R A I L

The Journal of Robotics, Artificial Intelligence & Law

fastcase **FULL COURT PRESS**

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@ meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Show Me Your Secrets: How the Use of Trade Secrets Relates to the Demand for Transparent Artificial Intelligence—Part II

Sander Vogt*

As the undeniable rise of artificial intelligence ("AI") in modern society continues at an astounding pace, the calls for its trustworthy development and implementation grow ever louder. In particular, society's widespread demands for transparent and understandable AI decision making can hardly be ignored. Parallel to these developments, the use of trade secrets is becoming an increasingly popular and attractive form of intellectual property protection within the AI industry.

If one were to jump to conclusions, then few terms seem as opposing as "secrecy" and "transparency." Yet, this article posits that society's demands for trustworthy and understandable AI and industry's desire to comprehensively and effectively protect its AI-related assets are not set on a collision course. Rather, a flexible approach to regulation may accommodate the plethora of interests, technical realities, complexities, and limits inherent to this debate. With the European Commission's Draft Artificial Intelligence Act breaking new ground in April 2021 as the first-ever proposal for a broad, horizontal regulation of AI, the question of reconciling the emergent principle of transparency and the use of trade secrets becomes increasingly relevant to regulators. This article provides an analysis of the relevant movements, policies, legal frameworks, and other considerations that shape this discussion in the United States, European Union, and the People's Republic of China.

This second part of a two-part article discusses the rise of trade secrets and trade secrecy and transparent AI. The first part of the article, which appeared in the July–August 2022 issue of The Journal of Robotics, Artificial Intelligence & Law, *discussed the rise of AI.*

The Rise of Trade Secrets

The Prominence of Trade Secrets in the Realm of Artificial Intelligence

Developers of new technologies have generally always understood the need for intellectual property protection. Indeed, there are those who suggest that a corporation's "intellectual capital" is

its most valuable asset, regardless of which business it is in.[97] In the software industry, intellectual property law has given software developers an incentive to invest in emerging technologies by providing a legal mechanism through which some of the value of software can be encapsulated and translated into wealth.[98] Taking into account the staggering economic power of the rising artificial intelligence ("AI") industry, it comes as no surprise that intellectual property–related questions are of significant importance.

It has been stated that the software industry and its relation-ship to intellectual property can be described not only through its three preferred forms of protection, namely copyright, patents, and trade secrets, but also by different phases of preference (although these should not be seen as strict intervals).[99] The first phase, char-acterized by a strong vertical structure in the industry and heavy integration with physical hardware, saw software developers rely primarily on trade secrets supplemented by contract law.[100] The second phase was that of copyright, as a direct result of the U.S. Congress' push for greater propertization of copyright.[101] During this second phase, the IT industry morphed into a more horizon-tal structure with software becoming increasingly detached from mere code-based interactions with hardware. In a third phase, the software industry looked favorably upon patent protection, as the limits of copyright protection caused software developers to look elsewhere.[102] However, the limits of patent protection have fueled a fourth phase characterized by a "robust reliance on the backdrop of trade secrecy at the cost of more disclosure-oriented regimes like copyright and patent law."[103]

Even though the secretive nature of trade secrets limits empirical analysis to broad surveys and those cases that reach final rulings,[104] it is known that the use of trade secrets is booming and common in many industries.[105] Following this trend, the AI industry has wit-nessed a strong shift toward the use of trade secrets as well.[106] For example, trade secret theft and litigation have been gaining signifi-cant traction in the past few years in the fields of new technologies such as robotics, virtual reality, and autonomous vehicles.[107]

Definitions and Legal Frameworks for Trade Secrets: A Comparative Analysis

In terms of regulation, trade secrets have long been considered a somewhat neglected form of intellectual property. As will be

shown below, the leading jurisdictions in AI development have only recently revamped legal frameworks for the protection of trade secrets. This article will discuss definitions of trade secrets and aspects of their protection mechanisms in the United States, the European Union, and China. The choice for these jurisdictions is based on empirical analysis.

A global study conducted in 2018 by Asgard and Roland Berger, an AI-focused German venture capital firm and a global consultancy firm, provided useful insights into the global distribution of AI-related innovation. The United States leads the AI ecosystem with 40 percent of the total number of AI startups worldwide, with China following at 11 percent.[108] While no single European country achieves critical mass, the contribution of EU Member States as a whole amounts to around 14 to 15 percent of the global total and around 22 percent if one includes the United Kingdom in a European regional perspective.[109]

Below, this article will discuss certain national and regional systems, after first looking into the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights.

TRIPS

The WTO Agreement on Trade-Related Aspects of Intellectual Property Rights[110] ("TRIPS") is the most comprehensive multilateral treaty on intellectual property and worthy of brief discussion. Membership of the World Trade Organization is contingent upon acceding to TRIPS. The goal of TRIPS is to ensure that Member States harmonize and provide minimum standards for intellectual property protection and enforcement.[111]

Without specifically mentioning trade secrets, TRIPS does address "undisclosed information." Under Article 39, such information is worthy of protection if "(a) it 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." Member States should ensure that natural and legal persons have the possibility of preventing such 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.[112]

The United States

In the United States, the law of trade secrets is more the product of evolution under the common law than the product of statutes as is the case with copyright or patents.[113] The common law of the States governed trade secret law, with the 1939 Restatement of Torts providing some guidance. In 1979, the National Conference of Commissioners on Uniform State Laws sought to harmonize certain aspects of trade secret law throughout the United States and drafted the Uniform Trade Secrets Act ("UTSA"). It was enacted by 47 states (and the District of Columbia) and was approved by the American Bar Association.[114] In recent years, trade secret law has received renewed attention in the United States. Of significant importance is the recently adopted Defend Trade Secrets Act ("DTSA") of 2016. The DTSA substantially revamps enforcement possibilities for trade secret owners, by providing a private civil cause of action for victims of trade secret espionage or theft where a trade secret has been misappropriated, and requires that the misappropriated trade secret is related to a product or service used in, or intended for use in, interstate commerce.[115] The DTSA thus aimed to supplement the UTSA by providing original federal jurisdiction, as the latter instrument only covered state law claims.[116] In the absence of diversity jurisdiction or a violation of federal law, many plaintiffs were previously left with overburdened state courts, leading to delayed and generally unattractive trade secret litigation under the UTSA.[117] In addition, the DTSA controversially provides for a formidable ex parte seizure provision, according to which a federal court may in extraordinary circumstances issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret in question, based on an affidavit or verified complaint.[118] Unsurprisingly, the DTSA has been called the "most significant expansion of federal involvement in intellectual property law in the past thirty years,"[119] and was one of the rare displays of confident bipartisanship on Capitol Hill in a polarized political environment.[120]

There are three definitions of a "trade secret" that are most frequently cited by courts in the United States. The first generally accepted definition can be found in § 747 comment b of the 1939

Restatement of Torts. Accordingly, a trade secret may consist of "any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[121] The UTSA defines trade secrets as "information, including a formula, pattern, compilation, program, device, method, technique, or process, 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."[122] A third definition originates from the Restatement (third) of Unfair Competition § 39 (1995), according to which a trade secret is "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."[123] Interestingly, despite the widespread adoption of the UTSA, most courts still refer to the 1939 Restatements definition.[124] The DTSA has largely adopted the UTSA's definition of trade secrets, thus causing courts to also rely on the 1939 Restatements definition in connection with DTSA.[125] In doing so, courts routinely apply a six-factor test to determine whether matter qualifies as a trade secret by examining: (1) the extent to which information is known outside a trade secret claimant's business including (2) by employees and others involved in the business, (3) secrecy measures, (4) the value of the information to the claimant and his competitors, (5) the effort or investment to develop the information, and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[126]

Trade secret law in the United Sates sets virtually no limit on the class or type of matter that is eligible for trade secret protection, in contrast to copyright or patent protection.[127] This is of particular importance in the realm of AI, where an array of different valuable components merit protection. As will be discussed further on, algorithms, data, and designs can thus also be protected by trade secrets.

The European Union

The legal framework for trade secrets in the European Union is Directive (EU) 2016/943 of June 8, 2016, on the protection of

undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure ("TSD"). The TSD was adopted to harmonize the disparate national trade secrets regimes of the Member States. Following the usual two-year transposition deadline, EU Member States had until June 9, 2018, to transpose the TSD into national law. The TSD harmonizes the definition of trade secrets throughout EU Member States. Accordingly, a trade secret is defined as "information which meets all of the following requirements: (a) it 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) it has commercial value because it is secret and (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."[128] Because the definition under the TSD is so broad, any data (including customer or user personal data and newly created data) can be protected by trade secrets.[129]

In addition, the TSD defines the relevant forms of misappropriation, as well as clarifies the need for guaranteeing reverse engineering and parallel innovation. Much like the DTSA, the TSD also harmonizes civil means through which victims of trade secret misappropriation may seek redress and emphasizes the need for avoiding unreasonable time limits and unwarranted delays.[130] The TSD also requires Member States to provide for injunctive and corrective measures where a judicial decision identifies an unlawful acquisition, use, or disclosure of a trade secret, including the prevention of the unlawful use and further disclosure of misappropriated trade secrets, removing goods that have been manufactured on the basis of a misappropriated trade secret from the market and the right to compensation for damages caused by the unlawful use or disclosure of the misappropriated trade secret.[131]

However, this harmonized approach should be somewhat nuanced.

First, the TSD only provides for so-called "minimum harmonization." This means that the 27 Member States are free to implement or maintain higher standards than those set by the TSD.

Second, because the TSD does not consider trade secrets a form of intellectual property,[132] trade secret holders may not rely on Directive 2004/48/EC of April 29, 2004, on the enforcement of

intellectual property rights or on Regulation (EU) 608/2013 on June 12, 2013, concerning customs enforcement of intellectual property rights. As a result, certain specific measures regarding evidence collection (such as counterfeit search and seizure proceedings) and border measures do not as such apply to trade secrets as they do to patents, copyright, and trademarks. Lastly, the TSD does not cover criminal sanctions, leaving this to the discretion of the Member States as well.

The People's Republic of China

Renewed attention toward trade secrets has not been limited to the West. The Chinese Anti-Unfair Competition Law ("AUCL") was recently amended in 2019 and significantly addressed trade secrets. Accordingly, a trade secret is defined as "technical, operational or other commercial information unknown to the public and is of commercial value for which the right holder has taken corresponding confidentiality measures."[133] This new definition disposed of the earlier requirement of a trade secret needing to be "capable of bringing economic benefits to the owner of rights" and covers any commercial information, rather than being limited to just technical and operation information.[134]

The AUCL has introduced certain major changes to trade secret protection in China by enlarging the scope of protection through the introduction of new forms of infringement, reducing the burden of proof for plaintiffs in trade secret litigation and enhancing liability and punishment for misappropriation.[135] For example, the compensation due for infringement can be up to five times the damages caused and the cap for such compensation has been raised to 5,000,000.00 RMB (approximately US$764,000.00 or €639,000.00). Trade secret misappropriation is also a crime, punishable by up to seven years imprisonment.[136] Although some have stated that China has one of the most advanced trade secret protection systems in the modern world,[137] it might be more accurate to state that recent amendments offer a promising view of future trade secret protection in China. It is no secret that seriously inadequate trade secret protection in China has been at the center of trade and intellectual property–related tensions with the West, as was most recently confirmed in a U.S. Trade Representative Report on China's WTO Compliance.[138]

Why Trade Secret Protection Is Attractive in the Realm of Artificial Intelligence

Intellectual property protection of AI requires creativity and flexibility, as there is no singular approach to protecting AI-related assets.[139] A dynamic approach is necessary, incorporating patents, copyright, and trade secrets interchangeably, where appropriate. However, because patents may not always be compatible with intellectual property strategies of AI developers, and copyright protection has its own limitations and uncertainties, it comes as no surprise that trade secrets are a desirable tool. This observation is in alignment with recent initiatives to revamp trade secret law in the United States, the European Union, and China. Below, this article discusses different reasons for the attractiveness of trade secrets for protecting AI-related assets.

Artificial Intelligence Is Not as Susceptible to Reverse Engineering and Independent Discovery

Independent discovery and reverse engineering are generally a proper means of obtaining a trade secret.[140] It logically follows that the attractiveness and value of trade secrets increases when the protected technology does not easily allow for independent discovery or reverse engineering, and where replacement by new innovations or where describing the technology cannot be done without significant effort.[141] A trade secret's vulnerability to reverse engineering depends on the complexity of the secret and the nature of the product itself. Intangible products or services can be considered less tractable to reverse engineering than material objects, as they generally provide less palpable and perceptible information.[142] Thus, where independent discovery or reverse engineering is not likely, trade secrets increase in usefulness and appropriateness.[143]

In the case of AI, independent discovery and reverse engineering is far from an evident task. Several factors related to the nature of AI stand out in this respect.

First, the vast amounts of input data (including training data, validation data, and testing data) through which a particular AI output is shaped make independent discovery impracticable. The particular combination of input data, as well as the method of creating and categorizing the different data sets, is also generally not susceptible to reverse engineering.[144] Furthermore, where supervised learning is involved in the case of machine learning

algorithms, the particular way in which an AI operator guides and trains the algorithms to interact with data introduces additional layers of difficulty.

Second, reverse engineering is also extremely unlikely in the case of "black box" AI, where the extreme algorithmic complexity of the machine learning process can prevent even the AI developers and operators from comprehending how decisions are reached.[145]

Third, because the creation of algorithms is a complex and very specific task, independent discovery is highly implausible. For example, in *ClearOne Communications v. Bowers*, it was held that because the development of trade secret–protected acoustic echo cancellation software involves numerous algorithmic and programming choices, it is very difficult or even impossible for two individuals working independently to produce the same algorithm.[146]

Trade Secrets Offer a Broad Scope of Protection

As is apparent from the definitions of trade secrets discussed above, there is virtually no limit to the class of information that can be protected as a trade secret, making a broad group of competitive assets protectable by trade secrets.[147] Trade secrets protect both technical and nontechnical information, ideas, and even facts, such as names and phone numbers on a client list.[148] This is of pivotal importance in the realm of AI. It has already been held that algorithms and source code are protectable or protected by trade secret law.[149] Furthermore, the broad scope of trade secret definitions in the United States essentially allows for the protection of data sets.[150] This is also the case under the TSD, as any data can be protected by trade secrets.[151] The same goes for trade secret law in China.[152]

As a result of these broad definitions of trade secrets in the United States, the European Union, and China, trade secrets are an attractive way of protecting valuable information that may not fall under copyright or patent protection. Because AI consists of several valuable components that are worthy of protection, trade secrets offer AI developers a convenient way to expand their intellectual property portfolio.

Patents May Not Be an Ideal Option for Protecting Artificial Intelligence

Patents are one of the most popular forms of intellectual property protection and are often considered the strongest.[153] However,

one should be careful not to draw the conclusion that patents are therefore the best option for protecting AI-related assets. There are two major reasons for this.

First, there is only limited patentability for AI-related assets, which has caused uncertainty.[154]

Second, trade secrets offer a certain degree of flexibility that cannot be matched by patents.

The U.S. Patents Act sets four categories of patentable subject, namely "processes," "machines," "manufactures," and "compositions of matter."[155] The two types of patents are utility patents, which protect the product, process, or machine or an improvement thereof, and design patents, which apply to the design of an article or manufacture.[156] The patent regime in the United States excludes abstract ideas, laws of nature, and natural phenomena as patentable subject matter, because monopolizing these tools by granting patent rights would impede innovation rather than promote it.[157] In a recent Guidance published by the U.S. Patent and Trademark Office (the "USPTO"), the USPTO clarified that the "abstract idea" exception extends to "mathematical concepts [such as] mathematical relationships, mathematical formulas or equations, mathematical calculations" as well as methods of organizing human activities and mental processes.[158] In theory, this excludes algorithms and models. Under the Alice/Mayo test of the Supreme Court, general manipulation and processing of data is not patentable. Simply implementing a mathematical principle on a physical machine cannot be considered a patentable application.[159]

Similarly, algorithms and models are not patentable under the European Patent Convention (as they are of an abstract mathematical nature), but AI inventions can be patented as a subset of so-called "computer-implemented inventions." This requires the algorithm or model to contribute to the technical character of the invention, by serving a specific technical purpose.[160] Under Article 25.1 of the Chinese Patent Law, rules and methods of mental activities are not eligible for patent protection, but an application will stand as long as there is a clear technical feature described in the claim.[161]

Conceptually, these patent regimes seem to be unfavorable toward AI-related assets such as algorithms, models, and data sets. Indeed, algorithms are essentially a mathematical expression of nature and are thus not patentable, as are other AI-related mathematical formulas and test strategies.[162] Patent law in the United

States, Europe, and China requires a practical application of an algorithm in order for it to even be considered as patentable subject matter, without it always being entirely clear what a "practical application" is. Furthermore, other components of an AI system, such as data sets, do not meet thresholds for patentability. However, despite these conceptual barriers to protecting AI-related assets with patents, patent applications for AI-related inventions are actually thriving.[163] China saw 389,571 AI-related patent applications over the past 10 years, ranking first in the world, accounting for 74.7 percent of the global total and more than eight times that of the United States,[164] although American companies still lead in terms of AI patents actually granted.[165] Furthermore, a report on Public Views on Artificial Intelligence and Intellectual Property Policy of the USPTO generally concluded that the patent system as it stands is as such not incompatible with emerging AI technologies.[166]

Nonetheless, despite a high number of patent applications for AI-related inventions, patent protection may still not be ideal for AI-related assets when compared to trade secret protection.

A first and obvious point is that trade secret protection does not entail disclosure (which, as the quid pro quo for obtaining a temporary monopoly on an invention, is a necessary step in the application process for a patent), thus allowing a competitive advantage to be maintained through confidentiality.

Second, the requirements of non-obviousness, novelty, and utility for patent protection[167] do not apply to trade secrets. In order to be protectable as a trade secret, the AI-related assets need only meet the requirements enshrined in the trade secret definitions discussed above.

Third, trade secrets have a broader scope of protection and can include components of AI that are not patentable.

Fourth, the costs associated with establishing trade secret protection are much lower in comparison to patents, which may be beneficial in a rapidly evolving technology like AI.[168]

Fifth, a trade secret does not require registration and trade secret protection is thus not contingent upon government approval, contrary to patents.[169]

Lastly, where patents only have a duration of protection of 20 years,[170] trade secrets will last for as long as the information remains confidential, which can extend well beyond the 20 year mark.[171]

When comparing patent protection to trade secret protection, it becomes clear that trade secrets may be preferable in a variety of

situations, such as when patentability requirements cannot be met, when the cost of pursuing patent protection outweighs the benefits, or when the need for protection extends beyond the 20-year mark.[172]

Copyright Protection of Software Is Complex and Uncertain

Copyright protection plays an important role for software, which is greatly relevant to AI. The purpose of copyright protection is to protect the creative works of the human mind and thus stimulate creativity in society.[173] As a general point, copyright protection is broader than patent protection, as any creative work may be covered by copyright so long as the work is "original" and is the "author's own intellectual creation" (the European standard)[174] or demonstrates "at least some minimal degree of creativity" (the U.S. standard),[175] as well as being fixed in a tangible medium.[176] Copyright protection is conferred automatically. In essence, copyright protection grants the author the exclusive right of compensation for the reproduction of his/her work, and a right of prohibition.[177] However, mere ideas, procedures, methods of operation, or mathematical concepts as such are not copyrightable.[178]

Copyright is an attractive form of intellectual property protection in the realm of AI, particularly for the protection of software code.[179] This is of great importance, as source code is considered the "lifeblood of software" embodying the potential of the code's creativity.[180] Of note, there is somewhat of a conceptual overlap between copyright and trade secrets in the context of software. Most software applications today are marketed in the format of object code, which is the chain of binary steps that constitute the directions sent to a computer's hardware.[181] Object code is generally protected by copyright, despite its functionality strongly outweighing any creativity in the code, while source code is now often protected by trade secrets.[182]

Furthermore, databases and other compilations of data (such as training, validation, and testing data sets) can be protected under copyright, even where the content itself is not protected, provided that the selection or arrangement of the data constitutes an intellectual creation.[183] EU law provides for a sui generis database right, which can protect the contents of a database.[184] As such, the maker of a database in which there has been a qualitatively or quantitatively substantial investment in the obtaining, verification, or presentation of the contents of the database will be endowed with

a right to prevent extraction and/or re-utilization of the whole or part of the contents of the database.[185] Conversely, pursuant to the Supreme Court's judgment in *Feist Publications, Inc. v. Rural Telephone Service Co., Inc.*, the content of databases cannot be protected in the United States, with no alternative method to protect databases having been provided by the U.S. legal system.[186]

Although copyright protection has its benefits, it also has its limitations. Some of its disadvantages are apparent when copyright is compared to trade secrets. For example, trade secret protection imposes no originality or creativity requirements and extends to non-copyrightable information such as ideas, procedures, methods of operation, and mathematical concepts. However, it can be argued that a larger point of interest is the increasing uncertainty as to how copyright and software relate in the face of increasing technical complexity.

As alluded to above, software has evolved extensively in the past decades, gradually becoming more than just literal code-based programs and moving more toward abstract ideas and designs rather than just code as a product of authorship.[187] This has given rise to much debate and uncertainty as to what aspects of software code are copyrightable. Generally speaking, copyright protection does not extend to the functionality of software, but only to the creative aspects of the code.[188] Yet, the paradox discussed above shows that object code is sometimes deemed worthy of copyright protection, although it is largely functional in nature.[189]

Recent developments have shed more light on the uncertainty of software-related copyright protection. The long legal battle between Google and Oracle, heralded as the "copyright case of the decade,"[190] was finally decided by the Supreme Court of the United States on April 5, 2021. The case concerned the question of whether Google had infringed upon Oracle's copyright on its Java declaring code during the development of the Android smartphone platform.[191] The Supreme Court ruled that Google did not violate Oracle's copyright, holding that Google's copying was fair use.[192] However, the central question of whether the valuable application programming interfaces[193] were indeed copyrightable in the first place was dodged by the Supreme Court. Google argued that declaring code is just a functional system of basic computer commands that should not be copyrightable, and that any other outcome would destroy the software industry. Oracle argued that Google's excessive copying threatened to undo the strong copyright protection that shaped

the American tech industry's success.[194] The prevailing argument was not identified.

Besides this uncertainty, the case of *Google v. Oracle* uncovers another potential weakness of copyright protection for software. A copyright holder cannot always prevent a user from copying the code for a limited purpose or modifying it, as this could be considered "fair use."[195] This fair use exception could see considerable expansion in lower courts as a result of *Google v. Oracle*.[196]

As these evolutions cause the fine line between copyrightable expression and mere idea to blur even further, a tendency toward embracing trade secrets emerges in response.[197] It is unlikely that the Supreme Court's recent decision to dodge a central (but technically difficult) question on the copyrightability of software code will stop this trend.

The Nature of Trade Secrets and the Tendency Toward Propertization

Before moving on to the analysis of how trade secrets and the principle of transparency interact, it is worthwhile to pause and consider the nature of trade secrets and the topic of propertization. The latter notion should be understood as the transitioning of rights, either contractual or extra-contractual, toward the realm of property rights. At this stage, it should become clear that a central theme of this article revolves around the question of entitlement to information. Whether an AI company uses trade secrets to protect its AI assets, or a section of the public demands information on how an AI application creates output, the base dynamic is about the right to either withhold or obtain information.

Traditionally, the purpose of trade secrets has been to protect against employees or other business partners from using a company's confidential innovations.[198] There is a debate as to whether trade secret protection should be understood as a post-factual tort mechanism designed to rectify a breach of confidence and remedy a loss of competitive advantage, or whether this concerns a (quasi) property right. It has been suggested that the answer lies in an integrated approach.[199] Indeed, trade secrets aim to protect confidential relationships, with the important condition that the subject matter is worthy of protection.[200] Simultaneously, trade secret protection does confer at least weak forms of property

rights.[201] It has even been argued that construing trade secrets as property rights rather than relational obligations allows for a better balance between the interests of employers and employees faced with trade secret accusations, enabling the interests of the workforce and the wider economy to benefit from the formation of new, creative enterprises.[202]

The contours of this debate on the nature of trade secrets echoes a larger underlying discussion on the propertization of intellectual property law in general. The debate on propertization also concerns the issue of expanding intellectual property laws and property analogies to intangible information, conceiving technological developments, business information, and customer-related information as property.[203] This question of balancing propertization and stimulating innovation is not a new one, and arguably begins with how one interprets the term "intellectual property" itself.[204] Some scholars emphasize the need for property entitlement in order to avoid the "tragedy of the commons."[205] Others claim that increasing propertization may create more problems than it solves and warn of the negative economic effects of over-propertization, such as the diminution of the level of innovation that would otherwise be achievable through a more balanced approach.[206] It is this realization that, in the context of data propertization, fueled the movement for open data that has since been reasonably successful.[207]

The original design of trade secret law was not necessarily to encourage the propertization of information. Trade secret law is responsive to competition policy in that it allows legitimate reverse engineering and independent discovery and maintains the requirement that information is only owned as long as the owner puts appropriate effort into maintaining secrecy.[208] Nevertheless, other forms of intellectual property protection have seen increasing propertization. Trademarks have seen an expansion in propertization in the digital environment through recognizing trademarks in domain names and the doctrine of initial interest confusion.[209] Similarly, copyright has also witnessed this tendency.[210]

These tendencies may be at odds with other societal values and priorities. As put in the words of Margaret J. Radin, Professor Emerita of the University of Michigan Law School, when considering the interfaces between the propertization of intellectual property and countervailing policies of free speech and competitive markets, "legal discourse would serve society better if new information practices did not cause costly periods of over-propertization

before we remember our roots." In addition, one must consider how an over-propertization of trade secrets may scrape against a new emerging policy described in this article: the demand for transparent AI.

Trade Secrecy and Transparent AI: An Analysis

Trade Secrecy and Transparency Cannot Be Mutually Exclusive

It has been recognized before that tension between the implementation of the principle of transparency and intellectual property protection may arise.[211] As put by Jessica Meyers, "transparency is not just an abstract value, it has practical consequences."[212] Juxtaposing the prominence of trade secret protection for AI-related assets with the demands for transparent AI may then tempt the assumption that this concerns an epic battle between abstract concepts such as "secrecy" or "confidentiality" and "disclosure" or "transparency."

However, such an assumption would wrongfully oversimplify a far more complex dynamic that differs on a case-by-case basis. As a general observation, concerns of AI developers to maintain trade secret protection of AI-related assets that grant a considerable advantage in a competitive industry are, of course, logical. The same goes for societal expectations of trustworthy and understandable AI. Therefore, an approach that demands complete disclosure of all assets related to a particular AI system is unreasonable, as is the understanding that trade secret protection precludes any access to valuable information regarding the AI decision-making process.[213]

As alluded to above, a simple blanket approach to disclosure does not achieve the purpose of the principle of transparency. Simply dumping algorithms and vast amounts of data does not amount to meaningful transparency. In addition, explanations as to how machine learning models generate a certain output are not always readily available, and, even if they are, they may not always be understandable to humans. Complex models might have already adjusted themselves and evolved in the time between the generation of a certain output and the point of disclosure.

Furthermore, one must consider that there are methods to improve AI explainability without full disclosure as well as non-technical arguments against blanket disclosure.

First, one could argue that an overly strict principle of transparency entailing blanket disclosure might devaluate trade secrets to the point that innovation is no longer incentivized. Indeed, it has been stated that the increase in trade secrets litigation in emerging data-driven technology industries signals intense competition and thus a healthy market for innovation.[214]

Second, we must not forget that exaggerated transparency is neither expected nor expectable from humans. As legal realists have pointed out, decisions made by judges may sometimes be based on weak, unconscious rationalizations of underlying prejudices, stereotypes, or intuition.[215] If we cannot always explain what motivations lurk behind our decisions, will we then be able to comprehend the reasons for an AI system's decisions?

At the same time, an approach that leans too strongly on the over-propertization of trade secrecy is not a viable option either. This article has consistently referred to the strong call and extensive coverage of societal desire for understandable AI. Given the strength and scale of the movement for trustworthy AI, it is clear that a world in which trade secrets always prevail is inconceivable, as this will strongly undermine the development of human trust in AI applications.

In brief, approaching the dichotomy between trade secrecy and the principle of transparency as a zero-sum game is a lose-lose.

Reconciliation Requires Flexibility

The above discussion clearly demonstrates that the answer to the trade secrecy–transparency debate does not lie in a simple horizontal approach. As put by the IEEE, "rather than aiming for universal transparency standards that would be applicable to all uses of AI systems within a legal system, transparency standards should allow for circumstance-dependent flexibility."[216] Google states that given the fact that AI is a dynamic, constantly evolving technology, AI regulations should be adaptable over time and remain flexible across different applications.[217] This article agrees. One should indeed differentiate between a situation where AI systems are being used in the criminal justice system and where an AI system is used in a

business-to-business context for predicting the success of a client company's marketing strategy. Different applications of AI systems in different situations may require a different balance. This calls to the need for different approaches to resolving the tension between trade secrecy and transparency. The fairly recent TSD and DTSA and the increase in trade secret litigation might create new bodies of case law that incorporate the interests for trustworthy AI. These developments will have to be examined closely. Below, it will be demonstrated how different situations and different policies may produce different methods of resolution.

As a preliminary observation, it should be noted that there are technological advancements that may prove instrumental in overcoming the "black box" opacity of AI applications that impedes the fulfilment of the principle of transparency. Data scientists are currently building transparency tools that will increase our practical ability to interpret machine learning models.[218] The notion that there must be a trade-off between accuracy and performance of AI systems and their explainability or interpretability is also being challenged.[219] In addition, industry-led standards organizations are increasingly active in describing testable levels of transparency of AI systems, in order to measure compliance with substantive rules.[220] AI developers will need to consider implementing transparency considerations into the design of AI systems, so that the developers themselves can enable disclosure that respects intellectual property rights.[221]

Non-disclosure agreements, statutory confidentiality obligations, or granting limited access to duly appointed third parties constitute legal methods that may balance disclosure and trade secrecy in certain situations. For example, Article 70(1) of the recent EU Draft AI Act states that future regulatory bodies charged with assessing the conformity of high-risk AI systems with regulatory obligations shall respect trade secret protection of information and data under the TSD when performing their tasks.[222] Public authorities and notified bodies that need to be given access to confidential information or source code to examine compliance with substantive obligations will be placed under binding confidential obligations.[223] The IEEE recommends that policymakers consider the option of a public interest steward or trusted third party. This agent would then be given access to sensitive information (potentially protected by trade secrets) in order to answer public interest

questions, but still be under obligation not to disclose the specifics of such information.[224]

Another method of fulfilling the principle of transparency is through modes of explanation that do not undermine trade secret protection.[225] For example, in certain situations, counterfactual explanations that "describe the smallest change to the feature values that change the prediction to a predefined output" may provide more insight into the AI decision-making process, while not revealing the inner workings of the system and thereby protecting intellectual property.[226]

Although this article does not focus on the governmental adoption of AI, briefly examining the difference between the U.S. and European approaches demonstrates how solving the tension between trade secrecy and transparency is, above all, a matter of policy choices. For example, the American concept of governmental transparency is subdivided in "fishbowl transparency," which entails broad disclosure of information to the public, and "reasoned transparency," which requires that public authorities present reasons for their decisions. The protection of trade secrets and other proprietary information is considered an exception to the required disclosure of public information under fishbowl transparency.[227] There are examples of a different approach in European legal systems, which is not surprising considering the greater wariness of algorithms in Europe.[228] For example, the fairly recent French Law for a Digital Republic of 2016 exempted trade secrets from public disclosure requirements whenever a public body subjected residents to algorithmic processing.[229] However, the Conseil d'État (the highest constitutional authority in France) limited the scope of this exception by providing that if a public body relies solely on an algorithm for a decision, trade secrecy may not be relied on as an excuse for not disclosing its functioning.[230]

In a similar sense, the Administrative Supreme Court of Italy stated that holders of intellectual property rights cannot expect secrecy in view of the prevailing public right to "full knowability of the algorithm used and the criteria applied."[231] Depending on its final outcome, the EU Draft AI Act will allow for a new body of law to develop, as it proposes to resolve the tension between transparency obligations and the right to intellectual property protection by limiting transparency to "the minimum necessary information for individuals to exercise their right to an effective remedy and to

the necessary transparency towards supervision and enforcement authorities, in line with their mandates."[232] It will also be interesting to see how future decisions of the Court of Justice of the European Union will interpret the relationship between this provision and Articles 1(2)(b) and 5(d) TSD.[233]

Lastly, it is also interesting to consider how trade secrecy and transparency interact in the field of criminal law. An example is the well-known case of *State v. Loomis* before the Wisconsin Supreme Court. That case concerned the question of whether a criminal defendant's right to due process had been violated because the proprietary nature of an algorithmic criminal risk assessment tool, on which the trial court had partly relied to determine the length of a prison sentence, prevented defendants from challenging its scientific validity.[234] The Supreme Court rejected the criminal defendant's arguments for fishbowl transparency and held that the private company had a right to protect its proprietary information.[235] Clearly, there was no right to obtain any and all details concerning the proprietary algorithm's design.[236] However, even in these controversial situations, disclosure with reasonable respect for trade secrecy can be achieved through the use of protective court orders.[237]

Key Considerations for the Near Future

The above discussion demonstrates that there is no simple solution to the tension that may arise between the use of trade secrets and the demand for transparent AI. The competing interests that lie at the foundations of this debate will differ from situation to situation. Some might claim that the debate on trade secrets and the demands for transparent AI is a story of corporate interests competing with public policy interests, with strong intellectual property protection being the expression of the former and the principle of transparency the embodiment of the latter. However, one could also state that this debate concerns a competition between two public interests: the need for stimulation of innovation in emerging technologies on the one hand, and public desire for trustworthy AI on the other. It should come as no surprise that the wisest approach lies in accepting complexity and the need to assiduously seek an acceptable and reasonable outcome on a case-by-case basis. Indeed, smart, proactive regulation that both protects

public interests and fosters innovation will require regulators to achieve a complex balance.[238]

As the law stands today, with the exception of certain bodies of law that house similar principles of transparency with a limited scope, such as administrative law, criminal law, and the General Data Protection Regulation, there is currently no clear legal lens through which this tension can be examined. Moving forward, regulators will have to take into account a whole variety of factors when attempting to provide a framework to resolve the trade secrecy–transparency debate, if new approaches like the EU Draft AI Act are to be of real practical significance. These include, but are unfortunately not limited to, the complexity of AI, its myriad different applications that vary in degree of risk, the limits of human conceptions of transparency, technological implications, and "black box" AI, as well as the need to maintain the encouragement of innovation through trade secret protection.

Notes

97. Trade Secrets (ALM) § 1.02.

98. Bradford L. Smith & Susan O. Mann, *Innovation and Intellectual Property Protection in the Software Industry: An Emerging Role for Patents?*, 71 U. Chi. L. Rev. 241, 241 (2004).

99. *Id.*

100. *Id.*; Peter S. Menell, *Symposium: Toward a Third Intellectual Property Paradigm: Comments: The Challenges of Reforming Intellectual Property Protection for Computer Software*, 94 Colum. L. Rev. 2644, 2653 (1994).

101. Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 Cornell L. Rev. 1183, 1192 (2019).

102. Smith & Mann, *supra* note 98, at 242.

103. Katyal, *supra* note 101, at 1192. *See also* Aimee Fagan, *Trade Secret Litigation Now an Attractive Alternative to Patent Litigation*, Law.com (March 23, 2021), available at https://www.law.com/texaslawyer/2021/03/03/trade-secret-litigation-now-an-attractive-alternative-to-patent-litigation/.

104. Michael Fisch, *Empirical Methods in Trade Secret Research*, *in* Research Handbook on the Economics of Intellectual Property

Law (Vol. II—Analytical Methods) (Peter S. Menell & David L. Schwartz, eds.), Villanova Law/Public Policy Research Paper No. 2015-1021.

105. Lauren Davis, *Note: Secrecy for the Sake of It: The Defend Trade Secrets Act. A Devolving Global Market Based on the Legal Protection of Over-Secrecy*, 83 Brooklyn L. Rev. 359, 359 (2017); Aimee Fagan, *supra* note 103.

106. Huseinzade, *supra* note 12; Kop, *supra* note 12, at 319; Villasenor & Foggo, *supra* note 12, at 343; Coglianese, *supra* note 12, at 46.

107. David S. Levine & Christopher B. Seaman, *The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act*, 53 Wake Forest L. Rev. 105, 109-11 (2018); Alexis Kramer, *Trade Secret Cases Surge as Race for New Tech, Top Talent Heats Up*, Bloomberg BNA (May 10, 2017).

108. Asgard Capital Verwaltung & Roland Berger, *Artificial Intelligence—A Strategy for European Startups. Recommendations for Policymakers* (2018), 7, available at https://www.rolandberger.com/publications/publication_pdf/roland_berger_ai_strategy_for_european_startups.pdf.

109. *Id.*

110. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) (as amended on January 23, 2017).

111. Melvin Simensky, Lanning Bryer & Neil J. Wilkof, Intellectual Property in the Global Marketplace, Vol. 1: Electronic Commerce, Valuation, and Protection, O.28 (2d ed., John Wiley & Sons, New York, 1999).

112. TRIPS, Article 39(2).

113. Trade Secrets (ALM) § 1.01.

114. 1 Milgrim on Trade Secrets § 1.01 (2020); Jordana Balsam, *Booming Business and the Resulting Trade Secrets: How the Increase in United States and European Union Trade Led to Resulting Trade Secrets Directives and the Domination of the Intellectual Property Field*, 2 Int'l Comp., Policy & Ethics L. Rev. 503, 504 (2019).

115. 18 U.S.C. § 1836.

116. M. Claire Flowers, *Facing the Inevitable: The Inevitable Disclosure Doctrine and the Defend Trade Secrets Act of 2016*, 75 Wash & Lee L. Rev. 2207, 2216 (2018).

117. Davis, *supra* note 105, at 362.

118. 18 U.S.C. § 1836.

119. Davis, *supra* note 105, at 362.

120. Patrick Coyne, *What You Should Know About the Defend Trade Secrets Act*, Law360 (June 27, 2016).

121. 1 Milgrim on Trade Secrets § 1.01 (2020).

122. Uniform Trade Secrets Act, Section I (4).

123. Restat 3d of Unfair Competition, § 39.

124. 1 Milgrim on Trade Secrets § 1.01 (2020).

125. *Id.*

126. *Id.*

127. Trade Secrets (ALM) § 1.01; 1 Milgrim on Trade Secrets § 1.01 (2020).

128. Directive (EU) 2016/943 of June 8, 2016, on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Article 2.

129. Kop, *supra* note 12, at 319.

130. TSD, Article 6.

131. TSD, Article 6.

132. TSD, recital (1).

133. Anti-Unfair Competition Law of the People's Republic of China (2019 Amendment), Article 9.

134. Youping Ma & Guoquan Yang, *Are Trade Secrets an Alternative Way to Protect AI*, 283 Managing Intell. Prop. 63, 63 (2019).

135. *Id.*, at 64.

136. *Id.*

137. Ricardo V. Segate, *Securitizing Innovation to Protect Trade Secrets Between "the East" and "the West": A Neo-Schumpeterian Public Legal Reading*, UCLA Pac. Basin L.J. 59, 61 (2020).

138. U.S. Trade Representative, 2021 Report to Congress on China's WTO Compliance (February 2022), 48-49.

139. Lee J. Tiedrich, Gregory S. Discher, Fredericka Argent & Daniel Rios, *10 Best Practices for Artificial Intelligence-Related Intellectual Property*, 32 Intell. Prop. & Tech. L. J. 7, 1, 4 (2020); Paul Keller & Alexis Wilpon, *Obstacles in the Road: The Multi-Faceted Approach to IP Protection in the Autonomous Vehicle Sector*, 1 Robotics, Artificial Intelligence & L. 357, 368 (2018).

140. TSD, Article 3(1)(a); 18 U.S.C. § 1839, (6)(B); Trade Secrets (ALM) § 6.02.

141. Meyers, *supra* note 13, at 3.

142. Charles Cronin, *Lost and Found: Intellectual Property of the Fragrance Industry; From Trade Secret to Trade Dress*, 5 NYU J. Intell. Prop. & Ent. L. 256, 264 (2015).

143. Katyal, *supra* note 101, at 1215.

144. In addition, the structure of such data sets may be protected under copyright law.

145. Nicholson Price II, *supra* note 29, at 430.

146. *See ClearOne Communs., Inc. v. Bowers*, 643 F.3d 735, 754 (2011).

147. Prange & Lawson, *supra* note 4, at 37.

148. Meyers, *supra* note 13, at 5.

149. *Altavion, Inc. v. Konica Minolta Systems Laboratory, Inc.*, 226 Cal. App. 4th 26, 57; *ClearOne Communs., Inc. v. Chiang*, 608 F. Supp. 2d 1270, 1278-81 (2009); Keller & Wilpon, *supra* note 139, at 362.

150. Prange & Lawson, *supra* note 4, at 38.

151. Kop, *supra* note 12, at 319.

152. Ma & Yang, *supra* note 134, at 65.

153. Keller & Wilpon, *supra* note 139, at 357.

154. Kop, *supra* note 12, at 319.

155. 35 U.S.C. § 101.

156. 35 U.S.C. §§ 101, 171.

157. *Alice Corp. v. CLS Bank International*, 573 U.S. 208, at 216 (2014); *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, at 71 (2012).

158. Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. 50 (January 7, 2019), 52.

159. *Gottschalk v. Benson*, 409 U.S. 63, at 68 (1972).

160. European Patent Office, Guidelines for Examination, G.3.3, available at https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm.

161. Kang Quan, *What Are the Chinese Examination Standards for AI-Related Inventions?*, Managing Intell. Prop. (August 20, 2020), available at https://www.managingip.com/article/b1n06p9symf6mt/what-are-the-chinese-examination-standards-for-ai-related-inventions.

162. Keller & Wilpon, *supra* note 139, at 364-65.

163. Tiedrich et al., *supra* note 139, at 1.

164. SYNCED, *Tsinghua AI Report: China Applied for 389,571 AI Patents in the Past 10 Years* (January 25, 2021), available at https://syncedreview.com/2021/01/25/tsinghua-ai-report-china-applied-for-389571-ai-patents-in-the-past-ten-years/.

165. Georgia Leopold, *China Dominates AI Patent Filings* (August 31, 2020), available at https://www.enterpriseai.news/2020/08/31/china-dominates-ai-patent-filings/.

166. U.S. Patent and Trademark Office, *Public Views on Artificial Intelligence and Intellectual Property Policy*, *supra* note 19, at i-iii.

167. 35 U.S.C. § 102-3.

168. Prange & Lawson, *supra* note 4, at 35.

169. Keller & Wilpon, *supra* note 139, at 362; Katyal, *supra* note 101, at 1213.

170. TRIPS, Article 33.

171. Keller & Wilpon, *supra* note 139, at 365; Meyers, *supra* note 13, at 5; Katyal, *supra* note 101, at 1212; Jordana Balsam, *Booming Business and the Resulting Trade Secrets: How the Increase in United States and European Union Trade Led to Resulting Trade Secrets Directives and the Domination of the Intellectual Property Field*, 2 Int'l Comp., Policy & Ethics L. Rev. 503, 515 (2019).

172. Tiedrich et al., *supra* note 139, at 3.

173. Jane C. Ginsburg, Overview of Copyright Law, Oxford Handbook of Intellectual Property Law, 4 (Rochelle Dreyfuss & Justine Pila, eds., 2018,

Oxford University Press) (Columbia Public Law Research Paper No. 14-518, 2016).

    174. Case C-5/08, *Infopaq International A/S v. Danske Dagblades Forening* [2009] ECR I-6569.

    175. *Feist Publ'ns Inc v. Rural Tel Serv Co.*, 499 U.S. 340, 345 (1991).

    176. Keller & Wilpon, *supra* note 139, at 367; Ginsburg, *supra* note 173, at 4.

    177. Kop, *supra* note 12, at 301.

    178. TRIPS, Article 9 (2).

    179. TRIPS, Article 10(1); Keller & Wilpon, *supra* note 139, at 367.

    180. Katyal, *supra* note 101, at 1195.

    181. *Id.*, at 1192.

    182. *Id.*, at 1208.

    183. TRIPS, Article 10(2); Tiedrich et al., *supra* note 139, at 3.

    184. Directive 96/9/EC of March 11, 1996, on the legal protection of databases, Article 7 (1).

    185. Directive 96/9/EC of March 11, 1996, on the legal protection of databases.

    186. Margaret J. Radin, *Regime Change in Intellectual Property: Superseding the Law of the State with the "Law" of the Firm*, 1 University of Ottawa Law & Tech. J. 173, 175 (2004).

    187. Katyal, *supra* note 101, at 1196.

    188. Keller & Wilpon, *supra* note 139, at 367.

    189. Katyal, *supra* note 101, at 1208.

    190. Bill Donahue, *6 Things to Know About High Court's Google-Oracle Ruling*, Law360 (April 5, 2021).

    191. Bill Donahue, *Copyright Cases to Watch in 2021*, Law360 (January 3, 2021).

    192. *Google LLC v. Oracle Am., Inc.*, 2021 U.S. 1864, 11-36.

    193. Application programming interfaces essentially divide computing tasks in specific ways that are useful for future programmers in building certain functions in new programs. *See Google LLC v. Oracle Am., Inc.*, 2021 U.S. 1864, 12-14.

    194. Donahue, *supra* note 190.

    195. Donahue, *supra* note 190; Smith & Mann, *supra* note 98, at 242.

    196. Donahue, *supra* note 190.

    197. Katyal, *supra* note 101, at 1196.

    198. Keller & Wilpon, *supra* note 139, at 368.

    199. *Lariscey v. United States*, 949 F.2d 1137, 1141 (Fed. Cir. 1991); Trade Secrets (ALM) § 1.02, (8)(d).

    200. Trade Secrets (ALM) § 1.02, (8)(d).

    201. *ConFold Pacific, Inc. v. Polaris Industries, Inc.*, 433 F.3d 952, 958-959 (7th Cir. 2006). Compare to Case T-201/04, *Microsoft Corp. v. Commission of the European Communities* [2007] ECR 2007 II-03601, at 289: "It follows

330 of 38

from the foregoing considerations that … the protocols in question, or the specifications of those protocols, are covered by intellectual property rights or constitute trade secrets and that those secrets must be treated as equivalent to intellectual property rights."

202. Charles T. Graves, *Trade Secrets as Property: Theory and Consequences*, 15 J. Intell. Prop. L. 39, 41 (2007).

203. *Id.*, at 45.

204. Mark A. Lemley, *Review of Romantic Authorship and the Rhetoric of Property (Book Review Shamans, Software, and Spleens: Law and the Construction of the Information Society, by James Boyle)*, 75 Tex. L. Rev. 873 (1997), 895-896.

205. *Id.*, at 898.

206. Radin, *supra* note 186, at 178.

207. Lothar Determann, *No One Owns Data*, 70 Hastings L.J. 1 (2018), 35.

208. *ConFold Pacific, Inc. v. Polaris Industries, Inc.*, 433 F.3d 952, 958-59 (7th Cir. 2006); Margaret J. Radin, Cyberpersons, *Propertization and Contract in the Information Culture: A Comment on Information Propertization and its Legal Milieu*, 54 Clev. St. L. Rev. 23, 30-31 (2006).

209. *Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp.*, 174 F.3d 1036 (9th Cir. 1999); Radin, *supra* note 208, at 31-33.

210. Radin, *supra* note 208, at 35.

211. *Ethically Aligned Design*, *supra* note 11, at 227, 229, and 248; Hagemann & Leclerc, *supra* note 11, at 2; Meyers, *supra* note 13, at 9; Villasenor & Foggo, *supra* note 12, at 343; Huseinzade, *supra* note 12.

212. Meyers, *supra* note 13, at 9.

213. Villasenor & Foggo, *supra* note 12, at 343.

214. Kramer, *supra* note 107. It should be noted, however, that a lack of empirical analysis causes debate as to whether there truly is a perceivable causal link between trade secrecy and the stimulation of innovation (see Levine & Seaman, *supra* note 107, at 108).

215. *See* Coglianese, *supra* note 12, at 46-47.

216. *Ethically Aligned Design*, *supra* note 11, at 248.

217. Google, *Building a responsible regulatory framework for AI*, 4, available at https://ai.google/static/documents/building-a-responsible-regulatory-framework-for-ai.pdf (last visited on September 18, 2021).

218. Coglianese, *supra* note 12, at 46.

219. Rudin, *supra* note 87.

220. For example, the IEEE published a *Draft Standard for Transparency of Autonomous Systems* on June 9, 2021, available at https://ieeexplore.ieee.org/document/9451892.

221. *Ethically Aligned Design*, *supra* note 11, at 251-52.

222. EU Draft AI Act, Article 70 (1); EU Draft AI Act (Explanatory Memorandum), 11.

223. *Id.*

224. *Ethically Aligned Design*, *supra* note 11, at 251.

225. *Id.*, at 249.

226. Sandra Wachter, Brent Mittelstad & Chris Russell, *Counterfactual explanations without opening the black box: Automated decisions and the GDPR*, 31 Harv. JL & Tech. 2, 841, 882-83 (2017).

227. Coglianese, *supra* note 12, at 54.

228. Huseinzade, *supra* note 12.

229. Décret n° 2017-330 du 14 mars 2017 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique, Article R.311-3-1-2.

230. Décision n° 2018-765 DC du 12 juin 2018 (Conseil d'État): *"Il en résulte que, lorsque les principes de fonctionnement d'un algorithme ne peuvent être communiqués sans porter atteinte à l'un des secrets ou intérêts énoncés au 2 ° de l'article L. 311-5 du code des relations entre le public et l'administration, aucune décision individuelle ne peut être prise sur le fondement exclusif de cet algorithme."*

231. Huseinzade, *supra* note 12.

232. EU Draft AI Act (Explanatory Memorandum), 11.

233. Under Article 1(2)(b) TSD, the need to disclose trade secrets to public authorities for reasons of public interest shall not be affected. Under Article 5(d) TSD, the disclosure of a trade secret is not illegal for the purpose of protecting a legitimate interest recognized by Union or national law.

234. Coglianese, *supra* note 12, at 54.

235. *State v. Loomis* 881 N.W.2d 749 (Wis. 2016), at 770; Coglianese, *supra* note 12, at 54.

236. Coglianese, *supra* note 12, at 54.

237. Villasenor & Foggo, *supra* note 12, at 344. However, the authors note that compliance with protective orders can be financially prohibitive for many defendants.

238. McCarthy, *supra* note 36.

Bibliography

Treaties, Legislation, and Legislative Proposals

Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) (as amended on January 23, 2017).

Regulation (EU) 2016/679 of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Directive (EU) 2016/943 of June 8, 2016, on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

Directive 96/9/EC of March 11, 1996 on the legal protection of databases.

Defend Trade Secrets Act of 2016.

Anti-Unfair Competition Law of the People's Republic of China (2019 Amendment).

Décret n° 2017-330 du 14 mars 2017 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique.

European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (April 21, 2021) COM(2021) 206 final 2021/0106 (COD).

Uniform Law Commission, Uniform Trade Secrets Act of 1979.

Judicial Decisions

Alice Corp. v. CLS Bank International, 573 U.S. 208 (2014).

Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66 (2012).

Gottschalk v. Benson, 409 U.S. 63 (1972).

Diamond v. Diehr, 450 U.S. 175 (1981).

Feist Publ'ns Inc v. Rural Tel Serv Co, 499 U.S. 340 (1991).

Lariscey v. United States, 949 F.2d 1137 (Fed. Cir. 1991).

ClearOne Communs., Inc. v. Bowers, 643 F.3d 735 (Fed. Cir. 2011).

ClearOne Communs., Inc. v. Chiang, 608 F. Supp. 2d 1270 (Fed. Cir. 2009).

ConFold Pacific, Inc. v. Polaris Industries, Inc., 433 F.3d 952 (7th Cir. 2006).

Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp., 174 F.3d 1036 (9th Cir. 1999).

Altavion, Inc. v. Konica Minolta Systems Laboratory, Inc., 226 (Cal. App. 4th 26).

State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

Case C-5/08, *Infopaq International A/S v. Danske Dagblades Forening* [2009] ECR I-6569.

Case T-201/04, *Microsoft Corp. v. Commission of the European Communities* [2007] ECR 2007 II-03601.

Décision n° 2018-765 DC du 12 juin 2018 (Conseil d'État).

Literature

Books

Trade Secrets (ALM).

1 Milgrim on Trade Secrets (2020).

Fisch, Michael, Empirical Methods in Trade Secret Research in Peter S. Menell & David L. Schwartz (eds.), Research Handbook on the Economics of Intellectual Property Law (Vol. II—Analytical Methods), Villanova Law/Public Policy Research Paper No. 2015-1021.

Ginsburg, Jane C., Overview of Copyright Law, Oxford Handbook of Intellectual Property Law, Rochelle Dreyfuss & Justine Pila, Eds., Oxford University Press, 2018; Columbia Public Law Research Paper No. 14-518 (2016),

Russell, Stuart J. & Norvig, Peter, Artificial Intelligence. A Modern Approach, Prentice Hall (1995).

Simensky, Mevin, Bryer, Lanning, & Wilkof, Neil J., Intellectual Property in the Global Marketplace, Vol. 1: Electronic Commerce, Valuation, and Protection, 2d ed. (1999), John Wiley & Sons, New York.

Articles

Balsam, Jordana, Booming Business and the Resulting Trade Secrets: How the Increase in United States and European Union Trade Led to Resulting Trade Secrets Directives and the Domination of the Intellectual Property Field, 2 Int'l Comp., Policy & Ethics L. Rev. 503 (2019).

Brownlee, Jason, A Gentle Introduction to General Adversarial Networks (June 17, 2019), available at https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/ (last visited on April 23, 2021).

Clarke, Laurie, The EU's Leaked AI Regulation Is Ambitious But Disappointingly Vague, Techmonitor (April 15, 2021), available at https://techmonitor.ai/policy/eu-ai-regulation-machine-learning-european-union (last visited on April 20, 2021).

Clegg, Nick & Presenti, Jerome, Collaborating on the future of AI governance in the EU and around the world (June 15, 2020), available at https://ai.facebook.com/blog/collaborating-on-the-future-of-ai-governance-in-the-eu-and-around-the-world/ (last visited on April 15, 2021).

Coglianese, Cary, A Framework for Governmental Use of Machine Learning (December 8, 2020) (report to the Admin. Conf. of the U.S.), 46, available at https://www.acus.gov/sites/default/files/documents/Coglianese%20ACUS%20Final%20Report.pdf (last visited on April 26, 2021).

Coyne, Patrick, What You Should Know About the Defend Trade Secrets Act, Law360 (June 27, 2016).

Cronin, Charles, Lost and Found: Intellectual Property of the Fragrance Industry; From Trade Secret to Trade Dress, 5 NYU J. Intell. Prop. & Ent. L. 256 (2015).

Davis, Lauren, Note: Secrecy for the Sake of It: The Defend Trade Secrets Act. A Devolving Global Market Based on the Legal Protection of Over-Secrecy, 83 Brooklyn L. Rev. 359 (2017).

Determann, Lothar, No One Owns Data, 70 Hastings L.J. 1 (2018).

Donahue, Bill, 6 Things to Know About High Court's Google-Oracle Ruling, Law360 (April 5, 2021).

Fagan, Aimee, Trade Secret Litigation Now An Attractive Alternative to Patent Litigation, Law.com (March 23, 2021), available at https://www.law.com/texaslawyer/2021/03/03/trade-secret-litigation-now-an-attractive-alternative-to-patent-litigation/ (last visited on April 28, 2021).

Flowers, M. Claire, Facing the Inevitable: The Inevitable Disclosure Doctrine and the Defend Trade Secrets Act of 2016, 75 Wash & Lee L. Rev. 2207 (2018).

Graves, Charles, T., Trade Secrets as Property: Theory and consequences, 15 J. Intell. Prop. L. 39 (2007).

Hagemann, Ryan & Leclerc, Jean-Marc, Precision Regulation for Artificial Intelligence, IBM Pol'y Lab (January 21, 2020).

Huseinzade, Nazrin, Algorithm Transparency: How to Eat the Cake and Have It Too, European Law Blog (January 27, 2021), available at https://europeanlawblog.eu/2021/01/27/algorithm-transparency-how-to-eat-the-cake-and-have-it-too/ (last visited on April 26, 2021).

Katyal, Sonia K., The Paradox of Source Code Secrecy, 104 Cornell L. Rev. 1183 (2019).

Keller, Paul & Wilpon, Alexis, Obstacles in the Road: The Multi-Faceted Approach to IP Protection in the Autonomous Vehicle Sector, 1 Robotics, Artificial Intelligence & L. 357 (2018).

Kop, Mauritz, AI & Intellectual Property: Towards an Articulated Public Domain, 28 Tex. Intell. Prop. L.J. 297 (2020).

Kramer, Alexis, Trade Secret Cases Surge as Race for New Tech, Top Talent Heats Up, Bloomberg BNA (May 10, 2017).

Lemley, Mark A., Review of Romantic Authorship and the Rhetoric of Property, Shamans, Software, and Spleens: Law and the Construction of the Information Society. By James Boyle, Cambridge: Harvard University Press, 1996, pp. xvi, 270, 75 Tex. L. Rev. 873 (1997).

Leopold, Georgia, China Dominates AI Patent Filings (August 31, 2020), available at https://www.enterpriseai.news/2020/08/31/china-dominates-ai-patent-filings/ (last visited on April 11, 2021).

Levine, David S. & Seaman, Christopher B., The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act, 53 Wake Forest L. Rev. 105 (2018).

Linardatos, Pantelis, Papastefanopoulos, Vasilis & Kotsiantis, Sotiris, *Explainable AI: A Review of Machine Learning Interpretability Methods*, 1 Entropy 23, 18 (2021), available at https://doi.org/10.3390/e23010018

Ma, Youping & Yang, Guoquan, Are Trade Secrets an Alternative Way to Protect AI, 283 Managing Intell. Prop. 63 (2019).

McCarthy, Mark, AI Needs More Regulation, Not Less, The Brookings Institution Artificial Intelligence and Emerging Technology Initiative (March 9, 2020).

Menell, Peter S., Symposium: Toward a Third Intellectual Property Paradigm: Comments: the Challenges of Reforming Intellectual Property Protection for Computer Software, 94 Colum. L. Rev. 2644 (1994).

Meyers, Jessica M., Artificial Intelligence and Trade Secrets, 11 Landslide 17 (2019).

Mueller, Benjamin, *How Much Will the Artificial Intelligence Act Cost Europe?*, Information Technology & Innovation Foundation (July 26, 2021), available at https://itif.org/publications/2021/07/26/how-much-will-artificial-intelligence-act-cost-europe.

Prange, David A. & Lawson, Alyssa N., Re-Evaluating Companies' AI Protection Strategies, 272 Managing Intell. Prop. 35 (2018).

Price II, Nicholson, Regulating Black-Box Medicine, 116 Mich. L. Rev. 421 (2017).

Quan, Kang, What Are the Chinese Examination Standards for AI-Related Inventions?, Managing Intell. Prop. (August 20, 2020).

Radin, Margaret J., Regime Change in Intellectual Property: Superseding the Law of the State with the "Law" of the Firm, 1 University of Ottawa Law & Tech. J. 173 (2004).

Radin, Margaret J., Cyberpersons, Propertization and Contract in the Information Culture: a Comment on Information Propertization and its Legal Milieu, 54 Clev. St. L. Rev. 23 (2006).

Rudin, Cynthia & Radin, Margaret Joanna, Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From an Explainable AI Competition, Harvard Data Science Review (November 22, 2019).

Rudin, Cynthia, Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead, Nature Machine Intelligence (2019), 1(5).

Saif, Irfan & Ammanath, Beena, "Trustworthy AI" is a framework to help manage unique risk, MIT Tech. Rev. (2020).

Scoolidge, Peter & Weg, Jasmine, U.S. Artificial Intelligence Regulation Has a Long Way to Go, Law360 (May 10, 2019).

Segate, Ricardo V., Securitizing Innovation to Protect Trade Secrets Between "the East" and "the West": A Neo-Schumpeterian Public Legal Reading, UCLA Pac. Basin L.J. 59 (2020).

Smith, Bradfod L. & Susan O., Innovation and Intellectual Property Protection in the Software Industry: An Emerging Role for Patents?, 71 U. Chi. L. Rev. 241 (2004).

Thiebes, Scott, Lins, Sebastian & Sunyaev, Ali, Trustworthy Artificial Intelligence, Electronic Markets (October 1, 2020).

Tiedrich, Lee, Jungyun Choi, Sam & Yoon, James, NIST Solicits Comments on Four Principles of Explainable Artificial Intelligence and Other Developments, 4 Robotics, Artificial Intelligence & L. 29 (2021).

Tiedrich, Lee, Discher, Gregory S., Argent, Fredericka & Rios, Daniel, 10 Best Practices for Artificial Intelligence-Related Intellectual Property, Intell. Prop. & Tech. L. J., Vol. 32, No. 7 (2020).

Thomas, Rob, AI in 2020: From Experimentation to Adoption (January 3, 2020), IBM Think Blog.

Veale, Michael & Borgesius, Frederik Z., *Demystifying the Draft EU Artificial Intelligence Act*, 22 Computer Law Review International 4, 917 (2021).

Villasenor, John & Foggo, Virginia, Artificial Intelligence, Due Process and Criminal Sentencing, 2020 Mich. St. L. Rev. 295 (2020).

Vorhies, William, Artificial general intelligence—the Holy Grail of AI, DataScienceCentral.com (February 23, 2016), available at https://www.data sciencecentral.com/profiles/blogs/artificial-general-intelligence-the-holy-grail-of-ai (last visited April 25, 2021).

Wachter, Sandra, Mittelstad, Brent & Russell, Chris, Counterfactual explanations without opening the black box: Automated decisions and the GDPR, Harv. J. L & Tech., 31 (2017).

Reports, Surveys and Other Sources

OECD, Recommendation of the Council on Artificial Intelligence (May 21, 2019).

G20 Ministerial Statement on Trade and Digital Economy (June 2019).

Executive Office of the President (Office of Management and Budget), Memorandum for the Heads of Executive Departments and Agencies. Guidance for Regulation of Artificial Intelligence Applications (November 17, 2020).

U.S. Patent and Trademark Office, Public Views on Artificial Intelligence and Intellectual Property Policy (October 2020).

Department of Commerce, United States Patent and Trademark Office [Docket No. PTO–P–2018–0053] 2019 Revised Patent Subject Matter Eligibility Guidance, Fed. Reg. Vol. 84 No. 4 (January 7, 2019).

U.S. Trade Representative, 2021 Report to Congress on China's WTO Compliance (February 2022).

U.S. Food & Drug Administration, Executive Summary for the Patient Engagement Advisory Committee Meeting. Artificial Intelligence (AI) and Machine Learning (ML) in Medical Devices (October 2020).

National Institute of Standards and Technology, Four Principles of Explainable Artificial Intelligence, DRAFT NISTIR Interagency or Internal Report 8312 (August 2020).

Independent High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI (April 8, 2019).

European Patent Office, Guidelines for Examination, G.3.3, available at https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm.

House of Lords Liaison Committee, AI in the UK: No Room for Complacency, 7th Report of Session 19-21 (December 18, 2020).

Chinese National New Generation Artificial Intelligence Governance Committee, New Generation AI Governance Principles—Developing Respon-

sible AI (June 17, 2020), *see* http://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html (last visited on April 15, 2021).

IBM & Morning Consult, From Roadblock to Scale: The Global Sprint Towards AI. Executive Summary (2020).

Google's "Explainable AI," available at https://cloud.google.com/explainable-ai.

McKinsey & Company, Notes From the AI Frontier. Modeling the Impact of AI on the World Economy, McKinsey Global Institute (September 2018)

Asgard Capital Verwaltung GmBH & Roland Berger GmBH, Artificial Intelligence—A Strategy for European Startups. Recommendations for Policymakers (2018).

Rome Call for AI Ethics (February 28, 2020), available at https://www.romecall.org/ (last visited on April 16, 2021).

Future of Life Institute, 2017 Asilomar AI Principles, available at https://futureoflife.org/ai-principles/ (last visited on April 15, 2021).

Institute of Electrical and Electronics Engineers, The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, Ethically Aligned Design, First Edition (2019).

SYNCED, Tsinghua AI Report: China Applied for 389,571 AI Patents in the Past 10 Years (January 25, 2021), available at https://syncedreview.com/2021/01/25/tsinghua-ai-report-china-applied-for-389571-ai-patents-in-the-past-ten-years/ (last visited on April 11, 2021).

Keidanren (Japanese Business Federation), AI Utilization Strategy Taskforce, Committee on Digital Economy, *Opinions on the Proposed European Artificial Intelligence Act* (August 6, 2021), available at https://www.keidanren.or.jp/en/policy/2021/069.html.

Zhang, Daniel, Mishra, Saurabh, Brynjolfsson, Erik, Etchemendy, John, Ganguli, Deep, Grosz, Barbara, Lyons, Terah, Manyika, James, Niebles, Juan Carlos, Sellitto, Michael, Shoham, Yoav, Clark, Jack & Perrault, Raymond, The AI Index 2021 Annual Report, AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA (March 2021).