州市余杭区市场监督管理局) [Miao Moumou v. Yuhang Dist. Mkt. Supervision Admin. of Hangzhou], (2024) Zhejiang Intermediate People's Ct. Admin. First-Instance Judgment No. 89 (Hangzhou Intermediate People's Ct. Aug. 29, 2024) (China) [hereinafter "2024 Zhejiang Case on Business Advisor"). The decision was upheld by a Zhejiang appellate court. *See* Miao Moumou Su Hangzhou Shi Yuhang Qu Shichang Jiandu Guanli Ju (缪某某诉杭州市余杭区市场监督管理局) [Miao Moumou v. Yuhang Dist. Mkt. Supervision Admin. of Hangzhou], (2024) Zhejiang High People's Ct. Admin. Final Judgment No. 862 (Zhejiang High People's Ct. 2024) (China).

[161] 2023 Jiangsu Case on Business Advisor, *supra* note 160.

[162] *Id.*

[163] *Id.*

[164] *Cf.* Cui, *supra* note 3, at 18 (arguing that the data compilation in *Compulife* should be considered readily ascertainable when there was no access restriction).

plaintiffs seeking to protect "semi-public" data compilations.[165] This has been true even in cases involving more substantial restrictions on access to front-end data—such as login credentials, password protection, and explicit terms of service—where trade secret law would theoretically be more applicable under the *Compulife* approach.[166] For example, in a series of cases concerning airlines, third-party websites scraped flight information data by sending a significant volume of automated search requests to the user interface of airline websites, essentially harvesting the whole or a substantial portion of the back-end data compilations.[167] Some claimants argued that the sections being scraped by defendants were non-public and only accessible to authorized users through their accounts.[168] Still, the plaintiffs did not sue under trade secret law.[169]

Similar situations have occurred in China. In fact, Chinese courts are at the forefront of adjudicating enterprise data protection cases and have decided a considerable number of relevant disputes.[170] To date, the majority of cases

---

[165] The cases cited below are referenced solely to illustrate the potential applicability of trade secret law, without reaching any conclusions or arguments that the defendants' conduct in these cases necessarily constituted trade secret misappropriation. Whether there was a protectable trade secret and whether misappropriation occurred depends on the specific conduct involved and the portions of data scraped by the defendants. Further analysis of these issues will follow below. *See infra* Part III.

[166] Again, whether the back-end data compilations in particular cases qualify as trade secrets depends on the specific circumstances. This Article merely seeks to emphasize that in the subsequently discussed cases, where greater access restrictions are imposed on front-end data points, the back-end data compilations may likewise satisfy the secrecy requirement. This is especially true under the reasoning in *Compulife*, according to which even the absence of any access restrictions does not preclude trade secret protection. For further discussions on whether enterprise data in each type of case may satisfy the secrecy requirement, mainly the "not readily ascertainable" standard, see *infra* Part III.

[167] *See, e.g.*, Air Canada v. Localhost LLC, No. CV 23-1177, 2024 WL 1251286, at *1–2 (D. Del. Mar. 14, 2024) (sued under contract law); Ryanair DAC v. Booking Holdings Inc., No. CV 20-1191-WCB, 2024 WL 3732498, at *2 (D. Del. June 17, 2024) (sued under the Computer Fraud and Abuse Act (CFAA)); Ryanair DAC v. Booking Holdings Inc., 636 F. Supp. 3d 490, 496 (D. Del. 2022) (sued under the CFAA and contract law); Sw. Airlines Co. v. Kiwi.com, Inc., No. 3:21-CV-00098, 2021 WL 4476799, at *1–2 (N.D. Tex. Sep. 30, 2021) (sued under the CFAA, contract law, and more).

[168] *See, e.g.*, *Ryanair*, 636 F. Supp. 3d at 496 ("Ryanair alleges that the myRyanair section of the website is not public.").

[169] *See* cases cited *supra* note 167.

[170] For a list of Chinese cases related to enterprise data protection and other related unfair competition behaviors, see *Jin Wunian Shuju Fa Anli Huizong Mulu* (近五年数据法案例汇总目录) [*Summary Catalogue of Data Law Cases in the Past Five Years*], XIN LU REN (新律人) [NEW LEGAL PROF.] (Mar. 5, 2025), https://mp.weixin.qq.com/s/ImpIoSrMNHucjzzXMAjziw [https://perma.cc/MV5V-CSZF].

were decided under the general or specific provisions of the PRC Anti-Unfair Competition Law (AUCL), rather than the trade secrets provision.[171]

There are disputes that arguably resemble *Compulife*.[172] For example, the Shenzhen Intermediate Court once decided a case under the general provision

---

[171] For examples of cases not decided under trade secret law, see *infra* notes 172–176. In China, the AUCL contains one general provision (Article 2) and some specific provisions, including on trade secret protection (mainly Article 10). Each specific provision is designed to govern a particular type of unfair competition behavior. The general provision applies only when the conduct at issue does not fall into any specific provision. It serves as a broad and catch-all clause for other unfair competition conduct against accepted business ethics. Although trade secrets protection in China, due to its IP nature, follows a somewhat different internal logic from other specific provisions, it is nonetheless regulated under the AUCL. For a discussion of China's AUCL system and how the general provision under the AUCL is applied in IP cases, *see generally* Wenjie Ding & Li Chen*, A Functionalist Approach to a Principled Application of the General Clause of China's Anti-Unfair Competition Law in Intellectual Property Cases,* 12 QUEEN MARY J. INTELL. PROP. 512 (2023).

[172] *See, e.g.*, Hunan Yifang Ruanjian Gufen Youxian Gongsi Yu Beijing Weimeng Chuangke Wangluo Jishu Youxian Gongsi (湖南蚁坊软件股份有限公司与北京微梦创科网络技术有限公司) [Hunan Yifang Software Co. v. Beijing Weimeng Chuangke Network Tech. Co.], (2019) Beijing Intell. Prop. Ct. Civ. Final Judgment No. 3789 (Beijing Intell. Prop. Ct. Feb. 2, 2021) (China) (involving the scraping of public and non-public data of the social media platform Weibo); Shenzhen Shi Gumi Keji Youxian Gongsi Yu Beigao Wuhan Yuanguang Keji Youxian Gongsi (深圳市谷米科技有限公司与被告武汉元光科技有限公司) [Shenzhen Gumi Tech. Co., Ltd. v. Wuhan Yuanguang Tech. Co.], (2017) Shenzhen Intermediate People's Ct. Civ. First-Instance Judgment No. 822 (Shenzhen Intermediate People's Ct., Guangdong May 23, 2018) (China) [hereinafter "2017 Shenzhen Case on Bus Operating Data"] (a back-end data compilation of massive real-time data related to buses, such as running times and real-time locations); Anhui Meijing Xinxi Keji Youxian Gongsi Yu Taobao (Zhongguo) Ruanjian Youxian Gongsi (安徽美景信息科技有限公司与淘宝（中国）软件有限公司) [Anhui Meijing Info. Tech. Co. v. Taobao (China) Software Co.], (2018) Hangzhou Intermediate People's Ct. Civ. Final Judgment No. 7312 (Hangzhou Intermediate People's Ct., Zhejiang Dec. 18, 2018) (China) (back-end data compilations developed by Taobao, an online shopping platform, containing data points that include public information about shops and goods on the platform, as well as derivative data generated through analyzing public information); Beijing Taoyou Tianxia Jishu Youxian Gongsi Yu Beijing Weimeng Chuangke Wangluo Jishu Youxian Gongsi (北京淘友天下技术有限公司与北京微梦创科网络技术有限公司) [Beijing Taoyou Tianxia Tech. Co. v. Beijing Weimeng Chuangke Network Tech. Co.], (2016) Beijing Intell. Prop. Ct. Civ. Final Judgment No. 588 (Beijing Intell. Prop. Ct. Dec. 30, 2016) (China) (back-end data compilations of Weibo user information, including some parts that are only minimally accessible from the front-end); Shenzhen Shi Tengxun Jisuanji Xitong Youxian Gongsi Yu Zhejiang Soudao Wangluo Jishu Youxian Gongsi (深圳市腾讯计算机系统有限公司与浙江搜道网络技术有限公司) [Shenzhen Tencent Computer Sys. Co. v. Zhejiang Soudao Network Tech. Co.], (2019) Hangzhou Railway Transp. Ct. Civ. First-Instance Judgment No. 1987 (Hangzhou Railway Transp. Ct., Zhejiang June 2, 2020) (China) (data of messaging and social media platform users); Beijing Lianjia Fangdichan Jingji Youxian Gongsi Yu Beijing Shenying Chengxun Keji Gufen Youxian Gongsi (北京链家房地产经纪有限公司与北京神鹰城讯科技股份有限公司) [Beijing Lianjia Real Estate Brokerage Co. v. Beijing Shenying Chengxun Tech. Co.], (2021) Beijing Haidian Dist. People's Ct. Civ. First-Instance Judgment No. 9148 (Beijing Haidian Dist. People's Ct. July 29, 2022) (China) (data compilations of housing information available via user searches, but protected with anti-scraping measures to limit suspicious or automated searches); Shanghai Fuyu Wenhua

of the AUCL, wherein the plaintiff collected and maintained a back-end database of real-time data on bus operating times and locations, while permitting limited front-end data access to app users through specific searches.[173] Trade secret law was not invoked to protect this "semi-public" data compilation when the defendant scraped massive amounts of data from the back-end database.[174]

In another case decided by a Beijing court, the plaintiff, a real estate company, maintained a large-scale database containing housing data for over 100 million properties, including basic information on homes available for sale, transaction records, property photos, and floor plans. Users could access relevant housing data on the front-end through specific searches but were not granted direct access to the entire database. Likewise, trade secret law was not invoked to protect the database from the defendant's front-end data scraping activities.[175]

Similarly, in a case concerning AMap, a widely used map application and website in China that provides traffic congestion predictions for specific cities requested by users, the defendant scraped prediction data across 100 cities by sending automated requests to AMap.[176] Again, the case appears to involve a "semi-public" data compilation, as the back-end database compiling the prediction data is arguably inaccessible to normal users, who can only retrieve data for specific cities at the front-end by making particular requests.[177] The

---

Chuanbo Gufen Youxian Gongsi Yu Beijing Weimeng Chuangke Wangluo Jishu Youxian Gongsi (上海复娱文化传播股份有限公司与北京微梦创科网络技术有限公司) [Shanghai Fuyu Culture Commc'n Co. v. Beijing Weimeng Chuangke Network Tech. Co.], (2019) Beijing Intell. Prop. Ct. Civ. Final Judgment No. 2799 (Beijing Intell. Prop. Ct. Nov. 15, 2019) (China). (Weibo user information containing publicly accessible data, data available only after login, and non-public back-end data); Beijing Gaode Yuntu Keji Youxian Gongsi Yu Wande Xinxi Jishu Gufen Youxian Gongsi (北京高德云图科技有限公司与万得信息技术股份有限公司) [Beijing Gaode Yuntu Technology Co. v. Wind Info. Tech. Co.], (2023) Beijing Chaoyang Dist. People's Ct. Civ. First-Instance Judgment No. 21370 (Beijing Chaoyang Dist. People's Ct. June 26, 2024) (China) (derivative data on daily traffic congestion predictions for multiple cities, developed and analyzed using information and data collected from users).

[173] 2017 Shenzhen Case on Bus Operating Data, *supra* note 172.

[174] *See* Cui, *supra* note 3, at 16.

[175] Beijing Lianjia Fangdichan Jingji Youxian Gongsi Yu Beijing Shenying Chengxun Keji Gufen Youxian Gongsi (北京链家房地产经纪有限公司与北京神鹰城讯科技股份有限公司) [Beijing Lianjia Real Estate Brokerage Co. v. Beijing Shenying Chengxun Tech. Co.], (2021) Beijing Haidian Dist. People's Ct. Civ. First-Instance Judgment No. 9148 (Beijing Haidian Dist. People's Ct. July 29, 2022) (China).

[176] Beijing Gaode Yuntu Keji Youxian Gongsi Yu Wande Xinxi Jishu Gufen Youxian Gongsi (北京高德云图科技有限公司与万得信息技术股份有限公司) [Beijing Gaode Yuntu Tech. Co. v. Wind Info. Tech. Co.], (2023) Beijing Chaoyang Dist. People's Ct. Civ. First-Instance Judgment No. 21370 (Beijing Chaoyang Dist. People's Ct. June 26, 2024) (China).

[177] *See id.*

case was resolved under the general provision of the AUCL rather than trade secret law.[178]

The situation in the EU is slightly different because of its unique sui generis database protection regime. When it comes to scraping front-end data to form a substantial portion of the back-end compilation, some EU member states relied on the sui generis protection directly rather than trade secret law. For instance, in a French case involving Leboncoin, a classified ads website, the Paris Court of Appeal had little difficulty in granting *sui generis* protection to the plaintiff's database. The court held the defendant liable for scraping front-end data on the website—specifically, listings in the real estate subcategory—on the ground that the extracted content constituted a qualitatively substantial portion of the protected back-end database.[179] This ruling has since been applied and followed by lower courts in France.[180]

Even though the above disputes resemble *Compulife*, the claimants did not consider trade secret law as a viable avenue for protecting the "semi-public" data compilations that were acquired. Trade secret law has not been applied broadly to "semi-public" data compilations.

IV. REASONS AND PERILS: THE LIMITS OF TRADE SECRET LAW

The positive analysis in Part III highlights that the concept of enterprise data as trade secrets has been receiving increasing recognition when it comes to private data and data compilations. However, such a trend does not exist in the scenarios of "semi-public" data compilations. This presents a conundrum: why does trade secret law continue to receive limited recognition for "semi-public" data compilations as compared to private data and data compilations? Should it receive such attention? This Part answers both questions and sets forth normative arguments against any wider recognition.

---

[178] *See id.*

[179] Cour d'appel [CA] [regional court of appeal] Paris, Feb. 2, 2021, 17/17688 (Fr.) (LBC France SAS c. Entreparticuliers.com); *see* Aissatou Sylla, *France: Protecting a Website from Unlawful Data Scraping*, HOGAN LOVELLS (June 19, 2023), https://www.hoganlovells.com/en/publications/france-protecting-a-website-from-unlawful-data-scraping [https://perma.cc/5HAR-Y86J].

[180] *See, e.g.*, Cour judiciaire [TJ] Nanterre, May 31, 2024, 22/08082 (Fr.) (LBC France SAS c. Babel S.A.S.) (concerning a similar real estate sub-database).

A. Revisiting the Secrecy of "Semi-Public" Data Compilations

Regardless of the doctrinal possibility, there is a critical caveat for protecting "semi-public" data compilations as trade secrets: they must still satisfy the secrecy requirement despite front-end data points being accessible to the public. Even advocates of trade secret law protection for this type of enterprise data acknowledge that such protection requires some restrictions on access to the front-end data points such that the back-end data compilation cannot be easily obtained.[181]This caveat introduces the need to assess whether the back-end enterprise data is not readily ascertainable. It is unclear how strong the restrictions on access to front-end data points must be to prevent the public from too easily appropriating the back-end data compilations.

There are some clear scenarios on either end of the spectrum. On one end, access restrictions are so stringent that the front-end data is rendered largely private. A typical instance is business models that offer access to front-end data points through paid subscriptions and some accompanying technical restrictions. *DHI Group* is a representative example. The individual front-end resumes were only available to a limited number of customers who created accounts and paid subscription fees.[182] By subscribing, these customers were contractually restricted from reselling, further using, or making available the obtained resumes. [183] These terms functioned, at least in part, like confidentiality clauses to prevent the wider dissemination of individual resumes. There were similar restrictions on sharing login credentials, [184] and technical measures were in place to lock "users out of the database if they downloaded too many resumes over a short period of time."[185] Due to these measures, even subscribed users could not—without directly circumventing technical restrictions—easily obtain a substantial portion of the back-end data compilation of resumes, rendering it not readily ascertainable. Unsurprisingly, the plaintiff resorted to trade secret law, and the court upheld the trade secrets claims.

The Chinese cases concerning the aforementioned "Business Advisor" data product share a similar fact pattern. [186] Access to the front-end data was

---

[181] *See* Cui, *supra* note 3, at 11.
[182] DHI Grp. v. Kent, No. 21-20274, 2022 WL 3755782, at *8–9 (5th Cir. Aug. 30, 2022).
[183] *Id.* at *9–10.
[184] *Id.* at *10.
[185] *Id*. at *8 n. 8.
[186] Zhejiang Taobao Wangluo Youxian Gongsi Su Moumou Taoshu Youxian Gongsi (浙江淘宝

multilayered and restricted to paid users who subscribe to the corresponding service tiers. All subscribers were also subject to contractual terms requiring them to keep all data confidential and prohibiting them from reselling, transferring, licensing, or allowing others to use said data.[187] Thus, only a limited number of users could access substantial volumes of front-end data points, while most users could access only limited portions. This effectively rendered the entire back-end data compilation—namely the data product itself—not readily ascertainable to the public without either purchasing the highest-tier subscription (subject to contractual limitations) or directly bypassing technical restrictions and hacking into the system.

On the other end, no meaningful restrictions are attached to accessing the front-end data. Some business models exemplify this scenario. Several publicly accessible websites or applications—notably social media platforms such as X (formerly Twitter) and Reddit—represent such models.[188] These business models typically need to offer users very open access to their front-end data points, making them susceptible to massive scraping.[189] As a result, disputes are abundant. For example, the professional networking website LinkedIn is experiencing numerous data scraping attempts every day.[190] The Ninth Circuit has concluded that LinkedIn allows public access to data on its users' public profiles without requiring prior authorization.[191] Likewise, X is responding furiously to other companies' attempts to scrape data—such as tweets, comments, images, and videos—from its platform.[192] TikTok is another

网络有限公司诉某某淘数有限公司) [Zhejiang Taobao Network Co. v. Moumou Taoshu Co.], (2023) Su 01 Civ. First-Instance Judgment No. 4082 (Nanjing Intermediate People's Ct., Jiangsu June 12, 2025) (China); Anhui Meijing Xinxi Keji Youxian Gongsi Yu Taobao (Zhongguo) Ruanjian Youxian Gongsi (安徽美景信息科技有限公司与淘宝（中国）软件有限公司) [Anhui Meijing Info. Tech. Co. v. Taobao (China) Software Co.], (2018) Hangzhou Intermediate People's Ct. Civ. Final Judgment No. 7312 (Hangzhou Intermediate People's Ct., Zhejiang Dec. 18, 2018) (China).

187 *See* cases cited *supra* note 186.

188 However, it is hard to argue that the current version of X is such an open platform, as it has begun limiting logged-out users' access to tweets. *See generally* Melany Amarikwa, *Internet Openness at Risk: Generative AI's Impact on Data Scraping*, 30 RICH. J.L. & TECH. 533 (2024).

189 Training AI models involves massive volumes of data, most of which comes from scraping these publicly accessible platforms. *See id.* at 546–49.

190 hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1186 (9th Cir. 2022).

191 *Id.* at 1197–98.

192 *See, e.g.*, X Corp. v. Bright Data Ltd., 733 F. Supp. 3d 832, 840 (N.D. Cal. 2024) (alleging that Bright Data scraped public web data from X and sold it to others); X Corp. v. Ctr. for Countering Digital Hate, Inc., 724 F. Supp. 3d 948, 957–59 (N.D. Cal. 2024) (alleging that CCDH, a user of the X platform, scraped data from X and produced research reports and articles that X considered as false and misleading).

example, as it provides largely open access to its short videos and related information (such as user profiles and comments), making it susceptible to scraping by third-parties.[193] One Chinese case involves a similar situation. A website named "12365auto" collected, compiled, edited, and published hundreds of thousands of data entries containing customer complaints about various car models. Because it did not adopt any technical restrictions or require login credentials to limit access to these entries, the website became a target for data scraping by industry competitors.[194]

By keeping data compilations at the back-end while providing public access to individual data points at the front-end, these platforms held enterprise data satisfying the definition of "semi-public" data compilations. However, access to front-end data points was largely unrestricted, making it relatively easy to reconstruct a substantial portion or even the entirety of the back-end data compilation. Because such "semi-public" data compilations are readily ascertainable, they fall outside the reach of trade secret law.[195]

The extreme scenarios do not capture the full range of common business models in the data economy. Many business models occupy the space between the two poles and provide users with front-end access to data while also imposing certain access restrictions. These models have become increasingly

---

[193] Beijing Chuangrui Wenhua Chuanmei Youxian Gongsi Yu Beijing Weibo Shijie Keji Youxian Gongsi (北京创锐文化传媒有限公司与北京微播视界科技有限公司) [Beijing Chuangrui Culture Media Co. v. Beijing Weibo Vision Tech. Co.], (2021) Beijing Intell. Prop. Ct. Civ. Final Judgment No. 1011 (Beijing Intell. Prop. Ct. Mar. 16, 2023) (China). The defendant scraped the short videos, user information and user comments from TikTok). *Id.*

[194] Beijing Aodisi Pinpai Guanli Zixun Youxian Gongsi Yu Beijing Chezhiwang Xinxi Jishu Youxian Gongsi (北京奥蒂思品牌管理咨询有限公司与北京车质网信息技术有限公司) [Beijing Aodisi Brand Mgmt. Consulting Co. v. Beijing Chezhiwang Info. Tech. Co.], (2022) Beijing Intell. Prop. Ct. Civ. Final Judgment No. 3718 (Beijing Intell. Prop. Ct. Oct. 28, 2022) (China) (holding that the defendant scraping more than 50,000 data entries from the website constituted actionable unfair competition under the general provision of the AUCL). For other similar cases, *see* Zhejiang Tianmao Wangluo Youxian Gongsi Yu Guangzhou Ruiwei Xinxi Keji Youxian Gongsi (浙江天猫网络有限公司与广州锐微信息科技有限公司) [Zhejiang Tmall Network Co. v. Guangzhou Ruiwei Info. Tech. Co.], (2021) Guangzhou Internet Ct. Civ. First-Instance Judgment No. 1692 (Guangzhou Internet Ct. Nov. 23, 2022) (China) (finding that the defendant scraped data on goods, transactions, and logistics that was publicly available on Taobao, an online shopping platform); Beijing Weimeng Chuangke Wangluo Jishu Youxian Gongsi Yu Beijing Zijie Tiaodong Keji Youxian Gongsi (北京微梦创科网络技术有限公司与北京字节跳动科技有限公司) [Beijing Weimeng Chuangke Network Tech. Co. v. Beijing ByteDance Tech. Co.], (2017) Beijing Haidian Dist. People's Ct. Civ. First-Instance Judgment No. 24530 (Beijing Haidian Dist. People's Ct. May 17, 2021) (China) (finding that the defendant scraped public user posts and related information from the social media platform Weibo).

[195] This partially explains why the plaintiffs primarily sued under contract law or CFAA, not trade secret law, in these cases. *See* cases cited *supra* notes 190–194.

prevalent in the AI era, as many open platforms that were originally open now adopt measures to limit access and curb large-scale data scraping for AI training purposes.[196] This hybrid approach complicates the question of whether the back-end data compilations are readily ascertainable. For instance, at one point, X temporarily blocked unregistered users from browsing tweets, user profiles, and comment threads unless they signed into an account.[197] X also started restricting access to its API by charging users, making large-scale data scraping more difficult.[198] Some social media platforms such as Facebook and Instagram have long required account logins to view most content and limiting public access to APIs.[199] However, these limitations did not effectively deter data scraping on these platforms. Meta is suing several companies for scraping data from its Facebook and Instagram applications.[200] In *Meta Platforms, Inc. v. Ates*, the defendant created 10,000 automated Instagram accounts by scraping all user data on Instagram, including names, usernames, user profiles, posts, and pictures, and replicating the data on his Instagram "clone sites."[201]

In a similar dispute, the grocery-delivery app Instacart claimed that the Uber-backed online grocery rival Cornershop scraped product images, descriptions, pricing data, and other information from Instacart to launch a competitive platform.[202] Instacart alleged that Cornershop created Instacart user accounts to access its full catalog and conducted large-scale searches for retailer products, thereby scraping all data returned by Instacart.[203] In China, Taobao has also adopted technical restrictions, allowing users who are not

---

[196] *See* Amarikwa, *supra* note 188, at 550–56.

[197] Jess Weatherbed, *Twitter Has Started Blocking Unregistered Users*, THE VERGE (June 30, 2023, at 9:36 PM), https://www.theverge.com/2023/6/30/23779764/twitter-blocks-unregistered-users-account-tweets [https://perma.cc/CL85-CWXR]; *see* Amarikwa, *supra* note 188, at 553–54.

[198] *See* Amarikwa, *supra* note 188, at 554.

[199] *See id.* at 551–52.

[200] *See generally*, Facebook, Inc. v. Sluchevsky, No. 19-CV-01277, 2020 WL 5823277, at *6 (N.D. Cal. Aug. 28, 2020) (alleging that the defendants scraped Facebook user data by deceiving users into installing extensions that accessed and scraped Facebook's HTTP servers and by sending unauthorized commands that purported to originate from users); Meta Platforms, Inc. v. Soc. Data Trading Ltd., No. 21-CV-09807, 2022 WL 18806265 (N.D. Cal. Dec. 8, 2022) (alleging that the defendant scraped usernames, profile pictures, posts, likes, and follower information on Instagram by using automated accounts and bots).

[201] No. 22-CV-03918, 2023 WL 4035611, at *2 (N.D. Cal. May 1, 2023), report and recommendation adopted, No. 4:22-CV-3918, 2023 WL 4995717 (N.D. Cal. June 27, 2023).

[202] Complaint ¶¶ 1–8, Maplebear Inc. v. Cornershop Techs., Inc., No. 2:20-cv-00240, (E.D. Tex. July 16, 2020).

[203] *Id*. ¶¶ 81–83.

logged in to view only thumbnails of products, with full access to product information granted to users after logging in.[204]

Making certain front-end data viewable only after account login does not render otherwise readily ascertainable back-end data compilations trade secrets. Under this business model, all the front-end data points remain publicly accessible so long as members of the public simply create and log into free accounts. Therefore, it can be argued that scraping technology merely facilitates access to publicly available information rather than enabling acquisition of information that is otherwise difficult to access.[205] It would be counterintuitive for back-end data compilations to be considered secret when most front-end data points remain publicly accessible through free and unrestricted logins.[206] Accordingly, trade secrets protection can be easily ruled out for "semi-public" data compilations of online platforms whose business models dictate the public nature of their front-end content.

However, business models that involve more restricted and limited access to front-end data points make for more challenging case studies. *Compulife* again serves as an illuminating example. Unlike online platforms where front-end content is directly accessible to the public, each data point on Compulife's website—namely, each insurance quote—is generated and retrieved from the back-end database in response to user inputs.[207] While the website itself is publicly accessible, the front-end data points are not directly viewable. Thus, the Eleventh Circuit considered that reconstructing a substantial portion of the underlying database would require extensive and systematic querying, which would be highly impractical through manual human requests alone.[208] The court's opinion remained consistent despite the defendant's argument on appeal that the public could pull all insurance quotes from the database without any limitations.[209]

---

[204] Shaoxing Hengmou Keji Youxian Gongsi Yu Taomou (Zhongguo) Ruanjian Youxian Gongsi (绍兴衡某科技有限公司与淘某（中国）软件有限公司) [Shaoxing Hengmou Tech. Co., Shanghai Jingmou Network Tech. Co. v. Taomou (China) Software Co.], (2023) Zhejiang High People's Ct. Civ. Final Judgment No. 1113 (Zhejiang High People's Ct. Dec. 29, 2023) (China).

[205] *Cf.* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1171–72 (2016) (viewing login credentials as meaningful gates to differentiate between authorized and unauthorized access to contents).

[206] This partially explains why plaintiffs in these cases primarily sued under contract law or the CFAA, not trade secret law. *See* cases cited *supra* notes 200–202.

[207] *See supra* notes 86–90 and accompanying text.

[208] Compulife Software, Inc. v. Newman, 959 F.3d 1288, 1314 (11th Cir. 2020).

[209] Compulife Software, Inc. v. Newman, 111 F.4th 1147, 1162 (11th Cir. 2024).

At first glance, the Eleventh Circuit Court's reasoning may seem plausible. It suggests that the standard for assessing whether information is readily ascertainable hinges solely on the feasibility of using manual efforts to reverse engineer or independently develop it.[210] Applying this reasoning, it is true that *manually* pulling and recompiling these data points to form the back-end compilation is a lengthy and costly process, and the compilation is not easily reverse engineered through human effort alone. However, the legal standard for determining whether information is readily ascertainable is not confined to human means unaided by technological tools. The legislative comments to the UTSA merely state that information may qualify as "not readily ascertainable" if reverse engineering would be lengthy and expensive, without specify the particular means by which the reverse engineering must be conducted.[211] The only relevant inquiry is whether the means employed are "proper."[212]

Distinguishing data scraping technology from human effort as an illegitimate method of access seems artificial, as technological means have long been used to facilitate information acquisition.[213] Much has been written about how advancements have made it cheaper and easier to reverse engineer secrets that would previously have seemed well-kept and out of reach.[214] With the advent of AI technology—capable of rapidly searching, locating, and processing vast amounts of information—some argue that certain trade secrets may become significantly more discernable, spelling the end of their trade secret status.[215] While the "not readily ascertainable" standard is grounded in human abilities,[216] those capabilities have and will continue to evolve alongside advancements in technological tools made available to humans. Why, then, did

---

[210] *Id.* at 1162 ("[T]he whole compilation of them (which would be nearly impossible for a human to obtain through the website without scraping) can still be a trade secret.").

[211] *See* UTSA, *supra* note 43, § 1 cmt.

[212] *Id.* § 1(4)(i) ("not being readily ascertainable by proper means").

[213] The details of this issue will be discussed in the next section. *See infra* Part III.

[214] *See, e.g.*, Jacob S. Sherkow, *The Myth of DNA Trade Secrecy*, 75 U.C.L.J. 1047, 1088–90 (2024) (arguing that the development of DNA sequencing technology has gradually diminished the protectability of DNA sequence information as trade secrets); Samuel J. LaRoque, *Reverse Engineering and Trade Secrets in the Post*-Alice *World*, 66 KAN. L. REV. 427, 439–40 (2017) (arguing that advances in technology may make reverse engineering software codes easier); Hrdy, *supra* note 51, at 108–15 (discussing the ways to reverse engineer AI models and arguing that such reverse engineering may become easier, cheaper, and quicker).

[215] *See* Camilla Alexandra Hrdy, *Trade Secrecy Meets Generative AI*, 100 CHI.-KENT L. REV. 1, 8–12 (forthcoming 2025); David S. Levine, *Generative Artificial Intelligence and Trade Secrecy*, 3 J. FREE SPEECH L. 559, 581 (2023); Sprankling, *supra* note 8, at 206–08.

[216] *See* Sprankling, *supra* note 8, at 194–95.

the courts in *Compulife* not consider the extent to which the insurance quotes could be readily ascertained by humans employing available data scraping technology to extract and recompile the insurance quotes into a substantial portion of the back-end compilation?[217]

Applying the line of reasoning from *Compulife*, trade secret law may essentially extend its reach to most of the aforementioned airline disputes.[218] For example, in *Air Canada v. Localhost LLC*, Air Canada maintained a database that stored information about flight times, routes, and the amount of loyalty points customers needed to purchase a flight.[219] Users could retrieve specific data on particular flights by sending requests through the user interface. The defendant in the case allegedly scraped data from the database by using automated digital bots that sent thousands of search requests via the user interface over a two-day period.[220] Some airlines may adopt more technical restrictions on the availability of front-end data points by, for example, requiring that users log into an account, even if the account is free, to perform search requests. Such was the case in *Ryanair DAC v. Booking Holdings Inc.*, in which Ryanair repeatedly highlighted the non-public nature of the "myRyanair" section of its website; only authorized users with an account could view and purchase flights.[221] The defendant allegedly accessed the section without authorization and scraped the flight information data retrieved from the back-end database.[222] Per *Compulife*, such business models that make only select data points available at the front-end in response to customer queries involve not readily ascertainable "semi-public" data compilations. This raises the question: why have other airlines, which use similar data access and retrieval models, not asserted trade secret protection for their databases? Why have they not raised trade secret claims in litigation?

Upholding such claims would be inconsistent with the intent of trade secret law. Correctly applied, the "not readily ascertainable" standard is meant to account for the difficulty and cost of reverse engineering. In comparison, retrieving and recompiling these "semi-public" data compilations is neither overly difficult nor time-consuming. In fact, it may be no more costly than

---

[217] *See* Cui, *supra* note 3, at 18 (arguing that *Compulife* concerns a readily ascertainable back-end data compilation).
[218] *See* cases cited *supra* note 167.
[219] No. CV 23-1177, 2024 WL 1251286, at *1 (D. Del. Mar. 14, 2024).
[220] *Id.*
[221] 636 F. Supp. 3d 490, 496, 508–09 (D. Del. 2022).
[222] *Id.* at 496.

collecting and combining content on public-facing social media and online platforms. The technologies used to access, collect, and compile data for both types of business models are virtually identical, typically involving HTML or screen scraping, crawler scraping, or API scraping.[223]

This is why *Compulife* continues to stand as the only case that applied trade secret law to protect "semi-public" data compilations. If the *Compulife* standard of "not readily ascertainable" were to be broadly adopted, it could open the floodgates of trade secret protection, enabling online platforms that operate under more open-access business models to assert plausible claims.[224] After all, without technological assistance, humans cannot collect and recompile any large-scale data in a cost-efficient manner. As a result, virtually all "semi-public" data compilations could be deemed to satisfy the *Compulife* standard, regardless of how public the front-end data is. Adopting such a low threshold for "not readily ascertainable" clearly overlooks public interests in permitting third-parties to assess, collect, compile and analyze data across various platforms.[225] It would further exacerbate the platform data lockout concerns currently raised by several scholars, leading to outcomes that are unlikely to strike a sound balance between the protection of private interests and the public's access to information.[226]

The interim conclusion, thus, is that the secrecy of a back-end data compilation is undermined where the public can easily access and collect front-end data points through technological means. Still, one question persists: how protected must front-end data points be in order for the "semi-public" data compilations to be considered "not readily ascertainable" and therefore to receive trade secrets protection? This Article argues that trade secret law is normatively justified in offering protection only when front-end data access is as limited as in the aforementioned clear scenarios, such as the *DHI* and "Business Advisor" cases. Extending trade secrets protection beyond that to most other "semi-public" data compilations is unlikely to have efficiency gains that outweigh associated costs.

---

[223] *See* Amarikwa, *supra* note 188, at 539–40.

[224] *See* Toren (Part I), *supra* note 149 (arguing that the insurance quotes are public information and that, as such, it would be flawed for courts to hold the compilation of these quotes to be not readily ascertainable).

[225] *See* Elkin-Koren, Perel & Somech, *supra* note 3, at 1485–87.

[226] *See, e.g.*, *id.* at 1491–99 (discussing technological and legal barriers to accessing data); Amarikwa, *supra* note 188, at 550–56.

In addition to login credentials and API restrictions, platforms are currently adopting various technical measures to restrict automated access and scraping of their front-end data. Additional access restrictions typically include blocking requests from suspicious IP addresses, implementing rate and data limits, using technical checks to confirm human behaviors, and canceling unauthorized accounts.[227] For example, Meta has implemented lockout mechanisms, rate and data limits, and technical checks such as CAPTCHAs. It also deploys machine-learning models to detect and block suspicious scraping activities in addition to pre-existing login credential requirements.[228] In the previously discussed Chinese case concerning a back-end database of city traffic congestion predictions, the plaintiff (AMap) adopted measures like automatic pop-up terms of service, and technical safeguards that reject data retrieval when requests evidently exceed the normal frequency of human users.[229] Similar technical measures were used in the aforementioned Chinese housing data case.[230]

With these commonly adopted technical access restrictions in place, collecting and compiling front-end data points by scraping technology may become less productive without more advanced tools. Back-end data compilations may thus become less readily ascertainable. However, this does not necessarily mean that back-end datasets meet the "not readily ascertainable" standard required by trade secret law. These measures merely make collecting and compiling front-end data points slower and more challenging, not implausible.[231] Meanwhile, technological advancements

---

[227] *See* Amarikwa, *supra* note 188, at 555; Kerr, *supra* note 205, at 1166–76 (discussing ways to restrict access, including cookies, IP address blocking, and CAPTCHA—a way to detect non-human behavior, login credentials, and account cancellations).

[228] Meta Platforms, Inc. v. Bright Data Ltd., No. 23-cv-00077, 2024 WL 251406, at *1 (N.D. Cal. Jan. 23, 2024).

[229] Beijing Gaode Yuntu Keji Youxian Gongsi Yu Wande Xinxi Jishu Gufen Youxian Gongsi (北京高德云图科技有限公司与万得信息技术股份有限公司) [Beijing Gaode Yuntu Tech. Co. v. Wind Info. Tech. Co.], (2023) Beijing Chaoyang Dist. People's Ct. Civ. First-Instance Judgment No. 21370 (Beijing Chaoyang Dist. People's Ct. June 26, 2024) (China).

[230] Beijing Lianjia Fangdichan Jingji Youxian Gongsi Yu Beijing Shenying Chengxun Keji Gufen Youxian Gongsi (北京链家房地产经纪有限公司与北京神鹰城讯科技股份有限公司) [Beijing Lianjia Real Estate Brokerage Co. v. Beijing Shenying Chengxun Tech. Co.], (2021) Beijing Haidian Dist. People's Ct. Civ. First-Instance Judgment No. 9148 (Beijing Haidian Dist. People's Ct. July 29, 2022) (China).

[231] *See* Kerr, *supra* note 205, at 1166–70 (considering cookies and technical checks like CAPTCHA as ways to slow a user's access); Amarikwa, *supra* note 188, at 555; Gintaras Radauskas, *AI and Data Scraping: Websites Scramble to Defend Their Content,* CYBERNEWS (Nov. 15, 2023), https://cybernews.com/editorial/ai-data-scraping-websites/

continuously pose threats to existing trade secrets.[232] Scraping bots have become increasingly "intelligent" and capable of circumventing restrictions to successfully extract targeted data.[233] Scraping technologies may also become increasingly accessible to industry actors who stand to benefit from the data.[234].

At this point, it can be posited that uncertainty is an inherent feature of the "not readily ascertainable" standard under trade secret law. Whether technical measures restricting access to front-end data are sufficient to render "semi-public" data compilations "not readily ascertainable" remains ambiguous. However, given the doctrinal possibility, courts should be entrusted with the task of deciding which business models around "semi-public" data compilations may satisfy the standard. The line between "readily ascertainable" and "reverse engineerable" (but not readily ascertainable) is a crucial but not a bright one under current law.[235] However, future line-drawing by courts could significantly (re)shape the dynamic between platforms and data collectors, especially if courts open the door of trade secret law to "semi-public" data compilations like the *Compulife* courts did. The mere doctrinal possibility of protection does not, from the normative perspective set out below, justify its extension.

Extending trade secret protection, which already resembles the property-like protections found in other areas of intellectual property law, comes with costs, so justifying expansion requires corresponding benefits.[236] One of the most critical benefits of trade secret law is its function of limiting the inefficient arms race between trade secret holders and potential appropriators, easing the burden on information holders to guard against all possible exposure of their trade secrets.[237] In traditional contexts, secret holders normally do not have a

---

[https://perma.cc/T46L-K9TR] ("With data scraping, you can never prevent 100% of the attempts. Your goal is to increase the difficulty level for scrapers to the correct level for your business.").

[232] *See supra* notes 214–215 and accompanying text.

[233] *See* Amarikwa, *supra* note 188, at 555.

[234] *See*, *e.g.*, *The Rise of AI in Web Scraping: 2024 Stats That Will Surprise You*, SCRAPINGAPI (Dec. 4, 2024), https://scrapingapi.ai/blog/the-rise-of-ai-in-web-scraping [https://perma.cc/DQE5-NT6V]; *The Importance of Data Scraping—Trends, Benefits, and Tools in 2025*, BOXPIPER (Nov. 10, 2025), https://www.boxpiper.com/posts/the-importance-of-data-scraping-trends-benefits-and-tools [https://perma.cc/7YGP-ST3U].

[235] POOLEY, *supra* note 58, § 4.04 [4].

[236] For a full-length discussion on the cost-benefit analysis on the current form of trade secrets protection, *see generally* the articles cited in *supra* note 54.

[237] *See* 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, *supra* note 38, at 333–34.

business need to share their secrets, or any parts of them, with the public. The parties with whom they typically share information are employees and potential business collaborators, who can be subject to non-disclosure agreements and other reasonable measures to control further dissemination.[238] Trade secret law can spare secret holders from needing to adopt other, more burdensome safeguards against the actions of unrelated third-parties.[239] In this context, the "uncertainty" surrounding the "not readily ascertainable" standard is largely compatible with the law's intended function. When trade secrets are inherently private and only closely shared, the measures taken by holders to render information "not readily ascertainable" are mostly to restrict further disclosure and use by those who accessed the information legitimately. In these scenarios, the "not readily ascertainable" standard remains fact-dependent, [240] but trade secret holders generally understand the typical reasonable measures required to maintain the secrecy of their information, such as non-disclosure agreements and restrictions on broader dissemination.[241] Trade secret law operates to ensure that the "not readily ascertainable" status is not compromised by the lack of safeguards against unforeseeable conduct like espionage. Thus, in traditional industries, trade secret law can effectively promote business efficiency by reducing the need for excessive protective measures with limited uncertainty surrounding the "not readily ascertainable" standard.

"Semi-public" data compilations, however, prompt a different kind of arms race at the front-end. Because their business models depend public access to front-end data, data holders have increasingly adopted layered technical measures to restrict front-end data access and deter scraping. Meanwhile, scraping technologies continue to evolve in ways that circumvent these technical measures, resulting in a continuous arms race between data holders and scrapers. Opening the door of trade secret law protection to these "semi-public" data compilations, however, will not prevent such inefficient racing behavior.

---

[238] *See* Lemley, *supra* note 38, at 335–37.

[239] *See id.*

[240] After all, they cannot control whether competitors can independently development or reverse engineer based on publicly available information. Otherwise, there would be no protectable trade secret.

[241] Chinese law provides a list of typical measures. *See* 2020 Judicial Interpretation, *supra* note 47, art. 6. Empirical studies in the United States and China show that typical secrecy measures are roughly similar. *See* Almeling (State), *supra* note 40, at 81; Chen, *supra* note 40, at 237; Almeling (Federal), *supra* note 40, at 322.

When parts of trade secrets are shared with the wider public, rather than a limited number of parties, merely adopting reasonable measures to maintain the secrecy of the overall trade secret is not sufficient to satisfy the "not readily ascertainable" standard. The standard requires further restrictions on the public availability of the different components of trade secrets. As the court in *Rockwell Graphic Systems, Inc. v. DEV Industries*, *Inc.* explained, when various components of a trade secret are dispersed outside the corporate veil without adequate control measures, the trade secret holder is more likely to fail in asserting a misappropriation claim against a party that independently combines those components to reconstruct the secret.[242] Therefore, "semi-public" data holders must adopt sufficient control measures over their front-end data in order for the back-end compilation to satisfy the "not readily ascertainable" standard—regardless of how effectively they have limited direct access to the back-end data itself.

While data holders generally understand what constitutes sufficiently reasonable measures in traditional contexts, trade secret law offers little guidance in the case of "semi-public" data compilations. The threshold of protective measures required for their back-end compilations to meet the "not readily ascertainable" standard is unclear. This legal uncertainty leaves data holders with little assurance of protection and continued need for restriction measures to fend off evolving data scraping technologies. Conversely, the climate of legal uncertainty and evolving scraping techniques might motivate data holders to adopt even more technical safeguards on front-end access in hopes of successfully invoking trade secret protection against data scrapers for their back-end data compilations.

A costly and wasteful arms race between data holders and potential appropriators over access to front-end data would likely persist, or intensify, even with trade secrets protection. Thus, extending trade secrets protection to most "semi-public" data compilations will fail to bring the benefits of promoting business efficiency while exacerbating public interest concerns around allowing platforms to invoke a strong, intellectual property-like cause of action to sanction data scraping. Given such associated costs, it is doubtful that extending trade secret protection would yield a cost-beneficial outcome.

To summarize, this Article argues that opening the door of trade secret law to most "semi-public" data compilations is likely not an efficient approach. The "not readily ascertainable" requirement for "semi-public" business models is

---

[242] 925 F.2d 174 (7th Cir. 1991).

conceptually distinct from that applicable to trade secrets shared only with a limited number of parties. When front-end data is accessible to the public by design, there is little ability to impose effective non-disclosure agreements or clauses to restrict further dissemination of front-end data. When the focus necessarily shifts to regulating access to such front-end data, it becomes unclear how many restrictions would be sufficient, or whether any set of measures could effectively prevent data scraping. Two potential outcomes follow: (1) the arms race at the front-end is not alleviated but intensified, leading to inefficiencies; or (2) most "semi-public" data compilations fail to meet the standard, rendering trade secrets protection inapplicable.

This Article contends that the better approach is not to follow the *Compulife* standard, but instead to clarify that trade secret law does not apply to business models that allow public access to front-end data. The only business models that might still enjoy trade secrets protection are the extreme scenarios discussed at the beginning of this section—namely, those that maintain highly private front-end data accessible only to a limited number of users in a restricted manner.[243] The business models of most other organizations—such as social media platforms, online shopping platforms, and airlines—require them to allow as many users as possible to access their front-end data.[244] Thus, trade secret law is not a useful path for them.

But these businesses are not without legal remedies. They already have several alternative causes of action against data scrapers, including CFAA claims, trespass to chattels, and breach of contract.[245] *Compulife* centered on trade secret claims, likely because there were no valid access restrictions in place and no conditional access based on agreement to terms of service.[246] When more conventional claims have failed, courts should not adopt a paternalistic approach by opening the door to a rarer and significantly stronger

---

[243] *See supra* notes 182–187 and accompanying text.

[244] The importance of network effects for platforms is well established in the current literature. *See What Are Network Effects?*, HARV. BUS. SCH. ONLINE (Nov. 12, 2020), https://online.hbs.edu/blog/post/what-are-network-effects [https://perma.cc/E693-ZE77] (providing a general introduction to the concept of network effects); Venkatesh Shankar & Barry L. Bayus, *Network Effects and Competition: An Empirical Analysis of the Home Video Game Industry*, 24 STRATEGIC MGMT. J. 375 (2003) (arguing that network effects are strategic resources).

[245] *See* Liu, *supra* note 6, at 32; Benjamin L.W. Sobel, *A New Common Law of Web Scraping*, 25 LEWIS & CLARK L. REV. 147, 151 (2021).

[246] *See* Toren (Part I), *supra* note 149; Sprankling, *supra* note 8, at 213.

cause of action, especially as it may deter scraping activities pursued for publicly beneficial purposes.[247]

B. Data Scraping, Improper Means to Acquire, and Reverse Engineering

At this stage, an important and related question remains unanswered: whether using data scraping technology to scrape front-end data is equivalent to acquiring trade secrets through improper means—particularly when there are technical access restrictions and term of service preventing data scraping. This issue warrants a closer examination because it bears on the earlier discussion of the "not readily ascertainable" analysis, which presumes that the means used to ascertain a trade secret are proper.[248] Further, trade secrets liability is contingent upon a finding of misappropriation, which entails either the use or disclosure of trade secrets in breach of confidence, or the acquisition of trade secrets through improper means.[249] Scraping publicly accessible front-end data and recompiling it into the back-end compilation potentially implicates acquisition by improper means.[250]

Typical examples of acquisition by improper means are articulated in the current law and include offenses such as theft, bribery, misrepresentation, and electronic intrusion.[251] Front-end data scraping can be best categorized as a form of electronic intrusion. A classic example of electronic intrusion is *Physicians Interactive v. Lathian Sys., Inc.*, where the defendant used technology to hack into a computer system and take proprietary information.[252] Accordingly, use of scraping technology to directly hack into a platform where the back-end data compilations are stored would be a clear situation of acquiring information through improper means. For example, in a Chinese case involving the microblogging site Weibo, the defendant scraped back-end data,

---

[247] *See* Elkin-Koren, Perel & Somech, *supra* note 3, at 1483.

[248] *See supra* note 212 and accompanying text.

[249] *See supra* note 50 and accompanying text.

[250] For most "semi-public" data compilations, breach of confidence is generally not an issue, as users accessing only front-end data are typically not bound by any confidentiality agreements. The business models underlying these platforms dictate that front-end data is meant to be accessible to and shareable by the public, effectively negating the core premise of a duty of confidence. Moreover, users are even less likely to bear any confidentiality obligations regarding the back-end data compilation, as they never receive access to it in the first place.

[251] *See supra* note 50 and accompanying text.

[252] Physicians Interactive v. Lathian Sys., Inc., No. CA 03-1193-A, 2003 WL 23018270, at *8 (E.D. Va. Dec. 5, 2003); *see* Toren (Part II), *supra* note 149.

some of which was not even accessible at the front-end, by directly intruding into the back-end system.[253] This was undoubtedly misappropriation by improper means. *UAB "Planner5D"* is another typical example.[254]

However, data scraping only at the front-end is distinguishable from directly intruding into computer systems.[255] Scraping and recombining front-end data to form the back-end data compilation is conceptually more similar to legitimate reverse engineering. The definition of reverse engineering is roughly understood to be the process of working backward to extract know-how or knowledge from the product.[256] Reverse engineering can be complete or partial, for competitive or non-competitive purposes, and potentially immune from liability.[257] As discussed by Hrdy, using strategic prompting—namely, extensively querying a publicly accessible generative AI model to obtain its responses to infer its overall architecture, understand how it works, and acquire some of its training data—is within the definition of reverse engineering.[258] By analogy, using automated technology to query or send requests to platforms and scrape front-end data is akin to the AI model extraction and likely reverse engineering.[259] Platform products with front-end data access can be viewed as publicly available products that are open to view and study. Accessing, collecting, and recompiling front-end data to recreate the back-end compilation is arguably comparable to working backward to extract the underlying database that supports the consumer-facing platform products and their data retrieval functions.

Regardless of how conceptually similar front-end data scraping is to reverse engineering, *Compulife* seems to suggest that automation or use of advanced techniques to acquire information may be deemed improper in some circumstances, even where the platform permits basic user access and the

---

[253] Hunan Yifang Ruanjian Gufen Youxian Gongsi Yu Beijing Weimeng Chuangke Wangluo Jishu Youxian Gongsi (湖南蚁坊软件股份有限公司与北京微梦创科网络技术有限公司) [Hunan Yifang Software Co. v. Beijing Weimeng Chuangke Network Tech. Co.], (2019) Beijing Intell. Prop. Ct. Civ. Final Judgment No. 3789 (Beijing Intell. Prop. Ct. Feb. 2, 2021) (China).

[254] *See supra* notes 151–153 and accompanying text.

[255] *See* Toren (Part II), *supra* note 149.

[256] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974); Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1577 (2002).

[257] *See* Hrdy, *supra* note 51, at 109–10.

[258] *See id*. at 111–14.

[259] This assumes that courts would not consider any use of new automation of AI techniques to be improper as the *Compulife* court did. *See id.* at 138; *see infra* Part III for discussions on *Compulife*'s problematic standards on improper means to acquire.

defendant circumvented no technical access controls.[260] The Eleventh Circuit reached this conclusion by citing a famous case in trade secret law—*E. I. Du Pont de Nemours & Co. v. Christopher*—where the Fifth Circuit Court held that using an aerial vehicle to fly over a construction site to discover information was improper under the circumstances.[261] This case opened the door for courts to hold some behaviors improper depending on the facts, even if they are lawful under other laws and regulations.[262] However, directly applying *Christopher* in the context of front-end data scraping is flawed.

First, although *Christopher* is a landmark case cited frequently by scholars, it is infrequently followed by courts, partly because it adopts an overly loose standard for improper means.[263] Adopting a standard premised mainly on the protection of undefined "commercial ethics" overlooks an increasingly recognized goal of modern trade secret law—balancing primary and cumulative innovations.[264] As Sprankling notes, *Christopher* is slightly obsolete, in that it reflects the traditional policy aim of safeguarding commercial morality without accounting for the innovation effect.[265] It is not good policy to render front-end data scraping as improper by simply following *Christopher* as the *Compulife* courts did.[266]

Second, there appears to be an implicit assumption backing *Christopher*'s ruling: aerial photography was not reasonably foreseeable under technological norms at the time.[267] As technology evolved, and aerial photography became increasingly common and accessible to the public, norms may have changed such that *Christopher* would be decided differently today.[268] The same applies to front-end data scraping. The technology is not only evolving but is also becoming increasingly accessible to the public.[269] Companies are raising objections to others scraping their platform data, but many are themselves

---

[260] *See id*. at 115–16.

[261] 431 F.2d 1012 (5th Cir. 1970).

[262] Comments to the UTSA cite *Christopher* for the proposition that otherwise lawful conduct can be improper under the circumstances. *See* UTSA, *supra* note 43, § 1 cmt.; *See also supra* note 50 and accompanying text.

[263] *See* Toren (Part II), *supra* note 149; Sprankling, *supra* note 8, at 212.

[264] *See* Chen, *supra* note 33, at 170–72; Hrdy, *supra* note 51, at 110.

[265] Sprankling, *supra* note 8, at 214.

[266] *See* Hrdy, *supra* note 51, at 132–33.

[267] E.I. Du Pont de Nemours & Co. v. Christopher, 431 F.2d 1012, 1015 (5th Cir. 1970).

[268] *See* Sprankling, *supra* note 8, at 214.

[269] *See* Leonardo Rodriguez, *14 Best Web Scraping Tools in 2025 (Pros, Cons, Pricing)*, SCRAPERAPI BLOG (May 5, 2025), https://www.scraperapi.com/web-scraping/tools/ [https://perma.cc/2HLM-ERW9]; Lanfang Fei, *A Comparative Study on Public Interest Considerations in Data Scraping Disputes*, 20 INT'L J.L. IN CONTEXT 568, 570 (2024).

engaging in data scraping activities, particularly in the AI context.[270] It is questionable to easily consider data scraping as improper means against any widely accepted business ethics in itself.

When front-end data scraping targets not a completely public platform like in *Compulife*, but a platform with some technical restrictions on accessing and collecting front-end data, the issue becomes more complicated. Restrictions that merely slow access rather than truly blocking it do not appreciably change our prior analysis. As argued by Kerr, when platforms are open to all, restrictions—such as using cookies to record prior visits and prompt paywalls, blocking suspicious IP addresses, and using technical checks like CAPTCHA to test human behaviors—mostly function as speed bumps rather than real barriers to access.[271] Such platforms remain public in nature; the mere imposition of access speed restrictions does not transform them into private spaces where access is truly limited.[272] Circumventing these limitations does not, by itself, render the act of scraping improper, as the process still involves collecting publicly available information—albeit through automated bots that facilitate access. As noted in *Sandvig v. Sessions*, by its nature, scraping public websites without access restrictions "is merely a technological advance that makes information collection easier; it is not meaningfully different from using a tape recorder instead of taking written notes, or using the panorama function on a smartphone instead of taking a series of photos from different positions."[273]

When platforms maintain some form of genuine authentication, such as requiring login credentials, the analysis becomes even more muddied. Kerr distinguishes access speed restrictions from authentication, describing the latter as a real barrier to access.[274] If data scraping directly bypasses authentication—by, for instance, stealing others' credentials or directly circumventing technical restrictions—it is likely to be improper.[275] Suppose, however, that there is no direct bypass of authentication. Instead, scrapers access the platforms by automatically creating multiple accounts, such as in

---

[270] *See* ORG. FOR ECON. COOP. & DEV., INTELLECTUAL PROPERTY ISSUES IN ARTIFICIAL INTELLIGENCE TRAINED ON SCRAPED DATA 1, 20 (OECD Publ'g Feb. 2025), https://doi.org/10.1787/d5241a23-en (noting that technology companies and platform operators are both sources of scraped data and regularly scrape data themselves).

[271] *See* Kerr, *supra* note 205, at 1163–70.

[272] *See id.* at 1163–64.

[273] Sandvig v. Sessions, 315 F. Supp. 3d 1, 16 (D.D.C. 2018); Fei, *supra* note 269, at 570.

[274] *See* Kerr, *supra* note 205, at 1171.

[275] *See id.*; Sobel, *supra* note 245, at 173.

Ates, or obtaining consent from legitimate users to use their credentials, as in *Facebook v. Power Ventures*.[276] At first glance, access to the front-end data is authorized without bypassing authentication or any technical access barrier.[277] Considering this just as improper as directly bypassing behavior is not intuitively correct. Kerr acknowledges that the norms of the open web might, in some scenarios, condone behaviors that fall short of directly circumventing authentication, such as password sharing or reopening accounts after cancellations.[278]

From a normative perspective, trade secret law should not treat this behavior as improper means, as this may result in most platforms over-implementing and over-enforcing password protection, even for free accounts, in their venture to establish liability for scrapers. The effect would be an extreme outcome parallel to that resulting from adopting the lowest threshold for the "not readily ascertainable" standard: nearly all "semi-public" data compilations could qualify for trade secret protection, regardless of the extent to which their front-end data is publicly accessible[279] All back-end compilations would become "not readily ascertainable," as scraping from platforms with login requirements would constitute improper means, and manual collection without scraping technology would be prohibitively costly and impractical. At the same time, scraping and reproducing such compilations would amount to trade secret misappropriation. This extreme outcome would excessively favor data holders' interests over the public interest—particularly innovation, competition, and social benefits like scientific gains derived from scraping activities.[280] By leaving no room for permissible data scraping, such a legal rule could easily create information monopolies that harm data openness and entrench platform data lockouts. [281]

---

[276] 844 F.3d 1058, 1062 (9th Cir. 2016) (finding that the defendant had obtained user consent to access Facebook accounts via passwords).

[277] *See* Jamie L. Williams, *Automation Is Not "Hacking": Why Courts Must Reject Attempts to Use the CFAA as an Anti-Competitive Sword*, 24 B.U. J. SCI. & TECH. L. 416, 425–26 (2018).

[278] *See* Kerr, *supra* note 205, at 1175–80.

[279] *See supra* notes 219–225 and accompanying text.

[280] *See supra* note 225 and accompanying text.

[281] *See*, *e.g.*, David M. Adler, *Let the Bots Be Bots: Why the CFAA Must Be Clarified to Prevent the Selective Banning of Automated Access to Public Information*, 16 BROOK. J. CORP. FIN. & COM. L. 279, 295 (2021); *see generally* Ioannis Drivas, *Liability for Data Scraping Prohibitions Under the Refusal to Deal Doctrine: An Incremental Step Toward More Robust Sherman Act Enforcement*, 86 U. CHI. L. REV. 1901 (2019) (arguing that monopolists' ability to restrict data scraping poses a grave and novel threat to competition and should be regulated by the antitrust laws).

Unlike creating automated accounts or using others' accounts to access and scrape front-end data, scraping publicly available data without login restrictions may breach terms of service. Sprankling argues that scraping publicly accessible front-end data in violation of explicit clauses that prohibits such data scraping constitutes improper means.[282] This Article disagrees. As illustrated earlier, scraping publicly available front-end data is more akin to reverse engineering, an inherently legitimate behavior under trade secret law. Terms of use that prohibit data scraping essentially function as anti-reverse engineering clauses. The enforceability of anti-reverse engineering clauses has long received consistent attention from scholars.[283] As argued in another article, at least in some situations concerning software reverse engineering, these clauses should not be enforced even under contract law.[284] However, whether breaching these clauses can incur contractual liability remains uncertain across the United States, China, and the EU.[285]

Despite the potential for contractual liability, this Article argues that data scraping in breach of anti-reverse engineering clauses should not, by itself, be deemed so improper as to trigger trade secrets liability. Courts have adopted conflicting interpretations of whether reverse engineering in breach of contract can give rise to trade secrets liability, but the precedential value of these cases is limited.[286] In trade secret law, there is much stronger support for the legitimacy of reverse engineering. As the U.S. Supreme Court discussed in *Kewanee Oil Co. v. Bicron Corp.*[287] and *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*,[288] allowing reverse engineering is a key feature distinguishing trade secret law from patent law. It ensures competition and is an essential part of innovation.[289] In the words of Samuelson and Scotchmer, "if the intellectual property regime is well designed in the first place, we see no intrinsic reason why contracting should be allowed to circumvent it, especially in markets with

---

[282] *See* Sprankling, *supra* note 8, at 213.

[283] *See, e.g.*, Hrdy, *supra* note 51, at 133–47; Chen, *supra* note 51, at 797–812; Samuelson & Scotchmer, *supra* note 256, at 1626–30; Peter Henderson & Mark A. Lemley, *The Mirage of Artificial Intelligence Terms of Use Restrictions*, 100 IND. L.J. 1327, 1359–61 (2025).

[284] *See* Chen, *supra* note 51, at 811–17.

[285] *See id.* at 801–17; *see, e.g.*, Samuelson & Scotchmer, *supra* note 256, at 1626–30 (discussing the contractual liability imposed by anti-reverse engineering clauses and whether they can be preempted by copyright law).

[286] *See* Hrdy, *supra* note 51, at 138–42 (primarily discussing California cases).

[287] 416 U.S. 470, 489–490 (1974).

[288] 489 U.S. 141, 160–162 (1989).

[289] *See* Hrdy, *supra* note 51, at 159.

strong network effects."[290] Trade secret law has its own policy levers to maintain the balance between private and public interests.[291] Scraping front-end data to form "semi-public" data compilations typically happens in sectors with significant network effects that depend on maximizing user participation and public accessibility. Allowing anti-reverse engineering clauses to override the reverse engineering doctrine would undermine the doctrinal equilibrium intended by the law.[292] Trade secret law has already faced criticism for lacking sufficiently effective limits to preserve public interest, and trade secret overclaiming is a growing problem that merits new policy levers to curb such overreach.[293] Allowing platforms to invoke anti-reverse engineering clauses in order to leverage trade secret law against data scrapers—exposing them to property-like remedies such as injunctions and damages exceeding actual losses—would exacerbate the overclaiming problem.[294] Such an approach is unlikely to yield efficient outcomes that balance platforms' interests and the public interest in permitting data scraping.

C. No Trade Secrets Protection—Then What?

This Article concludes that most "semi-public" data compilations should remain unprotected by trade secret law. This leaves two further and equally important questions: should these compilations receive any legal protections? If so, what kind? It is beyond the scope of this Article to fully address these issues, but this Subpart offers several preliminary insights that may help direct future research.

---

[290] Samuelson & Scotchmer, *supra* note 256, at 1660.

[291] *See* Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401, 1408–12, 1420–38 (2014).

[292] *See* Hrdy, *supra* note 51, at 155 (characterizing reverse engineering as a well-established and important legal doctrine that limits the reach of trade secret law); Samuelson & Scotchmer, *supra* note 256, at 1583.

[293] *See generally* Camilla A. Hrdy & Christopher B. Seaman, *Beyond Trade Secrecy: Confidentiality Agreements That Act Like Noncompetes*, 133 YALE L.J. 669 (2024) (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); Varadarajan, *supra* note 291 (arguing that current trade secret law lacks an effective limiting doctrine and proposing the introduction of a fair use doctrine to address that issue); Fishman & Varadarajan, *supra* note 41 (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 (2019) (arguing that the law defines "infringing use" too broadly and proposing a narrower version).

[294] *See* Hrdy, *supra* note 51, at 82.

In contemplating grant of legal protection, it is worth reconsidering the fundamental rationale for protecting "semi-public" data compilations. China currently applies the AUCL to afford intellectual property-like protection. Some jurisdictions are actively debating the need for new legislation for data compilations.[295] Any move toward creating a new legal right or recognizing de facto property interests must be grounded in a robust law-and-economics analysis and supported by empirical evidence. This Article is skeptical that granting data holders property-like rights would lead to benefits that outweigh costs of such protection.

A more prudent approach could be to rely on existing legal causes of action to offer indirect protection by regulating front-end data scraping behavior. If scraping clearly circumvents access restrictions or disrupts the platform's functionality, scrapers can be liable under statutes that penalize unauthorized access. Where scraping violates accepted and enforceable terms of service, contractual liability may follow. The contract law framework may also produce more efficient results. When breach of contract is the sole consequence, potential scrapers may opt for an "efficient breach," compensating data holders while also advancing social welfare through the beneficial use of data.[296]

The foregoing analysis does not negate liability for data scraping when it infringes upon the rights of third parties—especially the privacy and personal information of platform users.[297] Where the legal conditions are met, users may directly sue data scrapers to safeguard their privacy and personal information interests. Direct regulations, such as the GDPR, might also be invoked to protect corresponding interests.

V. CONCLUSION

This Article has explored how trade secret law can continue to function within the data economy. Doctrinally, trade secret law appears resilient enough to protect data secrets—ranging from private data products to data compilations—even when some components are publicly available, so long as the combination itself remains secret. A positive examination of law and practice in the United States, China, and the EU affirms this doctrinal possibility. The Article has highlighted the growing and continuous recognition of trade secret law as protecting private data and data compilations. While *Compulife*

---

[295] *See supra* Part II.
[296] *See* Hrdy, *supra* note 51, at 161–62; Zou & Chen, *supra* note 53, at 383–84.
[297] *See* Fei, *supra* note 269, at 570–71.

appears to suggest that trade secret law can protect "semi-public" data compilations, a review of factually analogous cases paints a different picture. Except for a few extreme cases in which access to front-end data is heavily restricted to a limited number of users, trade secret law is rarely invoked in scenarios where front-end data is broadly accessible to the public.

This Article has examined why trade secret law remains underutilized for "semi-public" data compilations, and whether it should be extended further. The problem lies in the ambiguity surrounding the "not readily ascertainable" standard required for trade secrets protection. In traditional trade secret contexts, owners deliberately restrict access to all parts of the trade secret, and reasonable measures required to maintain secrecy are generally well-established. In the data economy, however, business models often require open access to front-end data for customer use. Under such circumstances, it becomes unclear what types or degree of restrictions to front-end access is sufficient to render the back-end compilations not readily ascertainable. This Article has argued that *Compulife* adopts an overly lenient interpretation of this standard, one that lacks doctrinal support within current trade secret law and risks extending trade secret protection to nearly any compilation built from publicly accessible front-end data.

The "not readily ascertainable" standard undeniably requires some form of access restriction. However, without clarity on this standard, holders of "semi-public" data compilations cannot be assured their data will be protected unless they adopt additional technical measures to prevent increasingly sophisticated data scraping. Ironically, the mere possibility of trade secret protection might incentivize data holders to adopt even more aggressive anti-scraping measures, escalating the arms race between platforms and data collectors—an inefficient outcome that trade secret law was designed to avoid. Thus, expanding trade secret law to encompass most "semi-public" data compilations fails to serve the doctrine's policy objectives. This Article argues for a high threshold under the "not readily ascertainable" standard, whereby trade secret law should protect only those "semi-public" data compilations where access to front-end data is restricted to a limited user base. The more common business models that deliberately permit wide access to front-end data should fall outside the domain of trade secret law.

Data scraping implicates another key element of trade secret misappropriation: acquisition by improper means. This Article has argued that scraping publicly available front-end data is more analogous to legitimate reverse engineering than to improper acquisition under trade secret law. The

existence of technical restrictions that merely impede access—without outright denying it—does not warrant recharacterizing scraping as improper. However, authentication requirements may introduce greater culpability. Directly circumventing authentication protections may constitute improper means under trade secret law, but merely creating automated accounts or using third-party credentials to access and recompile front-end data might not meet that threshold. Interpreting such actions as improper would render virtually all data scraping activities subject to trade secret liability—an outcome akin to the problems created by a lenient "not readily ascertainable" standard that fails to strike a reasonable balance between private property and public interests. Allowing terms of service that prohibit scraping to turn such conduct into improper means is functionally equivalent to allowing anti-reverse engineering clauses to create trade secret liability. Given the strong policy rationale in favor of preserving the right to reverse engineer, permitting platforms—especially those benefiting from network effects—to use contract law to circumvent this policy lever threatens the balance struck by the doctrine, and would likely lead to inefficiencies. This approach would also exacerbate the already pressing issue of trade secret overclaiming.

In sum, trade secret law is not applicable to most "semi-public" compilations. Its protections only extend as intended in the data economy—namely, to private data and compilations, as well as "semi-public" compilations whose front-end access is meaningfully restricted to a limited number of users, as in *DHI* or "Business Advisor." Trade secret law also cannot be used to sanction data scraping activities that do not involve intrusion into a data holder's system or direct circumvention of genuine access restrictions. In light of these limitations, it becomes imperative for future research to investigate whether, and under what alternative legal frameworks, these compilations should be protected.