TRADE SECRET CONFIDENTIALITY USING ARTIFICAL INTELLIGENCE AND AI TOOLS

TRADE SECRETS COMMITTEE

Committee Chair: Catherine Mateu

Committee Vice Chair: Scott Mayhew

STAKEHOLDER OUTREACH SUBCOMMITTEE

Subcommittee Chair: Mahua Roy Chowdhury

Subcommittee Members: Abdul Basit, Anju Khanna, Roberto Valenti, JV Abhay, Milan Milojevic, Sahil Malhotra

March 2025

TABLE OF CONTENTS

Introduction

In today's globalized economy, trade secrets represent a crucial form of intellectual property that enables businesses to maintain a competitive advantage by protecting confidential information. This paper provides an introduction to the impact of artificial intelligence (AI) on maintaining trade secret confidentiality. Because trade secrets rely on maintaining secrecy by using reasonable measures, an organization not only needs to understand the legal requirements of maintaining trade secret confidentiality but also must take into consideration the benefits and challenges of using AI technology.

Trade secrets encompass a wide range of confidential business information that provides economic value due to its secrecy. This can include formulas, manufacturing processes, business strategies, customer lists, and technical know-how, but also information on clients and suppliers, and administrative data. There are three key criteria for information to be classified as a trade secret. First, there should be secrecy. The information must not be publicly known or easily accessible to others in the same business sector. Second, there should be commercial value. The economic value of the information should derive from it being secret, providing the holder with a competitive advantage over its competitors. Finally, reasonable measures should be taken to maintain secrecy. The holder must take reasonable steps to keep the information confidential, such as by implementing non-disclosure agreements (NDAs) or robust digital security systems.

Unlike patents, which require registration and disclosure, trade secrets can last indefinitely if the conditions listed above are met. This makes them especially appealing in fast-moving industries where innovation outpaces the time needed for patenting, such as with technology and pharmaceuticals. Moreover, trade secrets allow businesses to avoid revealing proprietary knowledge to competitors, a key reason why many companies opt for this form of protection. In

addition, some information protected as trade secrets cannot be patented or protected through other IP rights.

Protecting trade secrets has become more critical and challenging in today's rapidly evolving digital landscape. As organizations increasingly rely on trade secrets to maintain their competitive edge, the need for robust, innovative security measures has grown substantially. Artificial Intelligence (AI) technologies have emerged as powerful tools in this ongoing battle to safeguard trade secrets. AI technologies, which are a broad set of computational techniques and approaches that aim to create systems capable of performing tasks that typically require human intelligence, can be leveraged to enhance the identification, maintenance, and security of trade secrets and to detect and prevent unauthorized access or disclosure of such information. Some key AI technologies include: (a) machine learning, (b) deep learning, (c) natural language processing, (d) expert systems, (e) adversarial machine learning, and (f) explainable AI (XAI)

Businesses and enterprises can apply these AI technology solutions to protect trade secrets by:

- preventing data loss,
- analyzing user behavior patterns to mitigate insider threats or attempted data breaches, devising encryption methods by analyzing and adapting to newer threats and adjusting the security protocols accordingly,
- refining access control policies in an organization,
- identifying and responding to potential threats in real-time,
- classifying documents that contain trade secrets,
- applying appropriate protection measures,
- detecting infringement of rights, and
- predicting other potential risks to trade secrets.

This paper is divided into two sections: Section I covers general considerations regarding trade secret confidentiality and AI, and Section II covers how AI tools can be used to enhance trade secret protection programs.

Section I: General Considerations Regarding Trade Secret Confidentiality and Artificial Intelligence

1. Overview

This section provides an overview of significant trade secret protection laws, including through various international treaties; potential benefits of using AI for creating and protecting trade secrets; and potential challenges to trade secret protection posed by using AI within organizations.

2. Trade Secrets: Legal Protection in the International, U.S., EU, and China Contexts

The concept of trade secrets and their protection has a long history dating back to ancient times. The law of trade secrets is the oldest form of intellectual property protection. During the Roman Empire, trade secret laws provided legal consequences for individuals who induced another agent to divulge secrets relating to their master's commercial affairs. European guilds during the medieval period widely practiced trade secrecy. Modern trade secret law, however, began in early 19th century England in response to the growth there of technology and know-how.

The term "trade secret" does not find categoric mention in international conventions, but an inference can be drawn from the Paris Convention of 1883, which, under Article 10, inclusively refers to unfair competition and provides that "any act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition." The principles in this broad definition help ensure a fair system that enables, even incentivizes, investment into the creation of intellectual capital by businesses. Following this early foundation, more specific trade secret laws took shape.

2.1 International Framework: The Role of the TRIPS Agreement

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), introduced by the World Trade Organization (WTO) in 1994, was a landmark development in the international protection of trade secrets. Article 39 of TRIPS specifically addresses undisclosed information, requiring member states to provide protection against unauthorized acquisition, use, or

disclosure of trade secrets that is contrary to honest commercial practices. This includes breach of contract, breach of confidence, and unfair competition.

TRIPS established minimum standards for trade secret protection globally and served as a foundation for many national and regional laws on trade secrets. The agreement requires that information be: (a) secret and not easily accessible; (b) commercially valuable because of its secrecy; (c) subject to reasonable protection measures to maintain its confidentiality.

TRIPS leaves considerable flexibility for member states to define and implement trade secret protection within their legal systems. For instance, the TRIPS Agreement does not provide a uniform definition of what constitutes "reasonable steps" or "commercial value," allowing countries to adapt their legislation to their specific economic and legal contexts.

2.2 U.S. Protection: The Defend Trade Secrets Act (DTSA)

In the United States, trade secret protection was traditionally governed at the state level through the Uniform Trade Secrets Act (UTSA), which has been adopted on a state-by-state basis. However, in 2016, the Defend Trade Secrets Act (DTSA) was passed, creating a federal cause of action for trade secret misappropriation. This marked a significant shift, allowing businesses to bring trade secret cases in federal courts and ensuring a more uniform application of trade secret law across the country.

The DTSA defines trade secrets similarly to how the TRIPS Agreement defines it, requiring that the information be secret, valuable, and subject to reasonable measures of protection. It offers several powerful remedies, including civil damages for economic loss due to misappropriation; seizure orders in cases where there is a risk of the trade secret being destroyed or misused; punitive damages for willful misappropriation; and injunctive relief to prevent the continued use or disclosure of the trade secret.

High-profile cases disputing potential misappropriation have highlighted the critical importance of trade secret protection in maintaining competitive advantage. The DTSA's introduction of

federal jurisdiction has also provided more consistency in trade secret litigation, making the United States a global model for effective trade secret enforcement.

2.3 EU Protection: Directive 2016/943 (EUTSD)

In the European Union, trade secrets were harmonized with the approval of Directive (EU) 2016/943, heavily influenced by the TRIPS Agreement. Prior to the Directive, trade secret protection varied widely across member states, creating legal uncertainty for businesses operating across borders. The Directive introduced minimum standards for the protection of trade secrets, ensuring consistency across the EU.

The EUTSD defines trade secrets similarly to how the TRIPS Agreement defines it, requiring that the information be secret, have commercial value, and be subject to reasonable steps to keep it confidential. One of the key provisions of the Directive is the requirement for confidentiality during legal proceedings, which protects businesses from exposing their trade secrets through litigation. This is particularly important in industries where the disclosure of a trade secret might irreparably damage a company's competitive position.

Additionally, the Directive balances trade secret protection with other public interests, such as whistleblower protections and freedom of expression. It allows for the lawful disclosure of trade secrets in cases where it serves the public interest, such as revealing corporate misconduct or illegal activity. This reflects the EU's broader commitment to balancing the interests of businesses with those of society.

2.4 China Protection: The Anti Unfair Competition Law (AUCL)

Trade secrets are protected in China under the Anti Unfair Competition Law (AUCL). The TRIPS Agreement played a pivotal role in shaping the Chinese legislation on trade secrets. For example, trade secrets definition in China is aligned to that provided by Article 39.2 of TRIPS. Article 9 of AUCL defines a trade secret as technical, business, or other commercial information unknown to the public, with commercial value, and protected by the owner with secrecy measures.

Having provided a brief overview of U.S. federal law, EU and China legislation, and international treaties regarding trade secrets, this paper will now discuss opportunities for protecting trade secrets using AI.

3. Opportunities for Protecting Trade Secrets Using AI Innovations

Using AI to manage trade secrets sounds contradictory due to the divergence between the intent of trade secrets law and the intent of AI technology. As there is no registration system, trade secrets maintain their value only as long as they are kept secret. AI, on the other hand, holds value based on greater amounts of input information that can be used to develop outputs and is agnostic as to the confidential nature of such inputs/outputs.

Even so, AI has the potential to provide practical tools to protect trade secrets. For example, AI can be used to stop unauthorized access by using advanced encryption methods.[1] AI can also be used to obfuscate confidential information by using advanced natural language processing (NLP)[2] and can create synthetic data that makes it harder to access sensitive data. AI can also assist in monitoring behavior patterns of employees to detect any deviation from normal patterns of access, login timings, location, etc. Monitoring behavior can ensure that employees are following internal policies and rules regarding the sharing of information.

AI tools can also be used to support employee education. AI can help to quickly develop learning tools for employees to generate their awareness about the proper ways of handling sensitive information. Employees can also be trained regarding what kind of information can be input into an AI tool.

[1] https://www.linkedin.com/advice/0/how-can-ai-help-protect-trade-secrets-grwvf#:~:text=Utilizing%20NLP%20for%20synthetic%20data,the%20digital%20fortress%20against%20infiltration.&text=AI%20enhances%20the%20protection%20of,secrets%20remain%20secure%20and%20proprietary.&text=Artificial%20intelligence%20takes%20the%20security,of%20the%20data%20to%20occur. And https://www.tangibly.com/product/predicted-portfolio/

[2] https://smith.ai/blog/where-do-generative-ai-models-source-their-data-information

Trade secret protection can serve as an alternative for protecting AI-generated innovations.[3] With digital inventions being limited by patent eligibility standards in different jurisdictions, trade secret protection is an attractive option. Due to the speed of digital innovations, it may be more viable for organizations to keep such inventions secret, rather than trying to patent them.

AI-generated inventions can add value to every part of an organization that is involved in the creation and usage of trade secrets. This can include algorithms, business methods, compilations, cost data, customer lists, designs, drawings, financial statements, formulas, inventions, marketing strategies, patterns, price data, product specifications, production processes, recipes, research findings, sales data, social media contacts, and software.[4] However, there may be challenges when it comes to protecting information generated by an AI system with regard to whether such information may be considered equivalent to that produced by a person.

For example, AI can generate inventions using massive datasets to produce results not previously conceivable. This is due to the prohibitive time and cost to develop such inventions or simply the lack of ability to process such massive amounts of data to obtain meaningful results. For proprietary AI systems, the outputs will be known or accessible only to the owners of the system.

On the other hand, in the event of a dispute, it may be a challenge to defend an AI-generated invention as a trade secret. For example, it may be difficult to prove that sufficient steps were taken to keep it a secret. If input data were taken from publicly available sources, proving that the output is a secret would be a challenge.

Certain steps can be taken by an organization to limit exposure of its secrets, like training employees as to what constitutes sensitive information, drafting AI policies for limiting access to AI tools, monitoring activities using AI tools, using contractual strategies like NDAs, and building proprietary AI systems.

---

[3] https://ipwatchdog.com/2023/11/28/ai-trade-secrets-winning-combination/id=170001/

[4] Sprankling, John G., TRADE SECRETS IN THE ARTIFICIAL INTELLIGENCE ERA (March 08, 2024). Available at SSRN: https://ssrn.com/abstract=4847813 or http://dx.doi.org/10.2139/ssrn.4847813

For an organization to decide whether to keep an AI-generated invention secret or to seek patent/copyright protection, there are certain criteria that must be considered. One is subject matter eligibility. Algorithms are difficult to patent in most jurisdictions as they are considered "a set of instructions." Though some jurisdictions allow patenting of algorithms with a technical effect, uncertainty remains around patent protection of algorithms. There are no separate categories or standards for determining patentability of AI algorithms. While it may be possible to patent AI algorithms and AI training models, it is very difficult to patent AI training data. Hence for data sets, trade secret protection is a better option.

Another issue is the disclosure requirement for patent protection, which must be tailored for each jurisdiction, and the potential for the sufficiency of a disclosure to pose a problem. AI-generated inventions may be difficult to disclose or describe, or the necessary disclosures may be too lengthy, substantially adding to the cost of a patent application. In addition, both the patent and copyright laws across jurisdictions[5] require an inventor/author to be a human being. Trade secret protection imposes no such limitation. Many jurisdictions do not have a *sui generis* system of trade secret protection and those that do have one do not impose such restrictions.

4. Challenges of Using Artificial Intelligence with Trade Secrets

While there are significant opportunities for using AI to generate and protect trade secrets, there are also challenges that should be addressed when looking to implement a robust trade secret protection program. To these ends, three areas are discussed here: (a) keeping trade secret information confidential on an AI platform; (b) whether to limit the access to or use of AI tools; and (c) possible reasonable measures to keep trade secret information secret.

[5] *Thaler v. Vidal*, 43 F.4th 1207, 1210 (Fed. Cir. 2022); similar decisions were given in other jurisdictions; *Thaler v. Perlmutter*, 2023 WL 5333236, *4 (D.D.C. Aug. 18, 2023): taken from supra, no. 3

With the increasing usage of AI, questions arise as to trade secrets protections measures when it comes to the types of AI tools. For example, is the tool an internal application (created internally), which may afford greater control over maintaining secrecy than with an external application?

Many companies will likely begin with an external application. If an external application is being used, then what controls can be put in place to prevent disclosure of trade secrets? Also, does the external application itself predict/propose future trade secrets? Do the owners of the external application have ownership or control of the trade secrets generated through the application? Or will trade secrets no longer be considered secret and therefore no longer protectable?

Another challenge with AI tools is how much information is shared when a project requires collaboration with consultants and other third parties. For example, an engineer at a certain company may be collaborating with a consultant hired by the same company on a new software tool. However, the consultant may also be working with another party on another aspect of the software tool (e.g., the user interface). If AI is being used within each of these interactions, which information is protected and which information is under threat of losing confidentiality? While the predictive aspect of AI is the core of its value, it is also this characteristic that makes AI such a significant risk when it comes to keeping information confidential. And this leads to the second challenge with AI: whether to limit the use of AI tools.

In organizations it is more than likely that AI is being used by a variety of workers, including but not limited to engineering, science, and computer science professionals. Limiting the use of AI tools may be a non-starter for several reasons. For example, if there is an AI tool intended for use by engineers, could a company fully prevent some or all of their engineers from using that specific AI tool? Also, if availability of AI tools is limited, would competitors have a greater advantage and get products to market faster than a company that has decided to implement policies restricting the use of AI? Limiting the use of AI tools might only result in engineers going ahead and still using AI on their own, resulting in an even greater risk.

Given the risks involved with using AI tools, what reasonable measures can be taken to protect trade secrets? One area of concern regarding the implementation of protective measures is how to ensure that the policies are not burdensome. For example, would an employee want to work at a place that analyzes and determines any use made of devices. Would such a policy be compliant with employment law?

Also, while the definition of reasonable measures is based on legal definitions, would such measures be considered reasonable to the employees within the organization? And, if these measures become too burdensome, would this lead to changes in how and when trade secrets can be used?

For example, will legislative bodies decide that AI-generated trade secrets are not protected as trade secrets? In addition, around April 2024, the U.S. Federal Trade Commission issued a rule banning noncompete agreements in particular circumstances (https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-rule-banning-noncompete). It would not be unreasonable to contemplate that there could be legal limitations placed on how AI is used for both trade secret protection and trade secret generation.

Accordingly, both technology and policy developers should be more holistic in their approach to trade secret protection, aiming to enhance the ease of employee compliance rather than creating additional burdens.

Section II: Enhancing Trade Secrets Programs Using AI Tools

5. Overview

Regardless of jurisdiction, safeguarding trade secrets is a vital component of intellectual property management for businesses in all sectors. This section will delve into the role of AI tools in enhancing trade secrets programs from an IP perspective. It will examine how AI technologies, such as machine learning and data analytics, can supplement traditional methods of trade secret protection by enabling proactive identification of sensitive information, its maintenance, and structuring; by providing secured placeholders for such information; by detecting unauthorized access or disclosure to third parties or accidental leakages; and by identifying potential threats to proprietary intellectual assets. By harnessing AI-driven solutions, organizations can strengthen their trade secrets management framework, mitigate the risk of misappropriation, safeguard their market position, and gain a competitive advantage. This section will also explore the legal implications of integrating AI tools into a trade secrets program, including considerations related to confidentiality agreements, data privacy regulations, and enforcement strategies.

6. Applicable AI Technologies in Trade Secret Protection

There has been much discussion worldwide about AI technologies. However, using AI tools to enhance trade secrets programs has not garnered much attention. Organizations can significantly strengthen their protection of trade secrets by strategically implementing AI tools across multiple aspects of their program.

AI technologies have significant advantages over traditional measures of protecting trade secrets. AI technologies have enhanced data analysis capabilities, pattern recognition, automated monitoring, predictive capabilities for risk and mitigation, efficient classification of risk, adaptive security measures, improved access control, faster incident response, and compliance management with prevailing law, which are lacking in traditional measures for the protection of trade secrets. They may not, however, be a complete replacement for conventional methods. Realizing this, organizations increasingly use AI technologies to enhance and complement existing security measures and create a more robust overall strategy for trade secret protection in an increasingly complex and threat-rich digital environment.

Companies providing solutions in the space, which as of this publication include businesses such as CrowdStrike, Fortinet, and Darktrace, are providing solutions incorporating AI technologies for threat detection, anomaly identification, and automated responses to potential security breaches that could compromise trade secrets and their protection, especially sensitive corporate data.

Organizations that have realized that one of AI's key advantages is its ability to learn and adapt to new threats may use multiple AI technologies that work in concert with the existing protection framework to create a comprehensive trade secret protection strategy. Many organizations have also appreciated the need for human expertise and decision-making when adopting and applying AI technologies.

AI technologies for trade secret protection broadly include:

6.1 Machine Learning

Machine learning is a subset of AI that has revolutionized the approach to trade secret protection. It incorporates pattern analysis, learning from vast amounts of data, and accurately and quickly identifying potential threats and anomalies. The ability to learn from data and make predictions or decisions is the essence of machine learning.

The key applications of machine learning in trade secret protection include:

- **Anomaly Detection**: Machine learning is an effective tool to identify unusual patterns in data sets and their access, file transfers, or employee/user behavior that may indicate a potential security breach or threat of leakage of trade secrets. Machine learning solutions, aim to establish users' standardized behaviors within an organization and bring any anomaly to the organization's attention. For instance, access to an unusually high number of confidential files by an employee outside of regular working hours is flagged as a potential threat to the organization. This assists organizations in planning and preparing appropriate rules and codes for data access, including trade secrets, thus preventing their leakage.

- **Predictive Analytics:** This involves analyzing historical data and current trends. Machine learning models can forecast potential risks to security and vulnerabilities in an organization's systems before they are exploited. One example included using machine learning for predictive threat detection to prevent an exfiltration attempt at a major European bank by identifying unusual data transfers before sensitive information could be compromised.

- **Labeling and Classification of Data**: Machine learning can categorize and label confidential and sensitive information. This assists organizations in ensuring that appropriate rules/codes are prescribed and that the appropriate security measures are applied to different types of trade secrets.

- **Adjusting Security Protocols**: Machine learning can assist in dynamically adapting security measures based on the nature, content, and context of data. This enables organizations to prepare and enforce a more nuanced and effective protection strategy, for example by automatically increasing security measures when patterns suggesting an attempt to access proprietary data are detected.

6.2 Data Science

Data science combines statistical analysis, mining, and machine learning to understand complex datasets. Data science plays a crucial role in trade secret protection in the following ways:

- **Data Collection and Analysis**: This process consists of gathering and processing relevant data from various sources, such as access logs, network traffic, and user behavior, to identify potential security risks. Data collection and analysis have effectively identified and prevented trade secret leakage in organizations, for example by associating data from various sources to identify employees leaking sensitive product designs to a competitor.

- **Reporting and Action**: Data science can enable organizations to prepare comprehensive reports based on which they can quickly identify and respond to threats. Various data visualization tools are available on the market. Organizations are using them to create

interactive dashboards for security monitoring, visualize access patterns, and quickly identify and address unusual activity that may indicate a threat to their trade secrets.

- **Decision-making Based on Data Insights**: Organizations are utilizing data insights to inform and optimize their security policies, to assist with efficient resource allocation, and to continuously improve protection measures. Data-driven security decisions have proven effective in improving trade secret protection policies.

- **Development of Predictive Models**: Organizations can utilize data science to develop sophisticated models to assess risks to their trade secrets, create early warning systems, and replicate potential attacks on their trade secrets. This type of prediction and prevention can occur well before organizations' traditional security systems could detect the threats.

7. Use Cases for AI Technologies in Trade Secret Protection

AI technologies' advanced monitoring and detection capabilities benefit organizations that want to monitor employee activities related to vital trade secrets, such as data collated during research and development, customer information, financial information, and strategic plans. AI systems can provide early warning of potential risks and leakages that may escape human observation in the usual course. These may include gradual increases in data downloads or unusual employee access patterns. Organizations can proactively protect their trade secrets while supporting compliance with legal requirements.

Because of their global scale and the volume of their trade secrets, the healthcare, hospitality, automotive, and financial sectors are most vulnerable to data breaches and leakages. These sectors are well-suited for adopting AI technologies to enhance their trade secrets programs.

The automotive industry is in the middle of a technological revolution, enabling the development of newer types of automobiles and related systems. This transformation has introduced new challenges to the protection of trade secrets. The threat exists to the industry as a whole. To protect against these threats, organizations in the automotive industry must

build greater security and resilience. An example is the Swedish state-backed research institute RISE's launch in 2022 of the RISE Cyber Test Lab for Automotive Cyber Security.

The healthcare industry faces increasing threats as actors are looking to target healthcare organizations for their highly confidential data and valuable information. Any data breach can have severe consequences, including the loss of sensitive patient data in addition to financial loss. Therefore, organizations providing healthcare services must understand the dangers of the potential threats and proactively protect themselves and their patients from potential harm. An example is the ransomware attack in 2022 on CommonSpirit Health, a large nonprofit hospital chain, which resulted in data belonging to more than 600,000 patients being compromised.[6]

The financial sector has always been a target of threats to its confidential information and trade secrets. Tools to extract confidential information, such as passwords and credentials from a system's memory, are often used to compromise an organization's intellectual assets. The use of AI technology can effectively predict threats and thus enable (or anticipate) the creation of additional layer(s) of protection against such threats in the financial sector (e.g., additional encryption of digits in financial reports and other similar strategies).

Apart from the specific industries discussed above, the case for the use of AI technologies in trade secret protection can easily be made for organizations of all sizes that have trade secrets that they wish to protect. The following are particularly effective strategies:

7.1 Active Identification of Trade Secrets

AI technologies can automatically scan and identify trade secrets within an organization's digital assets. Traditional methods of scanning and identifying trade secrets take time and effort; AI technologies enjoy a distinct advantage in carrying out these tasks efficiently. AI technologies can assist organizations by analyzing the content of documents, the metadata, and usage patterns, identifying new trade secrets that may be generated or acquired during

[6] https://www.bleepingcomputer.com/news/security/commonspirit-health-ransomware-attack-exposed-data-of-623-000-patients/

business, and continuously monitoring transferred data to detect potential leaks of sensitive information. For instance, organizations in the automotive industry may possess voluminous engineering drawings. AI technology may assist in scanning these voluminous documents across the organization's networks, successfully identifying previously unknown trade secrets in these documents, and protecting them from accidental disclosure.

7.2 Maintenance and Structuring of Trade Secrets

Once the trade secrets are identified, AI technology can automatically categorize and tag them based on their nature, importance, and sensitivity levels. Up-to-date records of these trade secrets can be maintained, and appropriate rules/regulations regarding their access can be prepared based on their classification. This intelligent data management through AI technology is most useful for large organizations. It prevents misclassification of documents and improves the strategy for protecting trade secrets.

7.3 Secured Storage of Trade Secrets

Once trade secrets are identified and categorized, the issue that requires attention is the storage of these trade secrets. AI technology can enhance the security of trade secret storage by creating and managing secure, encrypted repositories and implementing dynamic access control based on behavioral patterns and context. They can also generate secure and traceable references to trade secrets for use in less secure business environments.

7.4 Detection and prevention of unlawful access and disclosure of trade secrets

The capabilities of AI technologies to detect and prevent unlawful access and disclosure of trade secrets can be tapped by organizations to effectively protect their valuable trade secrets. AI technologies can be used for real-time analysis of access patterns to detect potential breaches, analysis of the behavior of employees and other members to identify threats to trade secrets inside the organization, and automated flagging or blocking of suspicious data transfers. As an example, Varonis Systems, Inc. used their system to detect and prevent a

potential trade secret theft at an organization operating urgent care clinics by identifying unusual file access by an employee.[7]

8. Benefits for Organizations Using AI Technologies in Trade Secret Protection

AI technologies offer organizations several advantages in the protection of their trade secrets. AI technologies enable organizations to create and implement a robust and dynamic environment for protecting trade secrets while improving detection and response capabilities for future threats, improved compliance within the organization, and significant cost savings due to automation and risk reduction. Implementing AI technologies for trade secret protection notably offers organizations the following advantages:

3.1 Enhanced Security

AI technologies' ability to process voluminous data in real-time vastly improves an organization's threat detection and prevention capabilities. For example, AI technology can reduce false positives, allowing users to focus on actual threats to trade secrets. As an example, Raytheon, a major defense contractor and industrial corporation, reported a significant reduction in inaccurate classification and threats to trade secrets after implementing AI technology-powered security tools.

3.2 Increased Efficiency

The automation of routine security tasks enables organizations to utilize their human resources better. This allows organizations to employ human resources to deal with more complex security threats that they may face.

3.3 Scalability

AI technologies can be scaled when organizations feel the need to protect the growing volume of trade secrets or to deal with higher threats. AI technologies can quickly adapt

[7] https://info.varonis.com/hubfs/Files/docs/research_reports/2021-Healthcare-Data-Risk-Report.pdf

and evolve depending on the nature and degree of the threat landscape. This is especially vital for certain organizations, such as those in the e-commerce space to help them maintain a robust protection system of their customer data and trade secrets even when the business is scaling quickly.

3.4 Predictive Power

AI technologies' predictive capabilities can enable organizations to identify and address potential weaknesses in trade secret management before these vulnerabilities are discovered and exploited to the organization's detriment.

3.5 Compliance with Laws and Regulations

AI technologies can help organizations adhere to data protection regulations such as GDPR, as well as internal regulations, by automating compliance checks and documentation.

3.6 Efficiency

The use of AI technologies in trade secret protection enables organizations to create efficiencies in terms of money and human resources. Initial implementation of AI technologies requires some investment; however, this must be weighed against the consequences an organization may face because of trade secret leakage.

9. Legal Implications of Using AI Technologies in Trade Secret Protection

While Section I of this paper deals with regulations regarding the use of AI technologies in protecting trade secrets, this section aims to briefly analyze the legal implications arising from using such technologies.

The use of AI technologies in trade secret protection introduces complex legal obligations. Such use raises important questions regarding the evolving standards of what constitutes reasonable measures for the protection of trade secrets under the law. Over time and with

increased usage, AI technologies may become an essential part of the reasonable measures that are required by organizations to categorize and protect a document as a trade secret. Organizations deploying AI technologies for trade secret protection will also need to plan for new forms of liability and legal risks. For example, organizations must consider potential liability for technology failures, including situations wherein AI technology gives a false positive, leading to wrongful accusations against employees for breach of trade secrets. Businesses must also ensure that the AI technologies and their results can satisfy legal inquiries while maintaining credible documentation to support any potential litigation.

The use of AI technologies creates a complex legal landscape where organizations will need to weigh the benefits of AI use against increased legal exposure and obligations. Legal exposure and obligations may arise, especially in the following fields:

4.1 Confidentiality

Maintaining the confidentiality of trade secrets while using AI technology is a challenge an organization may face. To overcome this challenge, AI technologies must be designed and implemented to maintain the confidentiality of the very trade secrets they protect. Care must be exercised by organizations using AI technologies to ensure that the technology they use does not inadvertently expose trade secrets through their outputs and decision-making processes. This may be achieved by having robust confidentiality clauses pertaining to trade secrets in contracts with providers of the AI technology processing the trade secrets.

4.2 Data Privacy

Data privacy is another critical aspect that organizations must consider when using AI technology to protect trade secrets. The review, monitoring, and analysis of data using AI technology must comply with the prevailing data protection regulations, such as the GDPR. Organizations must frame clear policies on data collection and usage by the AI technology systems they use and balance the need to protect their trade secrets and employee privacy rights, especially when monitoring communications and usage behavior.

4.3 Enforcement

Another relevant issue is the use and admissibility of evidence generated by AI technologies in court actions. While rules and practices to handle electronic evidence have been developed, evidence generated by AI technologies has added a new layer of complexity relating to reliability, transparency, interpretability, and bias in such evidence. Apart from the numerous risks regarding the authenticity and reliability of such evidence, the lack of transparency in AI algorithms is also a significant issue. Bias in the training data of AI systems can also lead to discriminatory results. The absence of standardized guidelines for verifying evidence generated by AI technology further complicates the issue. Therefore, organizations should be prepared to explain and defend the outcomes of the AI technology they use if they are adduced in evidence.

Conclusion

Trade secrets are an essential component of intellectual property law, offering businesses a flexible and powerful tool to protect their valuable, confidential information. The TRIPS Agreement has been instrumental in shaping international trade secret protection. In the European Union, the TRIPS Agreement influenced the development of harmonized laws through Directive 2016/943. For the United States, being a signatory to the TRIPS Agreement eventually led to the passage of the Defend Trade Secrets Act, which provides a robust federal framework, allowing companies to protect their trade secrets in an increasingly competitive global market. The TRIPS Agreement has also inspired the Anti Unfair Competition Law in China, and other regions such as India are considering adopting specific regulations (Protection of Trade Secrets Bill, 2024) for the protection of trade secrets.

Trade secret protection can be a more efficient and effective protection mechanism than some other forms of IP protection, because it does not have the same potential requirements for protection as those other forms of protection, for example, a trade secret does not need to be created by a human being. Also, trade secrets can protect certain kinds of information—such as large data sets—that would not be eligible for protection under the other types of intellectual property laws.

With the acknowledgement of trade secret protection via international treaties and many domestic laws, organizations have the opportunity to use AI for both trade secret protection and trade secret generation. In doing so, there should be an understanding of both the benefits and challenges that come with the use of such technology, for example, ensuring that misappropriation of trade secrets does not occur and that trade secret protection policies do not become a burden for the employees of an organization.

.

The adoption and use of AI technologies—particularly machine learning and data science— to protect trade secrets and devise strategies for such protection, offers a powerful new approach to organizations across various industries to safeguard their valuable intellectual property. AI technologies assist organizations in proactively identifying and securing trade secrets; developing and maintaining robust protection measures; and detecting and preventing unauthorized access or disclosure, or any potential threat of such disclosure. AI technologies have proven themselves to be valuable organizational tools, from preventing insider threats in financial institutions to safeguarding proprietary information in the manufacturing industry.

As threats to trade secrets continue to evolve due to technological advancements, embracing AI technologies will become increasingly essential for organizations seeking to maintain their competitive edge in the marketplace. Organizations must be at the forefront of these technological advancements to secure their trade secrets. Undoubtedly, the benefits of AI technology in protecting trade secrets are significant. However, organizations must be wary of such technology's legal and ethical implications. They need to develop the means to navigate these challenges.

Proper implementation of AI technologies, with consideration for confidentiality, data privacy, and legal enforcement, is crucial for realizing the full potential of these technologies in the critical task of trade secret protection. Organizations that can do this and successfully navigate the complex challenges posed by AI technologies will be well-positioned to protect their valued trade secrets and maintain their innovative edge.