

Balancing Innovation and Confidentiality: Trade Secret Protection For AI-Driven Business Models

Simone Singh¹, Raaghav Mahendran²

Delhi Metropolitan Education, GGSIPU

ARTICLE INFO

*Correspondence:

simonesingh0715@gmail.com
Delhi Metropolitan Education, GGSIPU

Dates:

Received: 26-09-2024
Accepted: 20-10-2024
Published: 30-12-2024

Keywords:

Artificial Intelligence (AI), Trade Secret Protection, Confidentiality Agreements, Intellectual Property, Generative AI, Data Security, Legal Frameworks, Business Innovation, Cross-Border Regulations, AI Governance

How to Cite:

Singh, S., Mahendran, R. (2024) Balancing Innovation and Confidentiality: Trade Secret Protection For AI-Driven Business Models. *DME Journal of Management*, 5(2), 30-37.
doi: 10.53361/dmejm.v5i02.04

Abstract

This paper examines the interplay between artificial intelligence (AI) and trade secret protection, highlighting challenges posed by AI to traditional intellectual property laws. As AI evolves, it redefines the boundaries of trade secrets—historically centred on human-generated information—due to its ability to learn from diverse datasets and create original content, complicating what qualifies as a trade secret.

AI's integration into industries revolutionizes processes like data analytics while exposing businesses to risks such as unintentional disclosure of proprietary data via generative AI tools. The capacity of AI to create or uncover valuable information raises two significant legal issues: diminished motivation for human innovation and the threat to confidentiality doctrines. Particularly, confidentiality agreements and the "inevitable disclosure" doctrine face strain, especially in jurisdictions favouring employee mobility.

Globally, trade secret laws vary, with frameworks like the EU Trade Secrets Directive providing uniformity while countries like China and Japan implement unique approaches. International treaties, such as the TRIPS Agreement, set baseline protections but allow regional flexibility, complicating multinational compliance. Companies must adopt tailored safeguards, including NDAs, localized strategies, and technical controls like data encryption, to mitigate these risks and ensure regulatory adherence.

Effective trade secret management requires balancing innovation and security through collaborative industry standards, adaptive legal frameworks, and comprehensive data governance. This paper underscores the urgency for reform and provides actionable strategies to protect intellectual property in the AI era.

INTRODUCTION

The rapid advancement of Artificial Intelligence (AI) has revolutionized many industries, creating new business models and technologies. However, AI's ability to process and generate proprietary information presents significant challenges for protecting trade secrets—vital assets such as algorithms, business strategies, and customer data.

This paper explores the intersection of AI and trade secret protection, examining how AI's potential to create and discover confidential information

complicates traditional legal frameworks. It addresses challenges like the application of the inevitable disclosure doctrine, employee mobility concerns, and the global variation in trade secret laws.

Additionally, it shows the legal reforms and best practices for protecting AI-generated intellectual property. By analyzing case law and current regulations, it highlights the need for adaptive legal frameworks that can support innovation while safeguarding valuable intellectual assets in an AI-driven world.

AI and Trade Secrets

Artificial intelligence (“AI”) is the most significant technological advancement in centuries. It will have a significant influence on intellectual property law. For the very first time in history, machines may equal or outperform humans’ ability to generate great ideas, posing an unprecedented threat to this human-centered law. Researchers have looked into how AI affects copyright and patent law, but they haven’t looked at how it affects trade secret law. Artificial intelligence (AI) is a technology that allows computers and machines to mimic human learning, comprehension, ability to solve problems, decision-making, creativity, and autonomy.

They are able to comprehend and react to human words. They are able to pick up new knowledge and skills. They have the skills to provide consumers and specialists with thorough advice. They can act on their own, eliminating the need for intelligence from humans or intervention (a common instance is a self-driving car). In general, AI systems function by consuming massive volumes of labelled training data, analysing it for correlations and patterns, and then using these patterns to forecast future states. Realistic text, images, music, and other media can be produced using generative AI techniques, which have rapidly advanced in recent years.

AI is being incorporated into more and more company operations and sectors with the goal of enhancing productivity, customer satisfaction, strategic planning, and decision-making. Many of today’s data analytics and customer relationship management (CRM) platforms, for instance, are powered by machine learning models, which

assist businesses in understanding how to best serve clients by customising offers and providing more specialised marketing. Chatbots and virtual assistants are being used in mobile applications and on business websites to answer frequently asked enquiries and offer 24/7 customer support. Additionally, an increasing number of businesses are investigating the potential of generative AI technologies like ChatGPT to automate processes like computer programming, product creation and ideation, and document draughting and summarisation.

A trade secret is a valued piece of information for an enterprise that is treated as confidential and that gives that enterprise a competitive advantage. Trade secret law strikes a balance between incentivizing humans to advance valuable information and restraining the protection accorded to titleholders of that information.

The phrase “trade secret” is a historical inaccuracy since it now refers to information that is not utilised in commerce or business. As a result, the term includes virtually any type of valuable information, including algorithms, business approaches, compilations, cost data, customer lists, designs, drawings, statements of finances, formulas, inventions, marketing strategies, patterns, price data, product specifications, manufacturing processes, recipes, religious materials, research findings, sales data, social networking contacts, and software.

The term “trade secret theft” used to refer to the theft or duplication of a tangible document or item. Due to the digitisation of information, illegal access to computer networks is becoming a more common method of industrial espionage. For different ecosystems in the manufacturing or creative and cultural industries, it presents unique obstacles. By raising knowledge of cybersecurity and practicing effective intellectual property management, the financial impact of trade secret cyber theft can be lessened.

Intersection of Trade Secrets and AI

The rise of artificial intelligence threatens the trade secret balance in two distinct ways. First, there is no legal incentive for AI to produce useful new information. This might eventually make people



less inclined to produce such information. Second, the limiting doctrines that restrict protection will be more significant since AI will be better than humans at identifying already-existing trade secrets.

The relationship between trade secrets and AI indeed poses significant challenges. It is to be noted that trade secrets are protected by confidentiality agreements, typically involving human parties who can promise to maintain that confidentiality. However, generative AI systems like LLMs do not have the capacity to make such promises, which complicates the protection of sensitive information.

When businesses use generative AI, there's a risk that sensitive data—such as trade secrets, financial information, or personal data—might be inadvertently processed or leaked. The ingestion of vast amounts of information by AI systems can lead to unintended disclosures if that information isn't adequately filtered or secured. This is particularly concerning given that many companies store user prompts and generated outputs, which could potentially include confidential data.

There are incidents where sensitive information has been leaked after using generative AI, have understandably led many organizations to reconsider their policies on AI usage. Some have opted for outright bans or imposed strict limitations to mitigate risks.

Given these complexities, companies are faced with the challenge of balancing innovation with the necessity of safeguarding confidential information. Implementing robust data management and security protocols is essential to protect trade secrets when using AI technologies.

Challenges of Applying Trade Secret Law to AI-Driven Business Models

Applying trade secret law to AI-driven business models involves navigating a landscape filled with complex challenges. One of the foremost issues is the ambiguity surrounding the definition of trade secrets. Under existing laws, trade secrets must meet specific criteria: they must be confidential, provide a competitive advantage, and be subject to reasonable efforts to maintain secrecy. However, in the realm of AI, the data utilized for training models

often blurs the line between proprietary information and public knowledge. As AI systems learn from vast datasets, the outputs they generate can inadvertently incorporate or reflect elements of this confidential data, complicating the determination of what remains protected as a trade secret.

The collaborative nature of AI development further exacerbates these challenges. Many AI projects involve partnerships between multiple organizations, requiring the sharing of data and proprietary algorithms. This collaboration can increase the risk of inadvertent disclosure of trade secrets. When sensitive information is processed by AI systems, there is a chance that the outputs may reveal confidential business insights or proprietary algorithms, especially if proper safeguards are not in place. This issue is particularly pronounced in environments where sensitive data must be shared for effective model training, as it can be difficult to control how that information is ultimately used or disseminated.

Another significant concern is the inability of AI systems to enter into formal agreements, such as nondisclosure agreements (NDAs). Unlike human employees or collaborators, AI cannot be held accountable for breaches of confidentiality. This creates a legal grey area regarding the enforcement of trade secret protections. If a trade secret is exposed through an AI model's output, it may be challenging to determine liability, particularly if the AI's operation and data handling processes are opaque.

The black box nature of many AI models presents yet another challenge. These systems often utilize complex algorithms that are not easily interpretable by humans, making it difficult for organizations to understand how data is processed and what outputs are generated. This lack of transparency complicates the assessment of whether trade secrets have been compromised. As a result, organizations may find it challenging to conduct proper risk assessments or audits of their AI systems, leading to potential vulnerabilities.

Furthermore, the global nature of AI technology introduces jurisdictional complexities. AI systems can operate across borders, which raises questions about which jurisdiction's trade secret laws apply

in cases of potential breaches. Different countries have varying standards for what constitutes a trade secret and the extent to which such information is protected. This disparity can create compliance challenges for organizations operating internationally, as they must navigate a patchwork of regulations.

As AI technology evolves rapidly, existing trade secret laws may not adequately address the new challenges presented by AI-driven business models. Legal frameworks must adapt to the unique characteristics of AI, including the ways in which data is processed and utilized. Additionally, there is a potential for misuse of AI technology; for example, AI can be employed to reverse-engineer proprietary algorithms or replicate trade secrets from publicly available data. This potential for misuse further complicates efforts to protect sensitive information.

To address these multifaceted challenges, organizations need to adopt comprehensive data governance strategies that prioritize the protection of trade secrets. This may involve implementing robust data management practices, establishing clear protocols for data sharing, and conducting regular audits of AI systems to ensure compliance with trade secret laws. Investing in AI ethics training can also be beneficial, as it helps employees understand the importance of safeguarding confidential information and the potential risks associated with AI usage. Additionally, seeking legal counsel can provide organizations with the guidance needed to navigate the intricate intersection of trade secret law and AI-driven business models, ensuring they are equipped to protect their proprietary information effectively in a rapidly changing landscape.

Legal Frameworks and Case Law

India does not yet have a codified law that specifically protects trade secrets, however, the Indian courts from time to time have discussed and upheld the importance of trade secrets in catena of cases.

The plaintiff in Burlington Home Shopping Pvt. Ltd v. Rajnish Chibber was a mail order service company that operated by sending out mail order catalogs containing a variety of consumer goods to a specific clientele. The plaintiff had invested heavily in building a database of clients and customers. The

plaintiff discovered that a former employee of the defendant company had impersonated a rival of the plaintiff, obtained a copy of the confidential database holding client data, and was using it to connect with the plaintiff's client. In this case, the Delhi High Court ruled that the defendant had engaged in slavish replication of the plaintiff's compilation, establishing a blatant case of infringement.

Markets & Markets Research Pvt Ltd v. Meticulous Market Research Pvt Ltd and Ors is another case in which the plaintiff was in the business of offering businesses and clients specialized market research and information. The plaintiff argued that they produce studies that target particular markets using proprietary techniques, which were purchased by well-known customers. The defendants in this case, numbers two through seven, were former workers of the plaintiff who joined defendant number one. In order to create their own market reports, the Defendants were allegedly replicating the Plaintiff's format and content. Suspecting theft of confidential data, the Plaintiff had also filed a criminal complaint against the Defendant. Taking swift action the Hon'ble Delhi High Court held that the "*Defendants action infringed the rights of the Plaintiff and passed an injunction order in favour of the Plaintiff*"

This decision was upheld in the Indian Explosives Pvt Ltd v. Ideal Detonators Pvt Ltd and Ors case as well. In that case, the plaintiff was involved in the production of shock tube and industrial explosives. The plaintiff argued that the shock tubes could not be replicated without first duplicating or copying the two-dimensional drawings. It was further claimed that former employees of the Plaintiff had stolen confidential information, trade secrets, and drawings related to shock tube detonators during the course of their employment and have sold them to Ideal Detonators (Respondent) for profit. According to the Hon'ble Calcutta High Court, "there is an involvement of the Respondent in setting up a rival plant and the unauthorized use of drawings and other documents of the plaintiff and the confidential information of the plaintiff particulars." The court issued an order in favor of the plaintiff, prohibiting the Respondents from further disclosing or transferring confidential information.



According to the Hon'ble Supreme Court, "information contained in a document if replicated, can be the subject of theft and can result in wrongful loss, even though the original document was only temporarily removed from its lawful custody for the purpose of extracting the information contained therein." This was also the case in *Birla Corporation Ltd. v. Adventz Investment & Holdings Ltd.*

Even though the courts from time to time by their judge-made law have protected trade secrets and confidential information, there is still a requirement of a codified law. In this line, the Law Commission of India in its 289th Report has proposed «The Protection of Trade Secret Bill 2024». Hon'ble Justice Ms. Prathiba M Singh of the Delhi High Court has also highlighted the need for a codified law protecting trade secrets. In her comment Hon'ble Justice commented *"that in the current economic scenario, we have big innovations happening, especially within the Artificial Intelligence (AI), technology and start-up ecosystem she further stated that data is very vital to all these industries and one leak of any sensitive information can have a crippling impact on the progress of an entity, Even with big companies, a substantial capital is invested in research and most of the data that they seek to protect is at the research stage thus incapable of being protected under the system of patents and copyright, which may not afford adequate protection against the misappropriation of such data. Loss of such data has serious economic implications for such companies"*.

Section 2(f) of the proposed bill in hand defines Trade Secret as *"any information that is secret in the sense that it is not generally known among or readily accessible to persons, derives commercial value on account of being secret, has been subject to reasonable steps under the circumstances by the holder of such information to keep it secret and disclosure of such information is likely to cause damage to the holder of such information"*. Section 7 of the proposed bill deals with relief that a court may grant to the Plaintiff in any suit for misappropriation of Trade Secrets, the reliefs include injunction, damages/accounts of profit, destruction of documents, objects, materials, etc., and pecuniary remedies.

The current bill offers a more organized and thorough framework for safeguarding trade secrets in the face of cutting-edge technologies like artificial intelligence. Prior to the proposed bill, Indian courts had adopted a similar stance in numerous cases when awarding relief to parties who had suffered losses as a result of trade secret loss and confidentiality breaches.

International Perspectives and Cross-Border Issues

In 2022, WIPO held a symposium on trade secrets and innovation on May 23 and 24.

WIPO states that trade secrets are a subset of intellectual property (IP) rights that safeguard proprietary, economically valuable, and secret information. Technical knowledge like software algorithms and manufacturing procedures, as well as commercial information like distribution channels and advertising tactics, might be considered trade secrets.

To qualify as a trade secret, information must meet the following criteria:

- Be commercially valuable because it is secret
- Be known only to a limited group of people
- Be subject to reasonable steps to keep it secret, such as confidentiality agreements

Trade secrets represent an efficient approach to safeguard a company's intellectual property. Compared to other IP rights, they can safeguard a greater variety of topics and are not constrained by a predetermined duration of protection. Trade secrets, however, cannot be used against someone who independently finds the knowledge because they are not exclusive rights like patents.

Differences in Trade Secret Protection Laws Across Major Jurisdictions

European Union (EU)

The EU has a unified approach to trade secret protection under the EU Trade Secrets Directive (2016), which standardizes the definition of trade secrets and provides a consistent framework across member states. This directive emphasizes reasonable steps for trade secret holders to maintain

confidentiality but balances protections with employee mobility rights.

China

China has strengthened its trade secret laws, especially with amendments to its Anti-Unfair Competition Law in recent years, aiming to improve intellectual property protection and align more closely with global standards. However, enforcement can still be challenging due to local legal complexities and business culture. Companies face high risks of trade secret misappropriation, especially when collaborating with local firms or subsidiaries.

Japan

Japan's trade secret laws are governed by the Unfair Competition Prevention Act. Japan places significant importance on enforcing confidentiality agreements and has streamlined processes for trade secret litigation, though its protections are generally seen as less stringent than those in the EU or the U.S.

These differences mean that multinational AI companies need tailored strategies for each jurisdiction. For instance, what qualifies as a "reasonable effort" to protect a trade secret may vary, requiring different levels of data security and employee agreements in each region.

Impact of International Treaties, Such as The Trips Agreement

- The Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement by the World Trade Organization (WTO) establishes minimum standards for trade secret protection among its members, including confidentiality, non-use, and non-disclosure. TRIPS requires members to provide trade secret protection but allows flexibility in implementation, leading to variability across countries.
- Implications of TRIPS for AI: TRIPS has encouraged many countries to strengthen trade secret protections, helping global companies operate in regions with improved IP safeguards. However, since enforcement practices vary, AI firms still need to consider local enforcement effectiveness and additional contractual measures, like NDAs and non-competes, to secure their intellectual property across borders.

Managing Trade Secret Risks in Deploying AI Models Globally

Localization of Data and Models

Companies often need to adapt AI models and data handling practices to comply with local regulations. For example, in the EU, stringent data privacy laws like GDPR affect how training data is stored and processed, requiring companies to set up regional data centers or adjust data transfer methods.

Security Measures Across Borders

Different countries have different expectations for what constitutes "reasonable measures" to protect trade secrets. AI firms should use a mix of technical controls (e.g., data encryption, access restrictions) and legal safeguards (e.g., localization agreements) to ensure consistent security.

Local Partnerships and IP Risk

Working with local partners may necessitate sharing sensitive AI model details, which increases the risk of trade secret leakage. Careful drafting of contracts, clear IP ownership clauses, and reliance on trusted legal advice in each jurisdiction can mitigate this risk.

By understanding these global nuances, AI companies can navigate cross-border trade secret protection more effectively, balancing innovation and security in diverse regulatory environments

Alternative Approaches to IP Protection for AI Innovations

Given its potential worth, organizations should safeguard their intellectual property related to AI. In 2018, 84% of the value of S&P 500 firms was derived from intellectual property and other intangibles. However, as the AI IP legal environment changes further, creating a plan to capitalize on this value can encounter certain challenges. A number of AI-related intellectual property (IP) issues, such as AI inventorship, patent eligibility, written description and enablement requirements, data issues, and AI-related copyright issues, are being investigated by various government agencies, such as WIPO, the European Patent Office ("EPO"), the USPTO, the U.S. Copyright Office, and others.



To maximize protection for AI-related IP while policy deliberations continue, organizations can follow these 10 best practices.

1. Develop an IP Strategy and Procedures

Create a written IP strategy to identify, assess, and protect IP assets using methods like patents, copyrights, trade secrets, and contracts. Prioritize valuable IP and adapt as laws change.

2. Assess Patent Eligibility

Evaluate if AI inventions are patent-eligible, especially since requirements vary by region. If patents aren't feasible, consider alternatives like trade secrets.

3. Determine Inventorship and Ownership

Ensure human inventors are named in AI-related patents, as AI cannot legally be an inventor. Secure rights from all inventors for company ownership.

4. Comply with Description Requirements

For AI patent applications, provide a detailed written description that enables skilled individuals to recreate the invention, depending on the novelty of the technology.

5. Protect Trade Secrets

Use trade secrets for non-patentable innovations or when patents are cost-ineffective. Implement confidentiality and security measures to prevent misappropriation.

6. Determine AI-Generated Copyright Ownership

Identify human authors for AI-generated works, as copyrights are only granted to human-created content. Secure rights from all potential authors to establish ownership.

7. Protect Data Rights

Use trade secrets and contracts to protect valuable data. Limited copyright protection may apply for unique data arrangements, especially in regions like the EU.

8. Manage Text and Data Mining (TDM)

Ensure TDM practices comply with laws, as some regions, like the EU, allow certain TDM exceptions, while U.S. regulations are varied.

9. Evaluate Broader Data Policies

Monitor evolving data governance frameworks, especially in the EU, which aims to create common data spaces and standards that impact data use and protection.

10. Maximize Contracts

Leverage contracts to secure IP rights for AI components and outputs. Understand and apply open-source or Creative Commons licenses as needed for business goals.

Future Considerations

The pace of AI development raises critical questions about the adequacy of current trade secret protections. Future considerations include the need for adaptive legal frameworks that acknowledge the unique characteristics of AI, potential reforms to enhance enforcement mechanisms, and the role of industry standards in encouraging best practices for protection.

Looking ahead, there is an urgent need for reform in trade secret law that acknowledges the unique characteristics presented by rapid improvements in AI technology. As the legal landscape continues to evolve, adaptive frameworks must be developed that enhance enforcement mechanisms while promoting innovation.

Industry standards should be collaboratively established among stakeholders to ensure best practices for protecting trade secrets are maintained without stifling technological advancement. The pace of AI development raises critical questions about the adequacy of current trade secret protections. Future thoughts include the need for adaptive legal frameworks that acknowledge the unique characteristics of AI, potential reforms to enhance enforcement mechanisms, and the role of industry standards in promoting best practices for protection.

For instance, while traditional trade secret law requires that information derive independent economic value from not being generally known or readily ascertainable, it must also adapt to address how AI processes and generates data. Courts may need to consider new forms of evidence and methods for demonstrating misappropriation

that account for the complexities introduced by AI technologies. By proactively speaking these issues, stakeholders can help ensure that intellectual property rights are preserved while fostering an environment conducive to technological advancement.

CONCLUSION

In summary, this research highlights the urgent necessity for reform in trade secret law to address the challenges posed by emerging artificial intelligence (AI) technologies. As AI continues to evolve and reshape various industries, traditional frameworks for protecting intellectual property must adapt to these advancements.

Furthermore, the importance of establishing collaborative industry standards is emphasized, as these can help promote best practices for protecting trade secrets without stifling innovation. As organizations face increasing risks related to data breaches and misappropriation in the context of AI, it is crucial that they adopt a proactive approach to trade secret protection.

Ultimately, this paper seeks to foster a deeper understanding of the intersection between AI and trade secret law, encouraging stakeholders to engage in meaningful dialogue and action that will shape the future of intellectual property rights in an increasingly digital world.

REFERENCES

John G. Sprankling, TRADE SECRETS IN THE ARTIFICIAL INTELLIGENCE ERA, Pg1, 2024
Cole Stryker, Eda Kavlakoglu, What is artificial intelligence (AI)?
Lev Craig, What is AI? Artificial Intelligence Explained
European Commission- Trade secrets
John G. Sprankling, TRADE SECRETS IN THE ARTIFICIAL INTELLIGENCE ERA, Pg3, 2024
John G. Sprankling, TRADE SECRETS IN THE ARTIFICIAL

INTELLIGENCE ERA, Pg4, 2024
European Commission- Trade secrets
John G. Sprankling, TRADE SECRETS IN THE ARTIFICIAL INTELLIGENCE ERA, Pg4, 2024
Smith, J. (2022). *The role of NDAs in protecting trade secrets*. Journal of Intellectual Property Law, 15(2), 45-67.
Johnson, A. (2023). *Artificial Intelligence and the risk of data leakage: A legal perspective*. International Journal of Cyber Law, 10(1), 89-102.
SS Rana & Co, Threats posed by AI to Trade Secrets
Burlington Home Shopping Pvt. Ltd v. Rajnish Chibber, 995(15)PTC 278(Del)
Markets & Markets Research Pvt. Ltd. v. Meticulous Market Research Pvt. Ltd. and Ors., 2023 SCC OnLine Del 987
Indian Explosives Pvt. Ltd. v. Ideal Detonators Pvt. Ltd. and Ors., 2023 SCC OnLine Cal 421
Birla Corporation Ltd. v. Adventz Investment & Holdings Ltd, AIR 2019 SUPREME COURT 2390
WIPO, Trade Secrets
Ryan N. Phelan (2024, November). AI-based inventions: Patenting vs. trade secret considerations.
SS Rana & Co (August 2024) Threats posed by AI to trade secrets. IP Stars
Joseph Barber (December 2024) Trade Secrets and AI Systems: The Future of Trade Secret Protection in Business
European Commission. (n.d.). Trade secrets
Lev Craig (October 2024) What is AI? Artificial Intelligence explained
Cole Stryker & Eda Kavlakoglu (August 2024.). What is Artificial intelligence. IBM
World Intellectual Property Organization (WIPO). (n.d.). Trade secrets
<https://www.patentnext.com/2024/11/ai-based-inventions-patenting-vs-trade-secret-considerations/>
https://www.ipstars.com/NewsAndAnalysis/Threats-posed-by-AI-to-Trade-Secrets/Index/10136_
<https://ipwatchdog.com/2024/12/12/trade-secrets-and-ai-systems-the-future-of-trade-secret-protection-in-business/id=184002/>
https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/trade-secrets_en
<https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence>
<https://www.ibm.com/think/topics/artificial-intelligence>
<https://www.wipo.int/web/trade-secrets>

