TRADE SECRETS AS A SUBSTITUTE FOR AI PROTECTION: A CRITICAL INVESTIGATION INTO DIFFERENT DIMENSIONS OF TRADE SECRETS

Ahmed Raza

LLM Scholar Penn State Dickinson Law Pennsylvania State University, United States

ahmedraza.sajjad@gmail.com; aqr6275@psu.edu

Corresponding Author: *

DOI: <u>https://doi.org</u>	/10.5281/zenodo.151089	33	
Received	Revised	Accepted	Published
17 August, 2024	17 September, 2024	10 October, 2024	15 October, 2024

ABSTRACT

With the rapid and continuous growth of Artificial Intelligence (AI) technologies, protecting the intellectual property rights of AI inventions has become a critical concern for developers and innovators, seeking to maintain a competitive edge. Nevertheless, due to novelty and complexity of these innovations, conventional measures of intellectual property protection including copyrights and patents, have become ineffective. Under these circumstances, trade secrets offer an effective substitute or alternative tool for safeguarding AI technologies. Protecting proprietary information that gives a company a competitive edge, trade secrets provide a way for safeguarding AI discoveries without any restrictions that are otherwise imposed by copyrights and patents. In this way, trade secrets, unlike patents, does not demand public disclosure of an invention in return for protection. This article delves into the complexities of trade secret protection, exploring its legal principles, ethical challenges, and the evolving technological landscape shaping its application. Finally, through critical assessment of trade secrets' value in the context of artificial intelligence, it highlights the gaps in present legal frameworks and suggests possible legal remedies. *Keywords:* Artificial Intelligence, Trade Secrets, Intellectual Property, Legal Protection, AI Innovation, AI ethics

INTRODUCTION

Artificial intelligence (AI) technologies, once the province of science fiction, are rapidly transforming industries, economies and everyday life. From revolutionizing banking with predictive analytics and auto trading systems to healthcare with diagnostics from deep learning algorithms, AI has emerged as a catalyst of new ideas in a number of fields. With these potential benefits, its rapid growth and deployment has given birth to several challenges as well. One of these concern is about the effective protection of the intellectual property (IP) associated with artificial intelligence systems. The protections should not only protect the competitive egde of enterprise and producer, but also ensure the benefits derived from these efforts are fairly recognized and compensated, which will drive more innovation (Smith et al., 2018).

Patents, copyrights, and other traditional IP protection mechanisms have historically been used to protect rights of inventors and creators. However. these traditional frameworks, meanwhile, failing are to accommodate the complexity of AI-related inventions. The very nature of artificial intelligence-its ability to rapidly learn, develop, and generate new concepts-poses unique challenges to traditional intellectual property frameworks, which are typically ill-equipped to keep up with the speed and scale of AI innovation. Patents, for instance, require public disclosure of an invention in exchange for exclusive rights,



making it difficult to protect the most sensitive parts of artificial intelligence, such as training data or proprietary algorithms, without risking the loss of competitive advantage. Similarly, copyright protects fixed expressions of ideas such as software codes and does not cover the functional or algorithmic nature of artificial intelligence systems. Encrypted intellectual properties hold serious inadequacies specifically in protecting the artificial intelligence technologies in the crucial industries where the stages of innovation are rapid and out of sight. In light of these limitations, trade secrets have emerged as a remarkable alternative or addition to traditional IP safeguards. In contrast to patents, a trade secret is characterized as a confidential business information with a competitive advantage that is not disclosed for public. This quality is particularly attractive for protecting AI innovations as it enables companies to preserve the secrecy of key elements such as algorithms, models and datasets for as long as they desire to maintain it.

These substantial benefits of trade secrets does not come without challenges and limitations. Trade secrecy can be tricky to maintain over long periods, particularly in fields where information is where constantly circulating and those technologies could potentially be reverse engineered or uncovered using data mining techniques. However, trade secrets are still enforceable so long as the stakeholders take reasonable steps to keep the information confidential, but such bounds are increasingly difficult to uphold in the face of modern technological interconnectedness. Legal frameworks and the moral implications of protecting AI technology through trade secrets must be examined at length. This article provides in-depth assessment of advantages and disadvantages of trade secrets in protecting Artificial Intelligence bv considering characteristics of AI systems in their development processes. Trying to find out how existing systems could be amended or improved to accommodate the needs of artificial intelligence developers, it also examines the legal, ethical, and technological factors that impact trade secret protection. Finally, the article evaluates the efficacy of trade secrets in protecting artificial intelligence technologies and recommends potential solutions to resolve existing regulatory gaps.

- Trade Secrets in the context of AI technologies: A comprehensive analysis of its functions
- The definition and scope of trade secrets

Trade secrets are a form of intellectual property that is, proprietary business knowledge or practices that lend an organization a competitive advantage. Trade secrets are defined largely by secrecy: the holder of the knowledge has to make reasonable efforts to keep it confidential, and the material has to be generally unknown or inaccessible to others. Trade secrets include manufacturing techniques, recipes, customer lists, sales strategies, software codes, algorithms, and models of machine learning etc. Although jurisdiction specifies its legal framework for trade secrets, generally speaking, trade secret protection is accorded to information deemed commercially significant because of its confidentiality. Legal protection depends on the holder's efforts to keep the material under confidence. Trade secret theft can result in civil lawsuits as well as in some jurisdictions with criminal penalties.

• The evolution of trade secrets: The birth Trade secret law in USA

A trade secret, is knowledge where reasonable are protections maintained to preserve confidentiality and which provides а competitive advantage. Trade secrets are welltechnologies suited for that cannot he independently discovered or reverse engineered, mainly the technologies that are obsolete by time they hit the market. Trade secrets have always been the lifeblood of protecting that competitive corporate information-even if no one seems to agree as to how trade secret law even began. Trade secrets can protect everything from nontechnical information, such as client lists, marketing strategies and sales tactics, to technical information and product designs. Trade secrets are addressed to almost any information provided that this information offers a competitive advantage. However, knowledge of the person or talents or abilities of an employee cannot be protected by trade secret.

Although patents, copyrights, and trademarks were secured within the confines of federal statutes, trade secrets lagged behind in IP protections, in both state-specific statutes and common law. Notwithstanding, trade secret law has witnessed immense development in United



States. In the United States, the 2016 Defend Trade Secrets Act (DTSA) specifically created a federal civil cause of action for trade secret theft, thus harmonizing trade secrets with other intellectual property rights (18 U.S. Code § 1836 -Civil Proceedings,). This federal law was introduced to provide a more efficient and rational means for an aggrieved trade secret owner to pursue infringers. By that time, reports of trade secret theft were at an all-time high (often by current or former employees), and were a major factor influencing Congress in drafting the DTSA. These violation of trade secrets were resulting in the loss of hundreds of millions of dollars, and the setback of millions of jobs (Cannan, 2017). The exact cost of trade secret theft is hard to calculate because it is relatively opaque and undetectable – a company may not discover that knowledge has been stolen for years. It is, moreover, nearly impossible to establish the monetary value of knowledge. Therefore, while accusing an employee, business partner, or competitor of trade secret misappropriation certainly carries reputational and relational risks of its own, a company must protect its trade secret for its own survival (Yeh & Congressional Research Service, 2016)

• The theft of trade secrets and International regulations

Article 39 of the 1995 Trade-Related Aspects of Intellectual Property Rights (TRIP) Agreement deals with trade secrets. Though the term "trade secret" is never mentioned, the agreement protects "undisclosed information," which is defined similarly to trade secrets. While the members of the World Trade Organisation are, as a matter of law, required to provide trade secret protection under the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), the effectiveness and enforcement of these laws, especially in the large developing economies like China, India and Brazil have been an issue for long (Yeh & Congressional Research Service, 2016). As the protection and enforcement in some countries is weak, it can have a significant negative impact on a company's efforts to protect its trade secret. In fact, in 79% of cases, the perpetrator is currently or formerly employed by the company from which the trade secrets are taken. This has been especially important in a period in which workers are frequently changing their jobs due to

shortage of labor in areas like artificial intelligence. To make matters worse, new employment models in which workers can sign contracts with multiple companies are quickly displacing the standard employment setup and so organisations must make sure that such personnel will not carry strategic business information with them (Bhalla et al., 2021).

3. The interaction of Trade secrets with other Intellectual property rights

Trade secrets offer several advantages over other types of intellectual property. From technical skills and nontechnical concepts all the way to facts - including names and phone numbers on a client list - trade secrets provide much wider coverage than the other intellectual property rights. It is not necessary for all trade secrets to be original or unique. A second difference between trade secrets and other types of intellectual property is that they are protectable without the associated costs and timelines for registering the other forms of intellectual property. In contrast to the finite terms (30 years for patents, and life plus a defined number of years for copyrights), a trade secret lasts as long as the information is commercially valuable and kept secret.

A trade secret does not confer the holder a monopoly over the subject matter of the trade secret, unlike many other forms of intellectual property rights. Its material is only guarded against theft - unauthorized acquisition, use or disclosure. Thus, once a trade secret is publicly disclosed - even if such information is disclosed inadvertently it gives the _ up character/descriptive terminology of a trade secret. Not registering also carries consequences. Without formal registration, trade secrets are hard to define in most cases. On the other hand, opponents criticise the non-inventiveness of trade secrets, arguing that the appropriateness of paying owners to keep secret information should be closely scrutinized if it lacks originality or creativity (Moser, 2007)⁻

At first glance, trade secrets and patents are an odd couple. Trade secrets depend on nondisclosure; patents depend on disclosure. Trade secrets and patents, by contrast, can be "intensively" and "complementarily" exploited. A patent, for example, might cover a novel invention and trade secrets might cover the research results, know-how and data sets behind



the idea. Trade secrets can be especially beneficial before and after the patent is filed. Even negative results, data demonstrating the failure of some tech innovation, are trade secrets up until the patent application is filed. After the patent application, even a superior technology developed during the Research and Development activity is protected as trade secrets in the form of proprietary know-how. However the period of time for which they are kept as trade secrets, in case the advances are not revealed in patent filings, is still questionable.

4. The limitations of conventional intellectual property protections for Artificial Intelligence

Usually, trade secrets cover more general topic than other intellectual property rights. Undoubtedly, patent strategy affects trade secrets. In fact, opinions about the efficiency of the patent system could influence the trade secret demand. Trade secrets could be perceived as more appealing as patents are judged less effective and vice versa. Companies are thinking about different approaches in the current climate. Considering the nature of artificial intelligence technologies, the patent deal might not be optimal. While the corporation might never be able to find out whether a competitor is using the revealed technique, a patent application demands that the invention be fully detailed. Like any technology, artificial intelligence can be safeguarded using a variety of intellectual property assets-patents, copyrights, trademarks, trade secrets. This enables the covering of the widest possible subject matter, in which case some IP assets protect categories of subject matter excluded by other assets are covered. Moreover, several asset kinds increase the spectrum of remedies accessible in a conflict or lawsuit and offer extra protection should one of the assets prove invalid. Should a corporation choose trade secret from among several IP assets at hand?

Generally speaking, trade secrets are best suited for technologies that cannot be reverse engineered or independently developed without difficulty. It refers to technologies that cannot be defined without advancing significant effort. In this context, AI technologies are well suited for trade secret protection. Still, the calculus could change with time. For instance, although artificial intelligence technology could be difficult to identify now, future technological advancements could help detection. As rivals' reverse engineering skills rise, businesses can decide to patent instead of keeping trade secrets. The same effect could be experienced when technological advancement in artificial intelligence gets less complicated and as its acceleration slows down.

5. Legal and Operational Obstacles in Safeguarding AI through Trade Secrets

Although trade secrets provide AI with great protection, keeping and enforcing confidentiality presents various difficulties:

• Danger of Reverse Engineering and Access for contractor and employees

If AI models are made public, they can be reverseengineered especially in software or machine learning applications. Once an artificial intelligence model is put into operation, rivals could try to reverse-engineer the model or reproduce the results using like inputs. Secondly, maintaining confidentiality calls for tight internal controls to restrict access to private AI-related data. Contractor and employee access is thus limited. Businesses have to make sure staff members and contractors know their responsibilities with relation to trade secrets and sign non-disclosure agreements (NDAs).

• Global Concerns regarding IP laws and the issue of transparency

Trade secret protection gets more difficult given the worldwide development of artificial intelligence. Laws on trade secret protection vary among nations; so, protecting trade secret rights globally can be challenging, particularly in areas with poor IP enforcement. Considering the issue of transparency, Trade secrets might at times restrict openness, especially in sectors like banking or healthcare where artificial intelligence algorithms are applied to make high-stake decisions. The absence of public disclosure of algorithms begs issues regarding bias in artificial intelligence decision-making, justice, and responsibility.

• The issue of "Black Box" Puzzle

Many artificial intelligence systems, particularly deep learning models, function as "black boxes," in which case human understanding of the decision-making process is not readily clear.



Particularly when trade secrets hide the operations of important artificial intelligence technology, this lack of comprehension raises ethical questions regarding the fairness and transparency of AI systems.

6. Trade secrets and the horizon of their protection

First of all, businesses have to determine the proprietary data they want to safeguard, then create and carry out acceptable policies to guarantee continuous confidentiality. Such policies might include physical barriers (e.g., fences, walls, locks, and security guards), technical elements (e.g., encryption and passwords), staff access, and confidentiality agreements. Furthermore, the trade secret information retained should regularly be audited and modified as fresh confidential information is obtained and unwanted information is discarded. Moreover, trade secrets and artificial intelligence are not the kind of technological problems that exist in a vacuum. They reside in a legal and social realm subject to rules of justice, privacy and other safeguards.

7. AI technologies, Trade Secret Laws and the question of creativity

Although it is argued that trade secrets stifle innovation, it becomes particularly debatable when it comes to A.I. technology. This might be illegal under trade secret law which could be contrary to patent and copyright law and thus incentivize invention disclosure (Lemley, 2011). Such sharing allows people to circumvent or extend one another's creations and thereby keep advancing. If knowledge has to be concealed instead, then this virtuous loop is interrupted. Many companies will look into the same space over and over (in many cases), so inventors cannot build in ideas that are blind. Furthermore, because trade secret protection is immediate, e.g., for research and pre-invention data; therefore, even if an innovation never proceeds to an exposition, great ideas that have the potential to enable significant discoveries may not ever be disclosed (Simpson, 2005). This is especially relevant for artificial intelligence technology, one possible implication being that the diffusion of innovation may already be beyond the pale. And it all can reduce the potential for genuine AI progress to result from investments in artificial intelligence research and development and

provide access to data sources and train people required to keep making this technology better. Others contend that trade secrets can build incentives for disclosure, and thus innovation.

Legislation like trade secrets offer protections that could supplant investments in secrecy which businesses would otherwise make. Empirical evidence indicates that companies overinvest in secrecy measures without a trade secret law (Sherwood, 2019). In countries with weak legal protection or enforcement regarding trade secrets, for instance, businesses can take business decisions that will not adequately lessen disclosure, knowing that if that knowledge is disclosed, there will be no recourse. These are not merely small physical measures - walls, fences, armed security guards. In this regard, firms may be disinclined to look to outsiders for production or development even when it would offer additional efficiency gains, if it means sharing proprietary information (Lemley, 2008). Such restrictions on this type of knowledge between prospective business partners reduce commercialization and creativity. If employees' rights are - or even seem to be – overly restricted in terms of things they create for the company, employees may, for instance, have little incentive to be more creative. In fact, when companies have overreaching IP policies - including on trade secrets - that are revealed, employees can shy away from that company in general.

8. Confidentiality of Trade Secrets and the concern regarding free mobility of employees

It is also simple to justify; when an employee resigns all confidential properties of the organization should remain, but the worker should be allowed to take, his or her (soft) skills and competencies. However, figuring out where to draw this boundary is difficult. The knowledge skill of the employee are normally and intertwined with a corporation's confidential data. After all, trade secrets cannot safeguard all the valuable intelligence gained from a job. For example, those secrets are not called trade secrets which does not include the degree to which the employee's knowledge and abilities coincide with those who work in the trade and the worker's knowledge or skills are publicly known or easily obtainable by other businesses. If an employee could not take some part of the knowledge he or she acquires during his or her career to a new



employer, the employee would effectively be barred in taking on a new job in the field in which he or she is most capable and in which he or she could earn a living (Burk & McDonnell, 2016) . Employers also have an interest in enabling employees to move freely between roles within an industry. As a result, hiring qualified workers and getting them right to work on cuttingedge advances is a key aspect of a company's competitive health. In part, the DTSA outlines employer-employee relationship. The DTSA requires that any constraint on downward mobility must have an adequate nexus to the misuse of a trade secret, and that possession of personal knowledge alone is not enough (18 U.S. Code § 1836 - Civil Proceedings). The DTSA relief, however, may not on its face violate a state statute protecting or regulating the lawful conduct of a profession or trade. Trade secret law is just one area of law that governs employee mobility. It includes rules governing, innovation work-for-hire assignments, contracts, and noncompete and non-solicitation agreements that employees and companies must follow. These factors all encourage a highly considered approach to defining trade secrets within a company (18 U.S. Code § 1836 - Civil Proceedings). The secrets play into their hands because they retain its commercial value from private data and can determine what transfer information staff will take when they leave. Trade secrets, however, do place certain restrictions on job applicants. In this context, employers may refuse to allow prospective employees to see specific work completed by a previous employee.

9. The standards of fairness and transparency in the use of Trade Secrets

Since artificial intelligence directs and sometimes takes over human decision-making, it poses unique challenges. AI informs decisions about loan eligibility, insurance coverage, medical treatments, and countless other major issues. So, if you remove or reduce the factors of human decision-making — things like bias and errors then you arrive at more objective conclusions. However, algorithms are not more fundamentally fairer than human judgement. In artificial intelligence, it often hinges on training data in getting to a decision model. Indeed, if the

training data itself is biassed or prejudicial whether intentionally or inadvertently - such training can lead to biassed results. These algorithms too depend on decisions made by developers, such as what features should be fed to a decision-making. There might be discriminative effects if certain things are included or excluded. While companies have valid interests in protecting sensitive information, including the decisionmaking process, citizens must also have protected rights to information about the fairness of how artificial intelligence algorithms are both developed and used.

The Fourteenth Amendment of US constitution procedural justice for government requires agencies' decisions about, for example, which taxpayers will be audited. In the world of artificial intelligence, that could mean that each human used the same algorithm, and that it was designed so that no single group would find itself at a disadvantage. In addition, an emerging body of privacy legislation – most prominently the European Union's General Data Protection Regulation – requires transparency around the collection, use and storage of data. Transparency is not just an abstract concept; it has practical implications. If people do not have at least a general understanding of how artificial intelligence produces recommendations or predictions, they will be less inclined to trust or use it. How does a business adhere to legal or social norms that demand transparency while protecting its proprietary data? Most will say that forcing a corporation to show its source code is neither necessary nor sufficient to prove that it is open. But it can be difficult even for technical professionals to know how source code will behave.

Many artificial intelligence algorithms naturally evolve as they are exposed to particular data and learn from that data, even if they may be explainable. By the time they are reviewed, rules based on algorithms may also be outdated. There are technical solutions, however, to track where your training data came from, describe its attributes, and to find out if it's sufficiently representative. Moreover, there are ways to ensure that A.I. systems behave as expected. Human study can also highlight areas where prejudices and blind spots may creep in. While in certain instances transparency could be appreciated, absence of any regulation in this regard creates



other problems i.e if a company or agency was required to publish a detailed account of the guidelines it uses to make decisions about individuals, including a policy that explains its reasoning behind auditing individuals, that could allow for strategic gaming of the system (Kroll et al., 2017).

10. Conclusion

With regard to secrecy, flexibility, and the span of protection, trade secrets have become a practical and ever more popular tool for safeguarding Artificial Intelligence (AI) innovations as compared to conventional intellectual property safeguards. Trade secrets, unlike copyrights or patents, do not require public disclosure, allowing Al-driven businesses to keep the privacy of their private data models, algorithms, and technology. This feature is especially helpful in sectors where if this data is revealed, the rivals might readily reverse engineer or copy them. Furthermore, trade secrets give a long-lasting kind of protection since they remain valid as long as the secret is kept private, thereby giving artificial intelligence companies an ongoing edge in the market. However, the idea of using trade secrets to protect AI is not without difficulties. Its major risk is of reverse engineering - especially in an age of quick knowledge replication and reallocation. Moreover, the application of trade secrets for the protection of AI raises significant ethical issues. Transparency, fairness and accountability are crucial principles of A.I. development – especially when A.I. systems are used in sensitive fields such as health care, criminal justice and finance. Such trade secrets may prevent the public from accessing crucial information about the use of a given artificial intelligence technology, raising concerns about fairness and accountability in relation to these systems – especially when their decisions have societal impact. This struggle to balance between transparency and secrecy remains a challenge.

The analysis leads to the conclusion that a synergy between trade secrets, patents and copyrights to form a unified and flexible infrastructure to tackle the diverse issues raised by the rapidly shifting frontier of AI, may well be the future of AI protection. This model must be developed cooperatively, so that a complete transparency of state actions is ensured. In doing so, the authorities will not only halt the harmful use of AI, but also encourage advantageous and futuristic use of AI by ensuring innovation along with dispensation of justice.

REFERENCES

- Burk, D. L., & McDonnell, B. (2016). The Goldilocks hypothesis: balancing intellectual property rights at the boundary of the firm. Scholarship Repository. https://scholarship.law.umn.edu/faculty_articl es/177/
- Bhalla, V., Dyrchs, S., & Strack, R. (2021, March 2). Twelve forces that will radically change how organizations work. BCG Global. <u>https://www.bcg.com/publications/2017/peo</u> ple-organization-strategy-twelve-forces-radicallychange-organizations-work
- Cannan, J. (2017). A (Mostly) legislative history of the Defend Trade Secrets Act of 2016. In LAW LIBRARY JOURNAL (Vol. 109, Issue 3). https://www.aallnet.org/wpcontent/uploads/2018/01/Vol-109-No-3-A-Mostly-Legislative-History-of-the-Defend-Trade-Secrets-Act-of-2016.pdf
- 18 U.S. Code § 1836 Civil proceedings. (n.d.-b).
 LII / Legal Information Institute.
 <u>https://www.law.cornell.edu/uscode/text/18/</u>
 Cancer<u>1836</u>.earch
- Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. Penn Carey Law: Legal Scholarship Repository. <u>https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/</u>
- Lemley, M. A. (2008). THE SURPRISING VIRTUES OF TREATING TRADE SECRETS AS IP RIGHTS. Stanford Law Review, 61(2). <u>https://www.stanfordlawreview.org/wpcontent/uploads/sites/3/2010/04/Lemley.pdf</u>
- Moser, P. (2007). Why Don't Inventors Patent? *RePEc.* <u>https://www.researchgate.net/</u> publication/5188211_Why_Don't_Inventors_ Patent
- Smith, B., Shum, H., & Microsoft. (2018). The future computed. Microsoft Corporation. https://blogs.microsoft.com/wpcontent/uploads/2018/02/The-Future-Computed_2.8.18.pdf



- Simpson, M. P. (2005). The Future of Innovation: Trade Secrets, property Rights, and Protectionism - An Age-Old Tale. *Brooklyn Law Review*, 70(3), 10. http://brooklynworks.brooklaw.edu/blr/vol70 /iss3/10/
- Sherwood, R. M. (2019). Intellectual property and Economic development. In *Routledge*

eBooks.

https://doi.org/10.4324/9780429045530

• Yeh, B. T. & Congressional Research Service. (2016). Protection of Trade Secrets: Overview of current law and legislation (Report No. R43714). Congressional Research Service. <u>https://sgp.fas.org/crs/secrecy/R43714.pdf</u>

