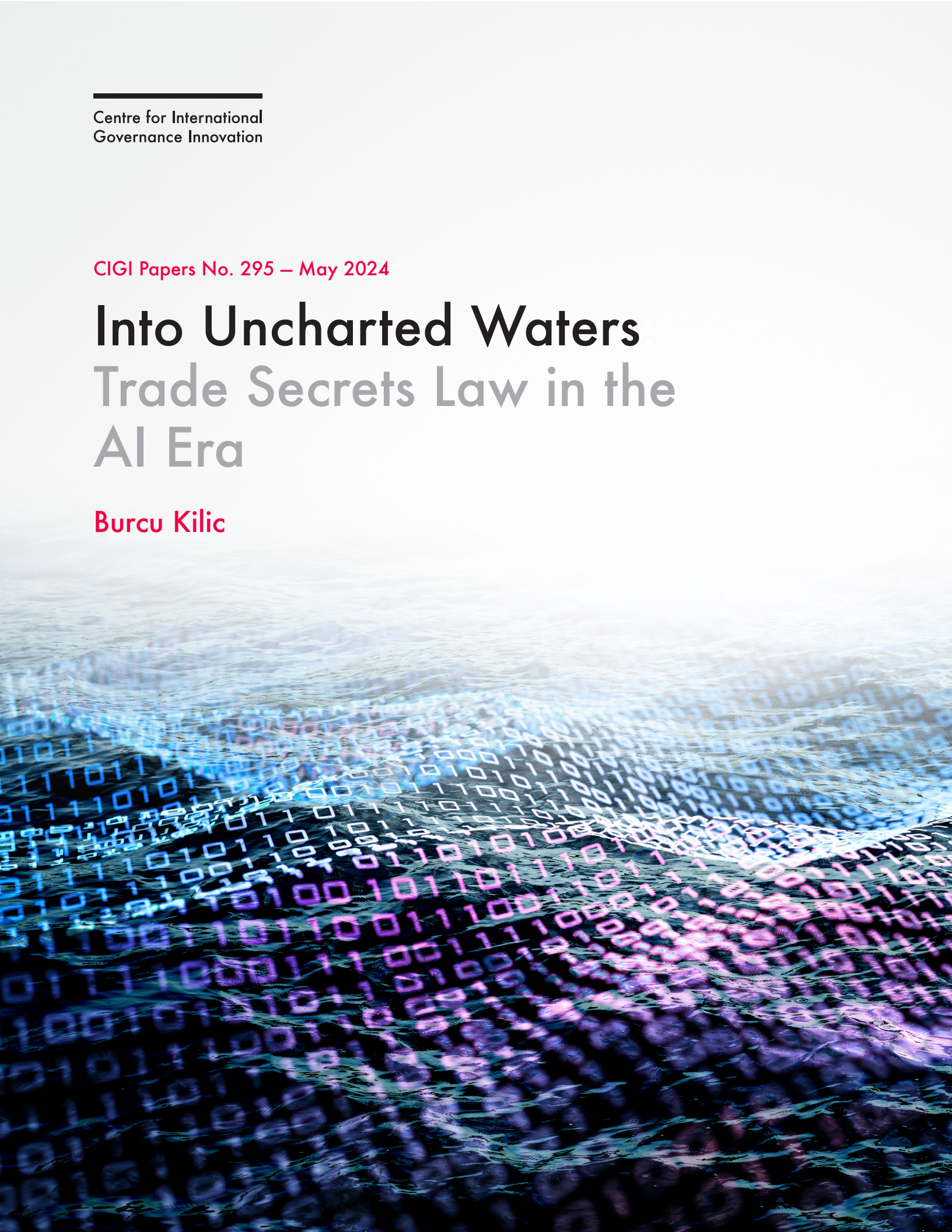
Centre for International
Governance Innovation

CIGI Papers No. 295 — May 2024

Into Uncharted Waters
Trade Secrets Law in the AI Era

Burcu Kilic



Centre for International
Governance Innovation

CIGI Papers No. 295 — May 2024

Into Uncharted Waters
Trade Secrets Law in the AI Era

Burcu Kilic

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director of Digital Economy (until February 2024) Robert Fay
Director, Program Management Dianna English
Program Manager Jenny Thiel
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Sami Chouhdary

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Burcu Kilic is a CIGI senior fellow, and a scholar, tech policy expert and digital rights advocate. She has worked with a diverse range of organizations across civil society, philanthropy and academia. Her research and writings cover digital rights, intellectual property (IP), innovation and trade, and she has provided technical advice and assistance in countries in Asia, Latin America, Europe and Africa.

As the former head of policy of Frontier Technology — a Minderoo Foundation initiative — Burcu guided the organization's approach to emerging technology, advocating for responsible, equitable and just solutions.

Before joining Minderoo, she directed the Digital Rights Program at Public Citizen, a non-profit consumer advocacy organization in Washington, DC, and also led their research on access to medicines. Her influence in tech policy, IP and trade underscores her commitment to policy entrepreneurship and rights-based advocacy. She champions collaborative civil society engagement, policy entrepreneurship and innovative policy development on a global scale. In 2015, she was recognized as one of the 300 Women Leaders in Global Health for her work on health and trade policy. From 2021 to 2022, she was a practitioner fellow with the Digital Civil Society Lab at the Stanford Center on Philanthropy and Civil Society.

She completed her Ph.D. at Queen Mary University of London and holds L.L.M. degrees in IP law from Queen Mary University of London, and information technology law from Stockholm University. She obtained her law degree from Ankara University, Türkiye.

Acronyms and Abbreviations

ACLU	American Civil Liberties Union
AI	artificial intelligence
CBP	Customs and Border Protection
DHS	Department of Health Services
DTSA	Defend Trade Secrets Act
EEA	Economic Espionage Act
EPA	Environmental Protection Agency
FDCA	Federal Food, Drug, and Cosmetic Act
FIFRA	Federal Insecticide, Fungicide, and Rodenticide Act
GDPR	General Data Protection Regulation
IP	intellectual property
IPRs	intellectual property rights
LLMs	large language models
MDA	Massachusetts Disclosure Act
PRA	Public Records Act
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UTSA	Uniform Trade Secrets Act
WTO	World Trade Organization

Executive Summary

As artificial intelligence (AI) rapidly evolves and integrates into our lives, discussions around transparency and accountability in AI systems become increasingly crucial. A critical yet often overlooked aspect of these discussions is the protection of trade secrets. There is a delicate balance between safeguarding proprietary rights and fostering an environment where AI can be scrutinized for fairness, bias and societal impact.

The crux of the issue lies in the legal ambiguity of trade secrets protection across jurisdictions. In the United States, trade secrets are considered intellectual property rights (IPRs), but the European Union does not provide them an exclusive IP protection. In international law, unlike the detailed provisions for patents and copyrights, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)[1] lacks a clear protection and exception framework for trade secrets, leading to diverse interpretations and practices around the world.

Exploring the legal uncertainties surrounding trade secrets, this paper demonstrates how expansive protection impedes the drive for transparency and accountability in AI. It argues that the current legal framework overly protects trade secrets in AI technologies, applying proprietary protection to source code, algorithms, training materials and data sets, thus creating barriers to accessing information essential for the public interest, including health, safety and policy development.

Addressing this challenge requires a rethinking of trade secrets law to establish clear limits and exceptions similar to those in other domains of IPRs. This paper contributes to the debate on AI by providing legal insights and suggesting reforms to balance proprietary rights with the need for transparency. It advocates for a legal reform incorporating public interest exceptions within trade secrets protection. Such reform would not only align with broader societal needs but also support innovation by ensuring that AI technologies are developed and deployed in an ethical and accountable manner.

Introduction

Rarely does a day pass without news, op-eds, reports or events centred on AI. Its widespread influence has led to a mix of excitement and significant concerns. The companies behind these technologies paint a grim picture of the future, while continuing to develop new tools, technologies and policy initiatives. AI now touches upon every policy area, from labour and global health to nutrition, finance and more. The landscape is filled with regulatory initiatives, global forums and policy proposals driven by tech giants and their allies, along with new government mandates and task forces. The rush to engage with AI is widespread, with experts from all sectors eager to contribute to the conversation.

With critical discussions on AI policy, regulation and infrastructure gaining momentum, there is growing agreement on the need for transparency and accountability in AI systems. These concepts have evolved beyond simple buzzwords and are now crucial for thoughtful and advanced policy dialogue. However, this raises several questions: For whom is transparency beneficial, and how can we ensure accountability? What are the necessary tools, systems and measures?

A significant but often neglected aspect of these discussions is the role of trade secrets. The foundational elements of AI systems, such as source code, algorithms, data sets and training manuals, are often protected as trade secrets. This poses a complex challenge at the crossroads of technology, proprietary rights and policy discussions shaping the AI landscape.

Trade secrets have a vague status in legal systems, varying greatly from one jurisdiction to another. In the United States, trade secrets are treated as a form of IPRs, while in contrast, the European legal systems do not recognize trade secrets as an exclusive IPR. The lack of legal consistency is primarily because there is no international consensus on the issue. Unlike patents and copyright, which are clearly defined under the TRIPS Agreement, trade secrets are not thoroughly regulated in international law, leading to a wide range of interpretations and applications in different legal systems.

1 WTO, *Agreement on Trade-Related Aspects of Intellectual Property Rights (unamended), Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization*, 15 April 1994, 1867 UNTS 154, 33 ILM 1144 (1994) (entered into force 1 January 1995) [*TRIPS Agreement*], online: WTO <www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm>.

The legal ambiguity surrounding trade secrets poses considerable challenges to AI policy development, particularly for initiatives aimed at enhancing transparency and accountability. Trade secrets are increasingly being used as a counterargument against requests for disclosure, access, data sharing and due process.

Discussions on AI governance often only lightly touch on or entirely sidestep trade secrets. Recently, it has become simpler to assert trade secrets protection claims but more challenging to dispute them, leading to overly broad protection of data, data sets, training materials, source code and algorithms. The lack of scrutiny of trade secrets, combined with a reluctance to discuss their limitations, impedes progress toward achieving transparency, accountability, regulation and innovation in AI. There is a clear need for more in-depth discussions and actionable solutions, as trade secrets currently lack defined boundaries, flexibilities and exceptions that are typical of other IP rights.

A growing body of literature discusses the challenges posed by the protection of trade secrets, creating barriers to accessing data and information crucial to the public interest, such as details about pharmaceuticals and vaccines, criminal justice and surveillance technologies, and environmental hazards. This trend toward greater secrecy conflicts directly with crucial public interests, including accountability, public safety and policy. This paper aims to synthesize key insights from this body of work by focusing on the legal aspects of trade secrets. It sets out to be the legal voice in the room, examining the often overlooked yet crucial world of trade secrets. It explores how trade secrecy can hinder access to vital information necessary for testing and evaluating AI technologies, particularly in identifying biases and discrimination, thereby impeding public policies and initiatives aimed at transparency and accountability. The goal is to provide legal clarity and direction in conversations on AI, focusing on this essential but frequently overlooked aspect.

If AI policy is a complex puzzle we aim to solve, then trade secrets represent a cornerstone piece. Without addressing this key element, our puzzle remains incomplete, missing a critical dimension.

The History of Trade Secrets

The origins of trade secrets law can be traced back to Roman law (Yenerall 2021), but its modern formulation was developed by the Anglo-American legal system. The courts in England and the United States first recognized a cause of action for damages based on the misappropriation of trade secrets in the nineteenth century (Lemley 2008).

The Anglo-American doctrine of trade secrets incorporates a series of related common law torts, such as breach of confidence, breach of confidential relationship, common law misappropriation, unfair competition, unjust enrichment, and torts pertaining to trespass or unauthorized access to a plaintiff's property (ibid.).

However, this modern concept of trade secrets is less firmly established in non-common-law countries. Its foundation rests on various legal theories, such as contract, property, fiduciary relationships and unjust enrichment (Czapracka 2012).

The question of whether trade secrets can be treated as property rights, akin to copyrights, patents or trademarks, remains unresolved. Civil law jurisdictions have traditionally shown reluctance to recognize trade secrets as IP rights.[2] This illustrates a key distinction in legal perspectives between common law and civil law systems.

In civil law systems, the protection of property rights, including intangible assets, is acknowledged as a fundamental right. Central to this protection is the *numerus clausus*[3] doctrine. This doctrine establishes that the number, nature, creation, transfer and termination of real rights are limited (and closed). As such, property rights as absolute rights are set using strictly defined parameters. They offer protection only for categories that are explicitly recognized and governed by law (ibid.). The doctrine does not allow for the autonomous

2 "Given that trade secrets are not a form of exclusive intellectual property right"; see https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/trade-secrets_en.

3 Directly translated from Latin, this term means "the number is closed." See Merrill and Smith (2000, 4).

creation of property rights through contractual agreements; such rights can only emerge as expressly outlined by law (Akkermans 2016).

This principle extends to the main forms of IP — patents, copyrights and trademarks — categorizing them as a finite set of primary exclusive rights over legally recognized intangible assets. The *numerus clausus* approach not only specifies the available classes of these rights but also curtails the influence of contracts in determining the "movable boundaries of private property" (Correa 1997, 131–32).

Moreover, under civil law, trade secrets are often categorized uniquely as "de facto assets," "incomplete intellectual property rights" or "subjective rights" (known as "*subjektive Rechte*" in German and "*droit subjectif*" in French) (Czapracka 2012). Unlike other forms of IPRs, trade secrets occupy a somewhat ambiguous position, highlighting the complexity and diversity inherent in the property rights framework of civil law systems.

The Paris Convention

The Paris Convention for the Protection of Industrial Property (Paris Convention)[4] was one of the first multilateral treaties protecting intellectual property (IP). The Paris Convention applies to industrial property in the widest sense, including patents, trademarks, industrial designs and unfair competition. Notably, the convention does not explicitly mention trade secrets; instead, it addresses them within the context of unfair competition.

Article 10*bis* is a key provision within the Paris Convention, mandating that member countries offer robust protection against unfair competition. Unfair competition is defined as any act of competition "contrary to honest practices in industrial or commercial matters."[5] Article 10*bis* (3) describes three categories of cases that must be prohibited:

- **Acts likely to cause confusion:** This refers to any activity that may "create confusion by any means whatever with the establishment, the goods, or the industrial or commercial activities, of a competitor."
- **False allegations:** This category includes statements or allegations that can discredit a competitor's establishment, goods, or industrial or commercial activities.
- **Misleading indications:** This involves any indications or allegations that could deceive the public, particularly regarding "the nature, the manufacturing process, the characteristics, the suitability for their purpose, or the quantity, of the goods."

According to European legal traditions, the protection of trade secrets is fundamentally linked to unfair competition law. Civil law systems typically categorize the misappropriation of trade secrets as an act of unfair competition embedded within a broad protective framework. Consequently, continental European jurisdictions have traditionally seen no need for a separate standard for trade secrets protection, considering them well protected through a combination of unfair competition, contract, torts, employment and criminal law (Czapracka 2012). In 2016, the European Parliament adopted the European Trade Secrets Directive, which came into force in 2018.[6] This directive harmonizes how member states handle trade secrets, aiming to provide owners with increased protection and uniformity. It also provides exceptions to the enforcement of trade secrets law, such as instances in which the disclosure of a trade secret serves the purpose of whistle-blowing or protecting a legitimate interest recognized by the European Union or national law (Durkin et al. 2021).[7]

From the US perspective, categorizing the misappropriation of trade secrets as an act of unfair competition presented legal complexities. In

4 *Paris Convention for the Protection of Industrial Property*, 20 March 1883 (entered into force 7 July 1884, as amended on 28 September 1979), online: WIPO <www.wipo.int/wipolex/en/text/288514#P213_35515>.

5 *Ibid*, art 10*bis* (2).

6 *Directive (EU) 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] OJ, L 157/1.

7 *Ibid*.

the United States, unfair competition is primarily understood as the "passing off" of one's goods or services as those of a competitor. This definition did not offer the level of protection sought by US industries (Sandeen 2010). Over time, the rationale and objectives of US trade secrets law have significantly evolved, moving away from a focus on unfair competition and ethical business practices toward an "IP" framework: "Trade secrets are best understood, not as applications or extensions of existing common law principles (warranted or unwarranted), but as IP rights" (Lemley 2008, 25). In addition:

> Understanding trade secrets as IP rights allows them to take their proper place in the pantheon of social policy designed to encourage innovation. It also gives us a way to think about how those rights are designed, a way that has significant implications for how trade secret law looks and how it interacts with other laws. Most surprisingly, those implications are ones that offer greater, not lesser, latitude for competitors and departing employees than the unfair competition rationale most commonly articulated as an alternative. (ibid., 56)[8]

The TRIPS Agreement

The introduction of the TRIPS Agreement on January 1, 1995, marked a significant shift in the history of IPRs. The agreement emerged during the final stages of the Uruguay Round of the World Trade Organization (WTO) negotiations. TRIPS started a new era for IPRs by incorporating them into the global trading system.

Since 1995, TRIPS has been instrumental in shaping global IP policies and practices. It provides a detailed framework addressing various IP issues, including specific rules for IP enforcement and a binding dispute resolution process. Importantly, it also establishes minimum protection standards for IPRs that all WTO members are obliged to follow.

Throughout the TRIPS negotiations, intense debates arose over whether article 10*bis* required member countries to protect trade secrets. The position of each country largely depended on the strength of their laws against unfair competition. The United States, for example, led the group, arguing that article 10*bis* did not require the protection of trade secrets under unfair competition laws. For the United States, it was crucial to explicitly recognize trade secrets as a property right within TRIPS. The US negotiators aimed to ensure extensive protection in countries where the concept of misappropriation was not widely recognized.

Ultimately, the US efforts did not prevail (Nashkova 2023). Article 39 of the TRIPS Agreement only mentions "undisclosed information" and deliberately avoids its characterization as property. Instead, the drafters anchored the legal treatment of undisclosed information within the framework of unfair competition law, as outlined by article 10bis of the Paris Convention. Further emphasizing this approach, article 39 is built on the principles of unfair competition rules. Under this framework, data originators are entitled to prevent third parties from using their data only if such data has been acquired through dishonest commercial practices (United Nations Conference on Trade and Development-International Centre for Trade and Sustainable Development 2005).

Article 39 of the TRIPS Agreement only mentions undisclosed information, deliberately avoiding the categorization of this information as IP (see Box 1). The drafters of article 39 strategically placed the legal handling of "undisclosed information" under the purview of unfair competition law, as governed by article 10bis of the Paris Convention. The explicit mention of article 10bis of the Paris Convention in the TRIPS Agreement indicates the drafters' intention to clarify that the obligations under article 39 do not add to but rather develop those already contained in the Paris Convention. Article 39 does not establish a new form of IPR, contrary to the initial proposal by the United States during the early negotiation phases. The sole obligation imposed on member states is to offer remedies in instances where dishonest commercial practices occur (Correa 2007).

8 See Lemley (2008, 2), suggesting that "trade secrets can be justified as a form, not of traditional property, but of *intellectual* property" (emphasis in original).

Box 1: Protection of Undisclosed Information*

1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect *undisclosed information in accordance with paragraph 2* and data submitted to governments or governmental agencies in accordance with paragraph 3.

2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:

(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) has commercial value because it is secret; and

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.

**TRIPS Agreement, supra* note 1, s 7, art 39, online: WIPO <www.wipo.int/wipolex/en/text/305907> (emphasis added by author).

While the TRIPS Agreement includes trade secrets within its scope of IP forms, it does not mandate a specific theoretical framework for their protection. Article 1.2 of TRIPS categorizes undisclosed information as part of IP. Although such information is commonly referred to as "trade secrets" or "know-how," article 39 of the TRIPS Agreement neither uses these terms nor provides a definition for undisclosed information. In fact, the drafters intentionally refrained from using the term "trade secret" to ensure that the protection of undisclosed information in TRIPS did not align with or specifically require the adoption of a US-style trade secrets law. This deliberate choice aimed to avoid association with any particular legal system (Gervais 2008).

Article 39.1 clarifies that effective protection from unfair competition includes protection of undisclosed information and limits the protection of undisclosed information specifically "against unfair competition as provided in Article 10*bis* of the Paris Convention." This approach to protecting undisclosed information under the concept of unfair competition does not create exclusive rights, nor does it establish undisclosed information as a separate category of IP.

According to Carlos Correa (2007), the terminology used in article 39 of the TRIPS Agreement appears to confirm the non-proprietary nature of protection. In contrast to the sections on patents and trademarks, article 39 does not mention the "owner" of undisclosed information. This distinction suggests that control over such information does not equate with ownership or property rights (ibid.).

Article 39.2 of the TRIPS Agreement establishes the criterion that information must be met to be considered undisclosed. It must be secret (i.e., it is not generally known among, or readily accessible to, circles that normally deal with the kind of information in question), possess a commercial value, and be subject to reasonable steps —

under the circumstances — to be kept secret (for example, through confidentiality agreements). It also requires countries to create a private right of action for the holders of that information to initiate an action against those who exploit the information without consent in "a manner contrary to honest commercial practices." The agreement further clarifies, in a footnote, that it refers to "at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition."[9]

In contrast, article 39.3 requires member countries to actively ensure protection against unfair competition, focusing on the specific type of undisclosed information that governments require. It specifically addresses certain test data and other submissions necessary for marketing pharmaceuticals or agricultural chemical products that utilize new chemical entities and sets forth additional requirements for the protection of that information by governments under the Paris Convention article 10*bis*. The application and scope of article 39.3 have been subject to intense debate over the past decade, which falls outside the scope of this paper. However, it is crucial to note that even article 39.3's requirement for direct action against unfair competition does not confer exclusivity akin to other IPRs.

Notably, article 39 of TRIPS does not create an exclusive right over undisclosed information and hence provides no specific exceptions or limitations. The silence of the article underscores the drafters' intent of not being overly prescriptive about the protection of undisclosed information and leaving considerable policy space for member states. This flexibility allows them to tailor the protection of undisclosed information to their legal systems, whether in the form of exclusivity or protection against unfair competition, according to their respective legal systems.

At its core, TRIPS seeks to strike a balance between public access to information and technology and the rights of creators to secure returns on their investments. This balance is crucial in the context of trade to prevent distortions within the system. For TRIPS to remain an effective instrument for international public policy, it is essential that this balance between potentially competing interests be appropriately maintained (Kilic 2014). The objectives outlined in article 7[10] and the principles laid out in article 8[11] are critical for interpreting and implementing the rights, obligations and exceptions under the agreement. These provisions, reaffirmed by the Doha Declaration on the TRIPS Agreement and Public Health,[12] reiterate that TRIPS should be regarded as a means to achieve public policy objectives through the promotion of innovation and access to its results.

Article 8 is particularly significant because it establishes a basis for broader exceptions than those in article 7. It guides member states to adopt measures that serve the public interest in sectors crucial to their socio-economic and technological development. This clearly affirms that member states maintain the power and responsibility to protect and promote the public interest (Durkin et al. 2021). In addition, this approach provides them with the flexibility to introduce limitations or exceptions to article 39. This flexibility is applicable whether article 39 is interpreted broadly as encompassing trade secrets or in accordance with the specific language of the provision, focusing on protection against unfair competition.

Having established that the global standards of IP rules under TRIPS allow for flexibility and policy space in creating limitations and exceptions, the conversation naturally shifts to the tools available to governments to introduce exceptions and limitations for overly broad trade secrets protection, especially around AI technologies. The key question is whether governments have

9 *TRIPS Agreement, supra* note 1, art 39.2.10, n 22.

10 *Ibid*, art 7 ("The protection and enforcement of intellectual property rights should contribute to the promotion of technological innovation and to the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations.")

11 *Ibid*, art 8 (1. "Members may, in formulating or amending their laws and regulations, adopt measures necessary to protect public health and nutrition, and to promote the public interest in sectors of vital importance to their socio-economic and technological development, provided that such measures are consistent with the provisions of this Agreement. 2. Appropriate measures, provided that they are consistent with the provisions of this Agreement, may be needed to prevent the abuse of intellectual property rights by right holders or the resort to practices which unreasonably restrain trade or adversely affect the international transfer of technology.")

12 WTO, Ministerial Conference, *Declaration on the TRIPS Agreement and Public Health*, 14 November 2001, WTO Doc WT/MIN(01)/DEC/2, online: WTO <www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_trips_e.htm>.

the appetite and political will to do so. Given that many leading AI companies, both large and small players, are US-based, it is crucial to examine US law in this context. Trade secrecy is not a recent tech industry innovation; it has been a strategic tool for various industries — from pharmaceuticals to tobacco and chemicals to software — over the last 50 years. Lessons from these sectors are crucial for providing informed discussion on how to balance often-competing commercial interests in extensive trade secrecy with the public's need for access to and right to information to effectively manage risks and avoid harms.

To fully grasp the current landscape, it is crucial to understand how US law became a trade secret maximalist, leading to the emergence of "trade secret thickets" in various industries. The next part of the analysis will explore the shift where commercial interests in trade secrets began to overshadow public interests, including health, safety and well-being. This paper provides insights into the tactics and legal arguments employed by companies in the realm of trade secrets.

Trade Secrets Protection in US Law

The history of US trade secrets law presents an interesting contrast to that of other IPRs. While patents and copyright have their legal foundations clearly established in the Constitution and implementing federal statutes, trade secrets law has developed from common law and has been codified individually in most states. This highlights a contrasting philosophy: copyright and patent laws are granted to incentivize the creation and dissemination of new ideas, expressions and inventions, whereas trade secrets law focuses on protecting secrecy for competitive gain (Risch 2008).

The Federal Food, Drug, and Cosmetic Act (FDCA), enacted in 1938, first included provisions related to the non-disclosure of trade secrets. The FDCA explicitly prohibits government employees from disclosing commercial information, including trade secrets, provided by companies during the approval process.[13]

Another key foundation of trade secrets law is found in the Restatement (First) of Torts, which described trade secrets as "a process or device for continuous use in the operation of the business."[14] Trade secrets are protected under tort law due to violations of "relationally specific duties." Importantly, it did not create a "right of property in the idea" (Durkin et al. 2021, 132).

In 1979, the Uniform Trade Secrets Act (UTSA)[15] was adopted to codify the fundamental principles of common law trade secrets protection prevalent across different states. To date, the UTSA has been adopted by almost every state (48 states) (Cole 2021), and it defines a trade secret as: "information, including a formula, pattern, compilation, program[,] device, method, technique, or process,[16] that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[17]

The UTSA extends the definition of trade secrets beyond the scope initially set in the Restatement (First) of Torts. It specifically defines "improper means" as including theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, and espionage, whether by electronic or other means.[18] It also details "misappropriation" as acquiring, disclosing or using a trade secret when knowing or having reason to know it was acquired through improper means.[19]

The UTSA has been instrumental in reshaping US trade secrets law. Building on the UTSA's definition, the scope of what constitutes a trade secret has been significantly broadened to include

13 *Federal Food, Drug, and Cosmetic Act*, 21 USC § 331(j).

14 *Restatement (First) of Torts* § 757 (1939).

15 *Uniform Trade Secrets Act with 1985 Amendments*, 9 August 1979, amended 8 August 1985.

16 *Ibid*, § 1(4).

17 *Ibid*, § 1(4)(i)–(ii).

18 *Ibid*, § 1(1).

19 *Ibid*, § 1(2).

any "information" that is secret, has commercial value and is safeguarded by reasonable efforts to ensure its secrecy. The "informationalization" of the law has significantly blurred the lines in determining what qualifies as a trade secret. It has become increasingly challenging to categorically assert that any particular piece of valuable data or information held by a commercial entity does not qualify as a trade secret (Kapczynski 2022).

On a similar timeline in 1984, the Supreme Court held that trade secrets were property rights and thus protected against confiscation under the US Constitution.[20] The case revolved around Monsanto's submission of health and safety data about pesticides to the Environmental Protection Agency (EPA), as required by the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA). The early versions of FIFRA did not specify whether the submitted data would be publicly disclosed. However, a 1972 amendment allowed companies to classify certain data as trade secrets, thereby limiting public disclosure and use by competitors. This regime changed again in 1978 when Congress allowed data exclusivity or compensation rights for submitters while also permitting the EPA to disclose data for health, safety and environmental purposes, and to use it for approving similar products by other companies. Monsanto contended that such disclosure constituted an unconstitutional "taking" of its trade secrets, in violation of the Fifth Amendment (ibid.).

The lower court agreed with Monsanto, ruling that the EPA's disclosure of scientific data collected under the FIFRA amounted to an unconstitutional seizure of private property (Peterson 1984). This decision hindered public access to health and environmental information and restricted efforts by public and environmental health groups to monitor and assess the safety of pesticides, and raised broader concerns about transparency and public safety. Thus, the case presented a significant legal question regarding the constitutional protection of trade secrets under the Fifth Amendment, specifically given Monsanto's argument that the disclosure of the company's data constituted an unconstitutional "taking" of property, a contention that warranted a Supreme Court review.

In a unanimous decision, the Supreme Court rejected Monsanto's argument that the disclosure of health and safety data related to pesticides amounted to an unconstitutional taking of private property.[21] However, in a significant legal development, the court explicitly recognized for the first time that trade secrets could be considered a protected property under the Fifth Amendment.[22] This meant that a government that improperly revealed a trade secret could be required to pay compensation. The decision also confirmed that the 1978 FIFRA amendments specifically authorized the public disclosure of all health, safety and environmental data, thereby impacting Monsanto's expectations regarding confidentiality.[23] Amy Kapczynski interprets the case as follows:

> *Monsanto* therefore stands as another key moment in the encasement of trade secret law: by embracing trade secrets as constitutional "property" and concluding that their disclosure to the public was — at least under some circumstances — subject to a form of regulatory takings analysis, the Court invited an extraordinary conflict between state law and basic practices of democratic statecraft that have been embedded in our law since at least the era of *laissez faire*. The most dire implications could have been forestalled by a careful reading of its limited holding. But perhaps unsurprisingly, given the spirit of the times into which the case was born, other lower courts have instead read the case as requiring the encasement of trade secret law from democratic prerogatives. (Kapczynski 2022, 1420)

The recognition of property rights in trade secrets has been the subject of considerable debate. Scholars argue that trade secrets law is not distinct; it is essentially a collection of various legal norms, including contract and fraud, unified solely by their application in protecting confidential information. Indeed, the relational aspect of trade secrets liability rules aligns more closely with contract law than with property law (Bone 1998). Consequently, some argue that establishing property rights in

20 *Ruckelshaus v Monsanto* Co, 467 US 986 (1984) [*Ruckelshaus*].

21 *Ibid*. In this decision, Justice Harry A. Blackmun noted, "As long as Monsanto is aware of the conditions under which the data are submitted, and the conditions are rationally related to a legitimate government interest, a voluntary submission of data in exchange for the economic advantages of a registration can hardly be called a taking."

22 *Ruckelshaus* (*supra* note 20).

23 *Ibid*.

trade secrets may be unnecessary, as other legal frameworks, such as contracts and tort law, already provide adequate tools to safeguard against the misappropriation of ideas. This perspective challenges the need for distinct trade secrets protection, suggesting that existing legal tools are sufficient to address concerns related to the protection of secret information (Simpson 2005).

Following the landmark *Ruckelshaus v. Monsanto* decision, the rise of trade secrets protection in US law continued with the enactment of the Economic Espionage Act (EEA) in 1996. This legislation, which came in the wake of heightened awareness and legal recognition of trade secrets post-*Monsanto*, significantly expanded the legal framework for trade secrets, strengthening the safeguards available to industry. It is specifically tailored to address foreign espionage, imposing criminal penalties for the theft of trade secrets that benefit foreign governments, their instrumentalities or agents.[24] Congress has shifted the foundation for trade secret misappropriation liability more firmly into the domain of property than ever before. The enhanced protections embedded in the law have created a powerful tool for industry, enabling it to exclude valuable discoveries from wider society (ibid.).

Designed to safeguard information that is valuable and creates a competitive advantage, derives its value from its secret nature and has been the subject of reasonable efforts to keep it secret, the EEA has a scope that is broader than that of the UTSA, encompassing a wider variety of technological and intangible information (Nashkova 2023, 645). It defines trade secrets as "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible." Nonetheless, determining what constitutes a trade secret remains highly fact specific, dependent on the nature of the information and the particulars of how its confidentiality is maintained.

The legislative history of the EEA has raised significant concerns. Notably, Congress did not consult any IP experts during the legislative process. There was no substantial discussion about how the EEA would interact with the trade secrets law's objective of promoting innovation for societal benefit. Instead, the committee reports and floor debates surrounding the EEA predominantly reflect a pro-business stance. The testimony that was heard came exclusively from industry experts, who naturally had self-interested perspectives (Simpson 2005). The EEA has received considerable criticism from scholars for its lack of balance and consideration of broader societal impacts (ibid.).

Building upon the foundation set by the EEA, the US Congress took another significant step in 2016 with the passage of the Defend Trade Secrets Act (DTSA). This act was the result of a multi-year effort to federalize trade secrets protection, marking a significant expansion of trade secrets law. It established a federal private cause of action for cases involving the misappropriation of trade secrets, further solidifying the legal framework in this area, but it did not pre-empt state trade secrets law.[25]

In response to concerns about the potential conflict between trade secrets protection and public interest in accessing information, the DTSA incorporated whistle-blower protections, granting immunity to whistle-blowers who confidentially share information while reporting illegal activities to law enforcement or in the context of a legal suit, provided that their disclosures are made under seal. These whistle-blower protections are designed to strike a critical balance between maintaining the confidentiality of trade secrets and ensuring transparency and accountability, particularly in sensitive areas such as health, safety, civil rights, financial markets, consumer rights and environmental protection (Katyal and Graves 2021).

In conclusion, while the DTSA does provide some safeguards, they are far from being comprehensive or satisfactory. This aspect of the DTSA underscores its intent to protect trade secrets, but it also highlights the need for a stronger focus on public oversight and the enforcement of various laws that safeguard the broader interests of the public.

24 18 USC § 1831 – *Economic espionage*.

25 18 USC § 1838 – *Construction with other laws*.

Trade Secret Dilemma: At the Crossroads of Secrecy and Transparency

Trade secrets protection, broadened and strengthened through the decisions of US courts, presents a significant yet often overlooked challenge, potentially undermining access to information and various civil rights and protections. A core issue is the overly broad application of trade secret claims. The determination of what exactly constitutes a trade secret often relies significantly on the expertise and creativity of corporate legal counsel. This leads to an expansive interpretation, stretching the traditional boundaries of what is considered a trade secret. It is likely that a significant portion of IP related to AI is being protected as trade secrets in the United States, contributing to the broad application (Quinn Emanuel Trial Lawyers 2020). Often, information labelled as proprietary fails to satisfy the established legal criteria for trade secrets protection. This becomes particularly critical when the public interest demands a certain level of transparency, even in instances involving legitimate trade secrets.

Trade secret disputes increasingly involve not only direct competitors but also third parties, extending beyond the scope originally intended by trade secrets law. This expansion of trade secrets to cover basic services and publicly available information illustrates how trade secrets law can be strategically used or "weaponized" for the purpose of concealing information (Katyal and Graves 2021). This trend not only challenges the conventional understanding of trade secrets but also raises concerns about the implications of such practices for transparency, public access to information, and public health and safety.

For example, having access to the source code of software used for essential government services, such as benefit administration or understanding the inner workings of AI systems and their training data, is often vital for public policy and oversight. It underscores the need for a more equitable approach to trade secrets protection. While it may be important to safeguard proprietary information that meets the protection criteria, this should not come at the cost of concealing information that is crucial for public welfare and safety.

Trade secrets law has evolved to offer broad protection for what companies label as trade secrets, treating terms such as "secret," "proprietary" and "confidential" as synonyms for restricting access (Pooley 2022). This trend encourages extensive use of trade secret claims, often blocking disclosure demands and hindering public access and regulatory oversight.

This is not a new problem, yet it is frequently overlooked in the context of public policy debates. Various sectors, including pharmaceuticals, tobacco, software and chemicals, have encountered and continue to grapple with the trade secret problem. In numerous cases, civil liberties advocates, consumer groups, public health organizations, community leaders and individuals confront the expansive trade secret claims. Regrettably, courts have failed to support efforts to set limits on this kind of information secrecy.

This section aims to highlight the intimidating narrative constructed by companies around trade secrets, a narrative that demands immediate reflection and action. This is particularly urgent as emerging technologies such as AI increasingly influence our lives, shaping our future, rights and democracies. There are valuable insights to be gained from other sectors — insights that can inform discussions on potential future directions and reforms in trade secrets law.

In the years following the *Monsanto* decision, courts often interpreted trade secrets broadly, expanding the limits of trade secrets protection, especially in matters of disclosure and access.

In the post-*Monsanto* legal landscape, one particularly troubling case is *Philip Morris, Inc., v. Reilly*.[26] This case originated from the Massachusetts Disclosure Act (MDA), requiring cigarette manufacturers seeking to sell their products in the state to disclose any tobacco additives. The law's intention was to reduce public health risks and foster research on the health effects of components such as additives and flavourings, which tobacco companies typically keep

26 *Philip Morris, Inc v Reilly*, 312 F (3d) 24 (1st Cir 2002) [*Philip Morris*].

confidential.[27] Despite its significant implications for public interest, this law was never implemented but instead resulted in prolonged litigation.

The court ultimately sided with Philip Morris, recognizing that the cigarette ingredients were both a trade secret and property. It recognized that the companies had legitimate investment-backed expectations and ruled that the mandatory disclosure of their secrets constituted an unconstitutional taking of their property under the Fifth Amendment. While acknowledging the public interest in disclosure, the court expressed concerns[28] about the law's perceived lenient standards for disclosure, which stipulated that information could be released if it "could" benefit public health. This, the court feared, could result in significant private loss in the event of disclosure.[29]

The court was convinced that the tobacco companies had a property interest in their trade secrets. It viewed the MDA as transforming "private property into public property without compensation," constituting a clear violation of the Fifth Amendment's takings clause.[30]

In the ongoing struggle between the government's authority to regulate the common good and the property interests of companies, there is a growing concern that the balance may have shifted away from the public interest. The Philip Morris case provides an insightful but disconcerting perspective, suggesting that private property rights, especially those concerning trade secrets, have taken precedence over broader public health considerations and public interest.

This expansion has turned trade secrets protection into a significant legal hurdle, especially evident in legislative efforts addressing public interest policies on access, safety and health.

Fracking chemicals, linked to serious health risks, including cancer and neurological disorders, illustrate the tension between trade secrets and public interest (Kapczynski 2022). Despite the clear health implications of these chemicals, companies can claim them as trade secrets, often with minimal justification, merely by ticking a box. This practice, supported by the fossil fuel lobby, limits public access to crucial information about the chemicals contaminating groundwater.[31]

Despite growing concerns, the industry continues to lobby the EPA to claim trade secrets protection by asserting that "[h]ydraulic fracturing is a highly complex and competitive industry where trade secrets are critical assets" (Zink 2018, 1162). Consequently, public access to detailed information about these chemicals remains limited. Even in incidents of likely water contamination, companies such as Halliburton have managed to keep the list of chemicals used confidential (Kapczynski 2022).

While state regulators might know these chemicals, their ability to share this information is restricted, limiting access for researchers and the public. State-level regulatory bodies, where fracking oversight primarily occurs, frequently face resource constraints that limit their ability to provide extensive oversight (ibid.). This illustrates the impact of trade secrets protection claims on public health and safety, demonstrating the challenges in balancing corporate secrecy with the public's right to information in crucial health and environmental matters.[32]

From chemicals to cigarettes, trade secrets have frequently been utilized by corporations to restrict public access and disclosure, even in areas crucial to public health and safety that are regulated and subject to public oversight. This raises significant concerns about emerging technologies such as AI, where public oversight is minimal, and underscores the need to rethink trade secrets protection to ensure it does not obstruct public access to information.

27 US, *Massachusetts Disclosure Act: Massachusetts General Laws*, 1996, c 94, § 307B.

28 *Philip Morris, supra* note 26 at 32 ("For a state to be able to completely destroy valuable trade secrets, it should be required to show more than a possible beneficial effect").

29 *Ibid*. The court reasoned that "specific laws simply cannot destroy property interests."

30 *Ibid*.

31 "For instance, in Texas, after that state adopted a disclosure law, between April 2011 and December of 2012, fracking companies claimed trade secret or proprietary protection 10,120 times in reporting related to 12,140 instances of fracking. An investigation by the Obama-era DOE [Department of Energy] in 2014 came to a similar conclusion: trade secrets were being invoked 84% of the time" (Fink 2019, 1002).

32 *Ibid*.

Trade Secrets in the Automation Era

The responsibility for managing and operating public infrastructure and services, which traditionally lay with the government, is increasingly being transferred to private companies in the United States. In delivering essential services such as telecommunications, Medicare, Medicaid and welfare programs, these private companies adhere to commercial law standards and practices, including trade secrecy as a crucial tool (Levine 2011).

Automated decision making, be it via software or AI systems, suffers from a lack of transparency, enabling corporate dominance in public spheres, reducing transparency and accountability, and undermining public expectations of due process. This issue has been at the centre of countless cases, varying in facts, parties and years, but the underlying narrative remains consistent. When individuals challenge these automated decisions, they frequently receive the response that the systems or algorithms are protected as trade secrets, preventing government officials from disclosing the algorithms or source code. Often, those adversely affected by these decisions are from poor, marginalized and/or minority communities. They may find ways to bring their cases to court, either through class action lawsuits or with the help of pro bono lawyers, but then face resistance from companies that claim the algorithms are trade secrets, hence resisting disclosure.

When courts eventually compel disclosure and experts review the systems, it frequently becomes evident that the algorithms or systems are biased, lack critical data points or employ a one-size-fits-all approach that is unsuitable for the intended services. This pattern underscores the significant impact of automated decision-making systems on public welfare and the pressing need for greater transparency and accountability in their deployment and operation.

To provide a concrete example, in Idaho, the state implemented a new AI program in 2011 to determine budget allocations for Medicaid's homecare services. Individuals with developmental and intellectual disabilities who depended on the Medicaid program began noticing reductions in their homecare hours, typically between 20 and 30 percent (Stanley 2017). Under this program, beneficiaries were required to visit a medical assessment centre where an assessment provider would complete a proprietary form. This form detailed each individual's need for assistance in daily activities such as feeding, toileting and dressing (Brown et al. 2020). The data from this form was then manually entered into a digital budget tool, essentially an Excel spreadsheet, which then calculated a dollar amount for the assessed needs based on a proprietary database. This amount represented the annual budget for their services.[33] However, when beneficiaries questioned how these dollar amounts were determined and the rationale behind these cuts, especially since their disabilities and needs had not changed, the response from the Medicaid program was obstructive. Officials stated that the details of the calculation could not be disclosed because they were protected as trade secrets, thereby leaving recipients in the dark about the specifics of their service budget calculations.

The American Civil Liberties Union (ACLU) stepped in, representing 4,000 Idaho residents in a lawsuit demanding the disclosure of the formulations and assessment tools. The court sided with the ACLU, ruling that it was a violation of due process to reduce someone's health-care services by US$20,000 annually without a transparent explanation and relying on "black box" systems (Stanley 2017). Once the ACLU obtained the algorithms, it was revealed that the state had developed the formulas in-house, without proper validation, standardization or auditing. An expert review of these formulas revealed significant issues with both the data and the modelling. During the trial, trade secrets emerged as a point of controversy, especially when a third-party vendor that developed one of the assessment tools sought to restrict access to its assessment booklets, invoking trade secrets protection (ACLU 2023).

The court concluded that the department's formulas and assessments were so unreliable that they deprived people of their Medicaid budgets arbitrarily, violating the due process rights

33 "We asked a federal court to order the Department to disclose its system. Within a few weeks of filing suit, we got that order. Then we got the system. It was a set of formulas in a fairly basic Microsoft Excel spreadsheet. The Department's assessors enter annual assessment results into a copy of the spreadsheet for each person. The spreadsheet, in hidden cells, computes the person's budget amount" (ACLU 2023).

guaranteed by the Constitution. Ultimately, the court ordered a complete overhaul of the system.[34]

Despite being one of the most enlightening legal challenges against a black box system, it took the ACLU extensive effort — months of work, three experts and more than US$40,000 — to deconstruct and critique the system and an additional 2,000 hours of attorney and paralegal work to secure a settlement following the court's decision (ibid.). Trade secrets litigation is not only costly but also time-consuming, often stretching over years. For individuals without significant resources or support from organizations such as the ACLU, challenging these automated decisions becomes extremely difficult, highlighting a significant barrier to justice and accountability.

This pivotal case dates back to 2016, and one might have expected its lessons to guide the Idaho Department of Health and Welfare, which administers the Medicaid program, in its future practices. Unfortunately, it seems those lessons were overlooked. According to the ACLU of Idaho, the department introduced a new system created by a third-party vendor and once more used trade secrets to limit transparency and due process. As a result, people with developmental disabilities and their advocates are blocked from checking the system's manual for any biases, mistakes or other problems (ibid.). The Idaho department's actions reflect a broader trend among public agencies: the procurement of AI systems shrouded in trade secrecy in crucial public welfare systems, a practice that contributes to widespread confusion and harms beneficiaries.

Similarly, in Arkansas, the Department of Health Services (DHS) replaced nurse evaluations for homecare services with an algorithmic system. The rationale was that computers would be less expensive and less biased than nurses (Lecher 2018), who previously conducted comprehensive assessments using a 286-question form to determine a person's weekly homecare needs. However, once implemented, this new system produced arbitrary and illogical results (Citron and Calo 2021).

For example, the algorithm classified a foot amputee as having "no foot problems," ignoring the increased need for assistance due to amputation. Key individual details and continence history were overlooked, and the severity of conditions was not differentiated despite regulations requiring such distinctions (Lecher 2018). "Algorithmic absurdities" in automated decision making become evident in decisions such as the one where an algorithm allocated the same level of care to a person with quadriplegia, dementia or schizophrenia as it did to someone with only quadriplegia, blatantly ignoring the additional care needs associated with dementia and schizophrenia (Citron and Calo 2021).

In 2016, Legal Aid of Arkansas filed a lawsuit against DHS on behalf of physically disabled residents in Arkansas whose homecare was reduced by an average of 43 percent following the implementation of this algorithmic system. In extreme cases, aid was cut by more than 56 percent. The system left many severely disabled individuals without access to essential needs such as food, toileting and medicine for extended periods (De Liban 2017).

The lawsuit, which led to an injunction preventing DHS from using the automated system until it could justify its decisions, eventually resulted in a ruling that the state had failed to follow its own rulemaking procedures, including not providing adequate notice to those affected by the new methodology.[35] This case in Arkansas underscores the far-reaching consequences of relying on automated systems without oversight, particularly when critical public welfare services are involved.

In an encouraging development, a recent Federal Circuit decision from July 2023 may have far-reaching implications for those aiming to challenge the use of AI on due process grounds (Coglianese 2023). A recent Federal Circuit case, not directly related to AI but addressing the conflict between due process and trade secrets, ruled that trade secrets protection must yield to due process.[36] The dispute involved a company importing pencils purportedly manufactured in the Philippines. US Customs and Border Protection (CBP) contended that the importer violated trade rules by transshipping pencils from China through the Philippines to avoid anti-dumping duties assessed on pencils of Chinese origin. The importer protested that its due process rights

34 *K. W. v Armstrong*, 180 F Supp (3d) 703 (D Idaho 2016); see also *K. W. v Armstrong*, 789 F (3d) 962 (9th Cir 2015).

35 *Ark. Dep't of Human Servs. v Ledgerwood*, 530 SW (3d) 336, 340 (2017).

36 *Royal Brush Manufacturing, Inc v United States*, 75 F (4th) 1250 (Fed Cir 2023).

were violated because CBP did not grant access to confidential photos and business data from the Philippine manufacturer. This information was critical as it demonstrated the Philippine manufacturer's inability to produce the volume of pencils imported to the United States. CBP maintained it could not disclose this information due to confidentiality obligations (ibid.).

The Circuit Court rejected the government's argument, stating that the due process clause of the Constitution mandates that parties affected by government decisions have the right to view the evidence against them. This constitutional mandate takes precedence over statutory prohibitions on disclosing trade secrets. The court noted, "Because the Constitution authorizes, and indeed requires, the release of confidential business information in this case, the Trade Secrets Act does not stand in the way of such release" (ibid.). It held that CBP could have shared the confidential business information under a protective order, preventing further disclosure (ibid.).

Cary Coglianese (2023) suggests that this ruling opens a new avenue for legal challenges to agencies' AI applications, facilitating access to crucial information about the algorithms. This is particularly relevant when these algorithms are developed and deployed by private contractors claiming trade secrets protection (ibid.). This interpretation indicates a significant (and ideally lasting) shift in balancing trade secrets protections with due process considerations, especially regarding AI technologies employed by government agencies.

AI and Trade Secrets: Hidden Barriers

In his Senate testimony, Richard Eppink, legal director of the ACLU of Idaho, shed light on why the *K. W. v. Armstrong* case has become a significant reference point in discussions about AI systems. The case is referenced in the White House's October 2022 Blueprint for an AI Bill of Rights[37] and featured prominently in civil and human rights scholarship articles. Eppink highlighted that the case is particularly instructive because it vividly demonstrates the various ways automated decision-making systems can fail. The case implications are profound, especially considering the simplicity of Idaho's system. The fact that simple Excel spreadsheet formulas could give rise to a multitude of constitutional issues underscores the urgent need for robust governance to safeguard against potential problems in today's more advanced AI systems (ACLU 2023).

This concern, as articulated by Eppink, who has spent years challenging these systems to protect the most vulnerable, is crucial. The insights from all these cases demonstrate how trade secrets can create barriers to access and due process, highlighting the importance of challenging "trade secret thickets" that companies have woven around various types of data aggregation. These thickets can include an array of data aggregated on the source and processing of toxic waste; details about water and energy consumption, which Google required for constructing an innovative data hub in North Carolina; and information held by ride-sharing companies such as Uber and Lyft regarding the zip codes of their pick-ups and drop-offs (Fia 2022).

Nonetheless, they also shed light on the overwhelming challenges involved — the extensive time, effort and financial resources required to bring these systems to court and challenge trade secrets protection. These factors further complicate the pursuit of transparency and due process, making this a lengthy and costly endeavour.

This reality should fundamentally inform and shape our approach to AI governance and regulation. The shift from human to AI systems becomes particularly critical when AI systems take over tasks and make decisions once handled by humans, which are inherently accompanied by accountability mechanisms tailored for human oversight. This transition has led to a potential erosion of guarantees for transparency, accountability and due process. Unfortunately, accountability mechanisms and legal standards governing decision making have not evolved at the same pace as technological advancements (Kroll et al. 2017, 636). To address this, there is a pressing need for laws to adapt, aiming to reinstate the rights and values that were protected under the previous human-driven system. There have been proposals for legal and technical

37 See www.whitehouse.gov/ostp/ai-bill-of-rights/.

mechanisms to restore the status quo that existed before this shift (Citron and Calo 2021).

Since these suggestions were made in 2017, AI technologies have become more integrated into our lives, yet the fundamental problem remains unresolved. The increasing reliance of many government agencies on private companies for expertise and skills in AI systems has introduced a critical legal dilemma. Our legal frameworks and accountability standards continue to lag behind these rapidly advancing technologies.

When these companies assert trade secrets protection over their algorithms, training data, input parameters or any aggregated data, they effectively create a legal black box. This raises a critical question: Does the trade secrets protection claimed by these companies inevitably lead to the denial of due process rights for individuals or corporations (Coglianese 2023)? When the broadened and strengthened scope of trade secrets is factored into this equation, the problem becomes even more complex and opaque. This highlights the tension between proprietary protection in AI systems and the principles of transparency, accountability and the fundamental right to due process. A comprehensive and multifaceted response is needed that not only addresses the advancements in AI but also addresses the intricacies of trade secrets law.

In a landmark case from Seattle, Lyft and Uber (*Lyft, Inc. v. City of Seattle*) invoked the trade secret argument in an attempt to avoid submitting standardized quarterly reports to the city.[38] These reports included various data categories, such as the total number of rides and pick-up and drop-off zip codes. According to an agreement between the city, Lyft and Uber, the companies were obligated to provide these reports quarterly. However, Lyft's lawyers argued that the zip code reports constituted trade secrets under the UTSA and expressed concerns about confidentiality in transferring data to municipal authorities, despite the city's implementation of measures to safeguard the data.

The situation escalated in 2016 when an Austin-based ride-share analyst, under the Public Records Act (PRA), requested access to reports containing data from late 2015 to analyze evidence of redlining — to see if the companies were fairly serving communities of colour. The City of Seattle informed him that Lyft had claimed these reports were confidential, leading to legal action under the PRA for access to the reports (Gutman 2018). The King County Superior Court initially issued a permanent injunction, preventing the disclosure of these reports and agreeing with Lyft that the zip code reports were trade secrets under the UTSA (Monsees 2018).

However, the injunction decision was eventually overturned by the Washington Supreme Court, which granted access to the reports. The court ruled that the reports in question qualified as "public records" despite containing trade secrets. According to the court's decision, the disclosure of these records could be lawfully withheld only if it was determined that such disclosure "would clearly not be in the public interest and would substantially and irreparably damage a person or a vital government interest."[39]

The *Lyft* case provides crucial insights into the extent of trade secrets protection claims, or more accurately, the extent to which companies can assert trade secrets protection over data (Fia 2022). Despite the court's eventual ruling in favour of Seattle, the journey to that decision was lengthy, involving multiple courts, legal proceedings and significant legal costs, ultimately borne by taxpayers. For the City of Seattle, gaining access to data sets over which legal and contractual rights were established in a 2014 mediation agreement proved to be a resource-intensive endeavour. Despite their agreement to share data, both Lyft and Uber did not hesitate to assert trade secret claims over it. This case underscores the challenges posed by increasingly broad trade secrets protection, or claims thereof, and their far-reaching implications for data governance and public policy across various sectors, including transportation, labour and competition.

Since ChatGPT's launch in November 2022, large language models (LLMs) and generative AI have dominated AI discussions, catalyzing a broad industry-wide rush to adopt these advanced technologies. LLMs are revolutionizing how we live, work and conduct business with unprecedented speed. Yet they present several challenges, notably the risk of generating inaccurate, unreliable and, at times, hallucinated outputs. This issue stems

38 *Lyft, Inc v City of Seattle* 94026-6 (Wash Sup Ct 2018).

39 *Ibid*.

from the "garbage in, garbage out" principle, which is exacerbated by poorly labelled, inaccurate, biased or incomplete data sets (Awati, n.d.).

Most leading LLMs are developed by major tech companies such as Google, Meta, Microsoft and OpenAI. These companies typically prefer trade secrets protection over other IP rights for their LLMs, covering algorithms, training data, data sets and infrastructure as proprietary. This approach helps them preserve their competitive advantage without disclosing the specifics of their models to the public or to competitors. When required, they only disclose minimal details about the model architecture, training data and decision-making processes.

The secrecy surrounding the development of LLMs leads to opacity in their operation, significantly obstructing efforts to scrutinize these systems for biases, errors or ethical issues. It becomes challenging to ensure the safety of the data used in training or to identify inherent unfair biases within the models. As a result, the public is left with no choice but to trust companies' assurances, despite the fact that even the developers themselves may lack complete insights into how their models function. While they may understand the models' basic architecture, the complex behaviours that emerge from these models are often beyond clear explanation (Ramlochan 2023).

This is not a new challenge; it has deep roots within the tech industry. For instance, a 2021 internal memo from Facebook already highlighted engineers' concerns about their limited understanding and control over their systems (Zuboff 2022): "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' And yet, this is exactly what regulators expect us to do, increasing our risk of mistakes and misrepresentation" (Facebook Ad and Business Product Team 2021, 1; quoted in Zuboff 2022).

The emergence of LLMs such as GPT-4,[40] which are built on massive data sets, has only intensified this problem. Additionally, companies developing LLMs often refuse to disclose the sources of their training data, adding another layer of complexity. Given the high financial stakes, they favour trade secrets-protected, closed-source systems. However, the transparency offered by open-source projects not only enables the identification and resolution of vulnerabilities but also enhances the systems' quality through collaborative efforts within the community (Kreps 2024). A leaked internal Google document from May 2023 underscores this strategy, cautioning, "Keeping our technology secret was always a tenuous proposition" (Dickson 2023).

This scale and complexity of the models complicate not only the task of managing and overseeing but also understanding these advanced AI systems. Shielding AI systems — whether it is an algorithm or training data — as trade secrets tends to overly prioritize commercial interests, thereby creating barriers to due process. When algorithms or data sets are protected as trade secrets, there is an increased risk that they might reinforce existing biases and inequalities, leading to the emergence of a "techno-social divide." This divide essentially creates a barrier to accessing information, with profound implications for privacy, democracy, human rights, competition and social justice. It calls for continued efforts, comprehensive strategies and more rigorous legal frameworks to ensure that the deployment of AI systems does not compromise transparency, accountability or due process.

For better data governance, it is crucial to acknowledge and address the conflict between transparency, due process and trade secrets. Regulators and lawmakers must be aware of this inherent tension and incompatibility from the beginning. As they seek to balance the protection of trade secrets with the right to information access, the focus should be on the public's right to know. This perspective is key to ensuring transparency and accountability, thus keeping public interest at the core of discussions about the governance of AI technologies.

40 GPT-4 incorporates billions of text entries and operates with millions of parameters (Griffith 2023).

Public Interest Exceptions for Trade Secrets

Finding the Right Forum

IP protection has always been considered a form of public policy, with a balancing act between rights holders and the public interest at its core. However, the power dynamic inherent in the ability to own and control technological innovations has often led to IP serving as a tool of power and, when captured, a means for further consolidating it (Sell 2004). Today's IP standards, including trade secrets protections, have been largely shaped by the relatively small group of IP-intensive industries. These industries were able to recognize the value of IPRs early, shaping the laws in their best interest (Fia 2022).

Starting in the 1980s, US laws began to view IP protection more as a system of protection and exclusion rather than as a public policy instrument to encourage competition and diffusion. Global capitalism led by the United States exerted new pressure on the domestic landscape for IP protection (Sell 2004). The Supreme Court's recognition of trade secrets as property rights in 1984 and the post-*Monsanto* movement toward strengthening and broadening trade secrets should be viewed in this broader context.

Trade secrets protection has historically been closely intertwined with competitive and innovative progress, where the government has played a relatively modest role. However, the emergence of new technologies has amplified the need for robust safeguards in areas such as education, public health, civil rights, privacy, environmental protection and worker rights. The evolving technology landscape calls for greater government involvement and enhanced public oversight.

The current landscape is marked by extensive property rights and economic concentration in key industries, including technology. Trade secret protections that were once considered privileges have increasingly overshadowed the public policy obligations of the companies. As a result, the legal framework for trade secrets often falls short of delivering benefits to the public and protecting the public interest. This shift in perspective reflects a broader trend in IP law, highlighting the need for re-evaluating and potentially recalibrating the balance between private interests and the public good.

The concept of a public interest exception within trade secrets protection remains underdeveloped and inadequately explored. While briefly mentioned in the commentary to the UTSA and the Restatement (Third) of Unfair Competition, these references lack detailed explanation (Sandeen and Mylly 2021). Case law in this area is often confusing, with courts siding with companies and granting extensive protection to trade secrets (Levine 2011). This raises a crucial question: How can a clear and effective public interest exception for access and disclosure be integrated into trade secrets law and practice?

Looking at international law, key legal frameworks such as the Paris Convention and TRIPS do not explicitly address the exceptions for trade secrets. While the international IP regime may not directly provide the answers we seek, it does offer the flexibility and policy space necessary for incorporating public policy considerations into the evolving landscape of trade secrets protection. The policy space is crucial for aligning trade secrets protection with broader societal needs.

However, the emergence of trade secrets protection over source code and algorithms in recent free trade agreements raises significant concerns. Since the conclusion of the Trans-Pacific Partnership Agreement in 2015, there has been a notable trend in incorporating trade secrets protection within the e-commerce chapters of trade agreements. These provisions extend beyond TRIPS, establishing exclusivities over source code and algorithms with only minimal exceptions.

As technology advances, trade negotiators have started to recognize the limitations of these exceptions. Consequently, each subsequent trade agreement attempts to refine and make these exceptions applicable to the current state of technology. Yet as technology continuously evolves, these efforts consistently fall short. For instance, limited exceptions introduced in the United States-Mexico-Canada Agreement in 2018 are already outdated by the rapid advancements in generative AI and LLMs. This situation is reminiscent of the classic tale of the tortoise trying to catch up to the hare, where trade negotiators (the tortoise) consistently lag behind the technology (the hare).

The inclusion of extensive trade secrets protection in trade agreements merits a detailed separate review. For this discussion, it is important to note that trade agreements are not suitable forums for introducing public interest exceptions to address the growing challenges of extensive trade secrets protection. Instead, trade negotiators should be guided by domestic policies, incorporating exceptions established in national laws rather than dictating these standards internationally.

Domestic Pathways for Trade Secret Exceptions

Given the current trend toward recognizing trade secrets law as a form of IP, it logically follows that trade secrets should also encompass exceptions and limitations similar to those found in other IP domains. Developing these exceptions is essential for ensuring that trade secrets law balances the protection of commercial interests with the protection of broader public interest, particularly in contexts involving transparency, accountability and access to information.

Turning to US law, the challenge appears not to be a lack of familiarity among courts considering public interest in trade secret cases. Instead, the challenge lies in the absence of a structured framework or defined parameters within US law that explicitly outline the public interest considerations that should be factored into trade secret litigation. US law lacks a defined list of specific (although not necessarily exclusive) public interest issues that should be taken into account during trade secret litigation. The list may include concerns such as free speech and freedom of the press, free competition, employee mobility, regulatory oversight, the rights of collective organizations such as unions, and personal privacy interests (Sandeen and Mylly 2021).

For instance, the European Trade Secrets Directive,[41] enacted in 2016 and implemented into the laws of EU member states by 2018, presents a somewhat balanced approach to trade secrets protection. Unlike under US law, the directive does not establish such an exclusive property right over trade secrets. The recital of the directive explicitly states that it does not create any exclusive right.[42]

The directive's stance on trade secrets is somewhat ambivalent. It does not define trade secrets as either IP rights or as part of unfair competition law, although it tends more toward the latter (Aplin 2021). It is important to note that when the directive was introduced, the main lobbying industries were pharmaceuticals and chemicals (EDRi 2015), suggesting that considerations of the data economy or AI were not central to its formulation. However, its technology-neutral regime, which protects a wide array of know-how and business information, makes it a significant legal tool for today's data and AI economy (Fia 2022).

Rather than adopting an approach of broad rights with narrow exceptions, the directive seeks to establish a fair balance between rights and interests. It provides for exceptions to protection, placing the burden on the defendant to successfully establish these exceptions (ibid.). Article 5 of the directive lists these exceptions, aiming to balance the rights and interests of non-owners, such as small companies, consumers, researchers, journalists, public authorities and non-profit organizations. These exceptions include the right to freedom of expression and information; general public interest in revealing misconduct, wrongdoing and illegal activity; disclosure by workers and their representatives; and protection of legitimate interests recognized by EU or national law.

The interpretation of article 5 continues to be ambiguous. However, some suggest that within the framework of the General Data Protection Regulation (GDPR), the data subject's right to be informed might fall within the scope of this exception to trade secrets. As a result, the right to explanation cannot be denied on the grounds of safeguarding trade secrets (Mylly 2023). Likewise, if a direct link between the personal data and the algorithm can be established, the GDPR's transparency requirements could potentially supersede the trade secret claims of the companies (Foss-Solbrekk and Glenster 2022).

41 *Directive (EU) 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] OJ, L 157/1.

42 *Ibid*, recital 16 ("In the interest of innovation and to foster competition, the provisions of this Directive should not create any exclusive right to know-how or information protected as trade secrets").

This interpretation may open the door to greater transparency, ensuring that the protection of trade secrets does not override the individuals' right to understand the decisions made by or with the assistance of AI technologies.

The provision is interpreted as an "instruction to judicial authorities to Member States to interpret the existing provision in the light of Article 5" (Fia 2022; Aplin 2021). This allows for considerable flexibility in how member states implement the directive, which has arguably led to divergent paths of implementation, creating legal uncertainty in balancing trade secrets protection with public interest considerations (Aplin 2021).

However, when read in conjunction with recital 21, which explains the essential objectives pursued by the legislative act in EU law, this approach reinforces the fundamental rights and interests of non-owners and provides a set of tools for access and oversight (Fia 2022).

Although the directive strongly articulates the rights and interests of non-owners, it is anticipated that exceptions will likely become points of contention in national courts and the Court of Justice of the European Union (Aplin 2021). However, considering the relatively recent implementation of the directive, litigation related to trade secrecy and AI is still at an early stage (Fia 2022).

To the author's knowledge, there has been no specific judgment on this issue, and the legal landscape is still evolving. Future court decisions will be crucial in clarifying how the directive's provisions are to be interpreted and applied, particularly in cases involving extensive data sets. These forthcoming rulings will shape the balance between protecting trade secrets and ensuring access to large-scale data in the context of public interest and innovation.

The United States could potentially benefit from adopting an approach similar to Europe, which provides some guidance for handling trade secret claims and helps maintain a more equitable balance between protecting trade secrets and preserving public policy space.

Currently, in the United States, it falls on defendants to actively raise public interest issues in trade secret litigation. There have been notable cases where courts have given precedence to public interest arguments to limit or, in some instances, deny the protection of trade secrets. Such instances indicate a growing awareness and openness to balancing proprietary rights against broader societal values and public interests.

In fact, in her influential article about the public history of trade secrets, Kapczynski (2022) traces the evolution of trade secrets protection. She first examines the *Corn Products*[43] case from 1919, where the manufacturers challenged the state requirement to label the percentages of all ingredients in syrup. The Supreme Court ruled in favour of transparency and consumer knowledge over corporate secrecy. This case marked a significant shift toward the state's right to promote fair dealing.[44] Kapczynski then revisits a crucial case from 1937, *National Fertilizer Association v. Bradley*.[45] The case involved a legal challenge against South Carolina law, which mandated that the detailed ingredients of any fertilizer be clearly labelled and disclosed to the public. The petitioners claimed that such disclosure would compromise their core trade secrets and business interests, given their substantial investment of millions of dollars in developing these products. The case escalated to the Supreme Court, and the court unequivocally ruled that trade secret claims could not obstruct the disclosure of ingredients on labels. The ruling underscored the right of the state to exercise its police power and the public's right to fair dealing with corporate secrecy.[46]

Kapczynski suggests that these often overlooked cases (*Corn Products* and *National Fertilizer*) present an alternative vision for approaching trade secrets and their limits. She argues that they could have established a legal precedent, balancing corporate interests with democratic principles and the public's right to know. In her view, both cases provide a framework for more transparent

43 *Corn Products Refining Co v Eddy*, 249 US 427, 429–30 (1919).

44 *Ibid* at 431 ("It is too plain for argument that a manufacturer or vendor has no constitutional right to sell goods without giving to the purchaser fair information of what it is that is being sold....The right of a manufacturer to maintain secrecy as to his compounds and processes must be held subject to the right of the State, in the exercise of its police power and in promotion of fair dealing, to require that the nature of the product be fairly set forth").

45 *National Fertilizer Assn, Inc v Bradley*, 301 US 178 (1937).

46 *Ibid*, syllabus ("The right of a manufacturer to maintain secrecy as to his compounds and processes must be held subject to the right of the State, in the exercise of its police power and in promotion of fair dealing, to require that the nature of the product be fairly set forth").

and equitable handling of trade secrets, aligning legal practices with broader societal values:

> As the dangers of unregulated markets and the importance of public trust to market functioning began to be recognized, and the basic government construction of markets was also revealed, it was seen as utterly unproblematic to ask companies to reveal things about their products, with no need for elaborate justification — and certainly no constitutional problem — even in the face of trade secrecy claims. These cases have been forgotten, but remain good law. They help construct a through-line that is consistent not only with *Monsanto* (with a minor clarification), but that also makes sense read alongside contemporary First Amendment law, takings law and FOIA [Freedom of Information Act] law. (ibid.)

It is clear that we do not need to look far to find the basis for public interest exceptions for trade secrets protection. Drawing from the often overlooked but rich judicial history and legal foundations present in IP laws, there is ample opportunity to reform trade secrets law. Such reforms would not only align with the evolving landscape of technology but also provide a solid foundation for future AI regulations, ensuring they are crafted in a way that balances proprietary rights with the broader needs and rights of society.

Looking Forward

In our pursuit of ideal AI regulation, it is crucial to ask how trade secrets protection intersects with transparency and accountability in AI. The reality is that almost anything in today's tech landscape — algorithms, source code, data sets, training models or aggregated data — can be claimed to be a trade secret. Companies have historically utilized trade secrets protection claims to deny information access and disclosure requests, regardless of whether those requests come from courts, regulators, third parties or researchers. This expansive protection poses significant challenges in making AI technologies transparent and accountable.

It should be noted that not all information technology companies labelled as proprietary meet the requirements for trade secrets protection. Information that is public knowledge or that is widely recognized within an industry does not qualify for trade secrets protection.[47] When companies collect large amounts of data, they often claim these data sets are protected by trade secrets. It is unclear if these claims qualify for trade secrets protection and often end up being decided in court. Therefore, courts are essential in examining these claims, differentiating between genuine trade secrets and information that does not meet the established criteria. This judicial oversight ensures that the protection of trade secrets does not come at the expense of the right to a fair trial or the public's access to information. To effectively examine trade secrets protection claims and ask the right questions, courts must possess a basic understanding of these complex technologies. This requires a robust support system for the courts and regulators. Building capacity and bringing in technologists emerge as important initial steps. Through diligent examination of trade secret claims and distinguishing legitimate claims from overstated corporate claims, courts and regulators foster a legal landscape that carefully balances the rights of innovators with transparency and the public interest.

The challenges posed by extensive trade secrets protection in ensuring transparency and accountability are not new. Similar issues have been encountered in other industries, such as pharmaceuticals, chemicals and tobacco, where corporate secrecy has often restricted public access and due process. Many people have suffered due to these opaque systems stemming from overprotected corporate secrets.

Interestingly, trade secrets law does not typically dominate AI discussions as much as privacy, antitrust or internet regulation. This relative lack of deep policy discussion risks underestimating the impact of trade secrets law on transparency and broader societal issues. Venturing into this domain is akin to setting sail on uncharted waters; there are many uncertainties and disputes often result in lengthy court battles. Therefore, it is crucial to foster a deeper understanding of trade secrets and the limits of their protection. This calls for thorough

47 *Ruckelshaus* (*supra* note 20).

discussions among IP scholars, AI experts, public interest advocates, regulators and lawmakers.

IP rights are not absolute. The IP system incorporates built-in exceptions and limitations to strike a balance between IP protection and the public interest. Although trade secrets, as a contemporary form of IP, traditionally lack explicit limitations and exceptions within their domain, they can still be subject to limitations and exceptions that emerge from the IP legal framework.

There is growing academic interest in refining trade secrets law. Scholars are drawing on principles from other areas of IP law, such as copyright, trademarks and patent law. There are numerous proposals to borrow copyright exceptions such as fair use or patent flexibilities such as compulsory licences.

The "trade secret fair use" doctrine, for instance, introduces a multi-factor analysis for courts to better balance competing interests. This defence requires courts to evaluate specific factors to identify situations where trade secrets protection may hinder disclosures relevant to public health, safety and welfare (Varadarajan 2014). The analysis includes an examination of the purpose of the infringing use, the nature of the trade secret compared to the defendant's enhancements, the impact on the trade secret owner and the appropriateness of a reasonable royalty. This framework is particularly relevant for cases involving the "right to repair," addressing how companies control the maintenance and usage of their products (Katyal and Graves 2021; Varadarajan 2014).

Another example worth discussing is the concept of "thin trade secrecy." This concept is inspired by copyright's notion of "thinness," which limits the scope of copyright protection to foster innovation and creativity by allowing wider access to foundational ideas and information (Shipley 2007). In the case of trade secrets, "thinness" aims to strike a balance between safeguarding trade secrets and supporting public policy interests, particularly when the economic or creative value of a trade secret is minimal and at odds with broader public policy objectives (Feldman 2021; Katyal and Graves 2021). When applied to AI technologies (for example, data sets), this doctrine suggests that even if data sets are recognized as trade secrets by a court, the rationale for shielding them from public disclosure is fundamentally weak. Protection, in such cases, would be minimal and non-traditional, diverging from the core concept of IP as traditionally understood (ibid.). Any protection granted to such "thin" trade secrets should defer to a compelling public interest in disclosure.

This emerging body of research presents an opportunity to develop comprehensive strategies for trade secrets law and broader AI policy. Creating legal frameworks that protect (legitimate) trade secrets while also serving the broader public interest is crucial for crafting more effective AI policy and regulation. AI transparency calls for a nuanced approach, enabling the application of rights to information and due process within the trade secrets domain, aligning with the fundamental goal of IP rights.

One innovative solution within the IP framework is to mandate that AI systems be explanatory, emphasizing key features, offering context and explaining the rationale behind their decision-making processes. The public's interest in disclosure lies more in understanding the decision-making processes and accuracy of AI systems rather than in their internal mechanics, which are of more interest to competitors. Courts could potentially mandate such explanations in a manner that protects AI innovators while allowing legitimate inquiries to proceed. Explanation of the decision-making process does not compromise the trade secrets protection; targeted disclosure should be anticipated in order to strike the appropriate balance based on the core principles of the IP systems.

For more effective AI policy and regulation, focusing on this balance is crucial. There is no simple, one-size-fits-all solution, as trade secrecy has been exploited beyond its original intent. Initially designed to protect against the misappropriation of confidential business information, the scope of protection has now been extended to block disclosures to regulators, consumers, researchers and investigators. This overreach often places proprietary interests above the need for transparency, public disclosure and access, thereby reinforcing the "black box" nature of AI technologies and hindering progress toward the much-needed "glass box" transparency.

As we navigate the uncharted waters of trade secrets in the digital age, it becomes evident that our first step should be to ask the right questions before rushing toward solutions. This paper,

while not claiming to offer the definitive policy answers required, seeks to make a meaningful contribution to the ongoing AI policy discussions by exploring the expanding scope of trade secrets protection. It invites a critical look at its impact on AI policy. Lately, it has become trendy to discuss the significant implications of AI systems on human society. Indeed, the future and well-being of society may very well depend on how we manage the complexities and broad applications of trade secret claims. This paper is a modest step in questioning and potentially starting the discussion that could lead to a rethinking of trade secrets law, aligning it more closely with the needs and rights of society, particularly in the context of today's AI-driven world.

Works Cited

ACLU. 2023. "Testimony of Ritchie Eppink." AI in Government, United States Senate Committee on Homeland Security & Government Affairs. May 16. www.hsgac.senate.gov/wp-content/uploads/Testimony-Eppink-2023-05-16-1.pdf.

Akkermans, Bram. 2016. "The *numerus clausus* of property rights." In *Comparative Property Law: Global Perspectives*, edited by Michele Graziadei and Lionel Smith, 100–20. Cheltenham, UK: Edward Elgar.

Aplin, Tanya F. 2021. "The limits of trade secret protection in the EU." In *Research Handbook on Information Law and Governance*, edited by Sharon K. Sandeen, Christoph Rademacher and Ansgar Ohly, 174–94. Cheltenham, UK: Edward Elgar.

Awati, Rahul. n.d. "garbage in, garbage out (GIGO)." TechTarget. www.techtarget.com/searchsoftwarequality/definition/garbage-in-garbage-out.

Bone, Robert G. 1998. "A New Look at Trade Secret Law: Doctrine in Search of Justification." *California Law Review* 86 (2): 241–313. https://doi.org/10.2307/3481134.

Brown, Lydia X. Z., Michelle Richardson, Ridhi Shetty, Andrew Crawford and Timothy Hoagland. 2020. *Challenging the Use of Algorithm-driven Decision-making in Benefits Determinations Affecting People with Disabilities*. Center for Democracy & Technology. October. https://cdt.org/wp-content/uploads/2020/10/2020-10-21-Challenging-the-Use-of-Algorithm-driven-Decision-making-in-Benefits-Determinations-Affecting-People-with-Disabilities.pdf.

Citron, Danielle Keats and Ryan Calo. 2021. "The Automated Administrative State: A Crisis of Legitimacy." *Emory Law Journal* 70 (4): 798–845. https://scholarship.law.bu.edu/faculty_scholarship/838. https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1418&context=elj.

Coglianese, Cary. 2023. "AI, Due Process, and Trade Secrets." *The Regulatory Review*, September 4. www.theregreview.org/2023/09/04/coglianese-ai-due-process-and-trade-secrets/.

Cole, Grant. 2021. "Secrets, Sovereigns, and States: Analyzing State Government's Liability for Trade Secret Misappropriation." *Journal of Intellectual Property Law* 28 (1): 131–52. https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1466&context=jipl.

Correa, Carlos M. 1997. "Harmonization of Intellectual Property Rights in Latin America: Is There Still Room for Differentiation?" *Journal of International Law & Policy* 29: 109–33. www.nyujilp.org/print-edition/volumes-30-23/.

———. 2007. *Trade-Related Aspects of Intellectual Property Rights: A Commentary on the TRIPS Agreement.* Oxford, UK: Oxford University Press.

Czapracka, Katarzyna A. 2012. "Antitrust and Trade Secrets: The U.S. and the EU Approach." *Santa Clara High Technology Law Journal* 24 (2): 207–72. https://digitalcommons.law.scu.edu/chtlj/vol24/iss2/1.

De Liban, Kevin. 2017. "Seven Individuals with Disabilities Continue the Legal Fight against Secretive Medicaid Home Care Cuts." Legal Aid of Arkansas, January 30. https://arlegalaid.org/news-events/newsroom.html/article/2017/01/30/seven-individuals-with-disabilities-continue-the-legal-fight-against-secretive-medicaid-home-care-cuts.

Dickson, Ben. 2023. "How open-source LLMs are challenging OpenAI, Google, and Microsoft." *TechTalks* (blog), May 8. https://bdtechtalks.com/2023/05/08/open-source-llms-moats/.

Durkin, Allison, Patricia Anne Sta Maria, Brandon Willmore and Amy Kapczynski. 2021. "Addressing the Risks That Trade Secret Protections Pose for Health and Rights." *Health and Human Rights* 23 (1): 129–44. https://pubmed.ncbi.nlm.nih.gov/34194207/.

EDRi. 2015. "EU trade secrets Directive: threat to free speech, health, environment and worker mobility." *EDRi* (blog), March 23. https://edri.org/our-work/trade-secrets-directive-statement/.

Facebook Ad and Business Product Team. 2021. "Facebook Data Lineage Internal Document: ABP Privacy Infra, Long Range Investments [A/C Priv]." https://s3.documentcloud.org/documents/21716382/facebook-data-lineage-internal-document.pdf.

Feldman, Robin. 2021. "Intellectual Property: Naked Price & Pharmaceutical Trade Secret Overreach." In *The Judges' Book 5* (14): 93–100. https://repository.uchastings.edu/judgesbook/vol5/iss1/14.

Fia, Tommaso. 2022. "Resisting IP Overexpansion: The Case of Trade Secret Protection of Non-Personal Data." *IIC – International Review of Intellectual Property and Competition Law* 53: 917–49. https://doi.org/10.1007/s40319-022-01204-8.

Fink, Elliot. 2019. "Dirty Little Secrets: Fracking Fluids, Dubious Trade Secrets, Confidential Contamination, and The Public Health Information Vacuum." *Fordham Intellectual Property, Media and Entertainment Law Journal* 29 (3): 971–1024. https://ir.lawnet.fordham.edu/iplj/vol29/iss3/5/.

Foss-Solbrekk, Katarina and Ann Kristin Glenster. 2022. "The intersection of data protection rights and trade secret privileges in 'algorithmic transparency.'" In *Research Handbook on EU Data Protection Law*, edited by Eleni Kosta and Ronald Leenes, 163–83. Cheltenham, UK: Edward Elgar.

Gervais, Daniel. 2008. *The TRIPS Agreement: Drafting History and Analysis.* 3rd ed. London, UK: Sweet and Maxwell.

Griffith, Eric. 2023. "GPT-4 vs. ChatGPT-3.5: What's the Difference?" PCMag, March 16. www.pcmag.com/news/the-new-chatgpt-what-you-get-with-gpt-4-vs-gpt-35.

Gutman, David. 2018. "Uber and Lyft may have to disclose Seattle data they claim secret, Supreme Court rules." *The Seattle Times*, May 31. www.seattletimes.com/seattle-news/transportation/uber-and-lyft-may-have-to-disclose-data-they-claim-secret-supreme-court-rules/.

Kapczynski, Amy. 2022. "The Public History of Trade Secrets." *UC Davis Law Review* 55: 1367–1443.

Katyal, Sonia K. and Charles Tait Graves. 2021. "From Trade Secrecy to Seclusion." *Georgetown Law Journal* 109: 1337–1420.

Kiliç, Burcu. 2014. *Boosting Pharmaceutical Innovation in the Post-TRIPS Era: Real-Life Lessons for the Developing World.* Cheltenham, UK: Edward Elgar.

Kreps, Sarah. 2024. "Responsible science: What Sam Altman can learn (and not learn) from Nobel and Oppenheimer." *Bulletin of the Atomic Scientists*, February 26. https://thebulletin.org/2024/02/responsible-science-what-sam-altman-can-learn-and-not-learn-from-nobel-and-oppenheimer/.

Kroll, Joshua A., Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson and Harlan Yu. 2017. "Accountable Algorithms." *University of Pennsylvania Law Review* 165: 633–705. https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3.

Lecher, Colin. 2018. "What happens when an algorithm cuts your health care." *The Verge*, March 21. www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy.

Lemley, Mark A. 2010. "The Surprising Virtues of Treating Trade Secrets as IP Rights." *Stanford Law Review* 61 (2): 311–53. www.stanfordlawreview.org/print/article/the-surprising-virtues-of-treating-trade-secrets-as-ip-rights/.

Levine, David S. 2011. "The impact of trade secrecy on public transparency." In *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, edited by Rochelle C. Dreyfuss, Pauline Newman and Katherine J. Strandburg, 406–41. Cheltenham, UK: Edward Elgar.

Merrill, Thomas W. and Henry E. Smith. 2000. "Optimal Standardization in the Law of Property: The *Numerus Clausus* Principle." *Yale Law Journal* 110 (1): 1–70. https://doi.org/10.2307/797586.

Monsees, Paul R. 2018. "Ride-Sharing Services Lose Latest Trade Secret Battle." *The National Law Review*, June 11. www.natlawreview.com/article/ride-sharing-services-lose-latest-trade-secret-battle.

Mylly, Ulla-Maija. 2023. "Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information." *IIC – International Review of Intellectual Property and Competition Law* 54: 1013–43. https://doi.org/10.1007/s40319-023-01328-5.

Nashkova, Suzana. 2023. "Defining Trade Secrets in the United States: Past and Present Challenges – A Way Forward?" *IIC – International Review of Intellectual Property and Competition Law* 54: 634–72. https://doi.org/10.1007/s40319-023-01310-1.

Peterson, Cass. 1984. "Supreme Court Upholds U.S. Power To Publicize Pesticide Information." *The Washington Post*, June 27. www.washingtonpost.com/archive/politics/1984/06/27/supreme-court-upholds-us-power-to-publicize-pesticide-information/10bbb2dd-e7c5-45dd-9210-9e65447a4af1/.

Pooley, James. 2022. "The Artificial Distinction Between Trade Secrets and 'Confidential Information.'" IPWatchdog, July 28. https://ipwatchdog.com/2022/07/28/artificial-distinction-trade-secrets-confidential-information/id=150443/.

Quinn Emanuel Trial Lawyers. 2020. "The Rising Importance of Trade Secret Protection for AI-Related Intellectual Property." Firm memoranda, April 24. www.quinnemanuel.com/the-firm/publications/the-rising-importance-of-trade-secret-protection-for-ai-related-intellectual-property/.

Ramlochan, Sunil. 2023. "The Black Box Problem: Opaque Inner Workings of Large Language Models." Prompt Engineering & AI Institute, October 23. https://promptengineering.org/the-black-box-problem-opaque-inner-workings-of-large-language-models/.

Risch, Michael. 2008. "Why Do We Have Trade Secrets?" *Marquette Intellectual Property Law Review* 11 (1): 1–77.

Sandeen, Sharon K. 2010. "The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act." *Hamline Law Review* 33: 493–543. https://open.mitchellhamline.edu/facsch/314.

Sandeen, Sharon K. and Ulla-Maija Mylly. 2021. "Trade Secrets and the Right to Information: A Comparative Analysis of E.U. and U.S. Approaches to Freedom of Expression and Whistleblowing." *North Carolina Journal of Law & Technology* 21 (3): 1–61. https://scholarship.law.unc.edu/ncjolt/vol21/iss3/2.

Sell, Susan. 2004. "Intellectual Property and Public Policy in Historical Perspective: Contestation and Settlement." *Loyola of Los Angeles Law Review* 38 (1): 267–321. https://digitalcommons.lmu.edu/llr/vol38/iss1/6.

Shipley, David E. 2007. "Thin But Not Anorexic: Copyright Protection for Compilations and Other Fact Works." *Journal of Intellectual Property Law* 15 (1): 91–141. https://digitalcommons.law.uga.edu/jipl/vol15/iss1/3.

Simpson, Michael P. 2005. "The Future of Innovation: Trade Secrets, Property Rights, and Protectionism – an Age-Old Tale." *Brooklyn Law Review* 70 (3): 1121–63. https://brooklynworks.brooklaw.edu/blr/vol70/iss3/10.

Stanley, Jay. 2017. "Pitfalls of Artificial Intelligence Decisionmaking Highlighted In Idaho ACLU Case." ACLU News & Commentary, June 2. www.aclu.org/news/privacy-technology/pitfalls-artificial-intelligence-decisionmaking-highlighted-idaho-aclu-case.

United Nations Conference on Trade and Development-International Centre for Trade and Sustainable Development. 2005. *Resource Book on TRIPS and Development.* New York, NY: Cambridge University Press.

Varadarajan, Deepa. 2014. "Trade Secret Fair Use." *Fordham Law Review* 83 (3): 1401–54. https://ir.lawnet.fordham.edu/flr/vol83/iss3/9.

Yenerall, Joseph. 2021. "The Secret's Out: The Third Circuit Clarifies Pennsylvania Trade Secret Law in Advanced Fluid Systems, Inc. v. Huber." *Villanova Law Review* 66 (4): 813–30. https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=3501&context=vlr.

Zink, Julie E. 2018. "When Trade Secrecy Goes Too Far: Public Health and Safety Should Trump Corporate Profits." *Vanderbilt Journal of Entertainment and Technology Law* 20 (4): 1135–80. https://scholarship.law.vanderbilt.edu/jetlaw/vol20/iss4/4.

Zuboff, Shoshana. 2022. "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization." *Organization Theory* 3 (3): 1–79. https://doi.org/10.1177/26317877221129290.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org