Educational Administration: Theory and Practice
2024, 30(1), 6654-6660
ISSN: 2148-2403
https://kuey.net/

Research Article

A Comparative Analysis Of Trade Secret Protection In The Usa, Uk, Australia, And India: Best Practices Adoption In India

Janist Dhanol[1]*, Dr. Pradip Kumar Kashyap[2]

[1]*Research Scholar, Raffles ,University, Neemrana Janist10@gmail.com
[2]Assistant Professor of Law Raffles University, Neemrana pradiprgnul@gmail.com

Citation: Janist Dhanol, et.al (2024). A Comparative Analysis Of Trade Secret Protection In The Usa, Uk, Australia, And India: Best Practices Adoption In India, *Educational Administration: Theory and Practice*, 30(1) 6654-6660
Doi: 10.53555/kuey.v30i1.9972

ARTICLE INFO

ABSTRACT

Trade secrets constitute a significant category of intellectual property that provides enterprises across diverse industries with a substantial competitive edge. Comprehending and effectively protecting these sensitive assets is essential as globalization accelerates. This research article compares the legislative frameworks for trade secret protection in four prominent jurisdictions: the United States of America, the United Kingdom, Australia, and India. This study aims to evaluate the merits and drawbacks of each region's distinct strategy through an analysis of its statutory provisions, common law principles, and landmark case laws. Furthermore, it examines optimal strategies for the management and safeguarding of trade secrets, subsequently proposing potential legal and practical measures to enhance India's existing trade secret framework. The United States, United Kingdom, and Australia's experiences inform these tactics. This comparative analysis aims to establish a more robust and efficient framework for safeguarding trade secrets in India, thereby fostering innovation and economic growth.

Keywords: Trade Secrets, Intellectual Property, Comparative Law, USA, UK, Australia, India, Best Practices, Case Law, Legal Framework, Protection, Misappropriation.

INTRODUCTION

In today's knowledge-driven economy, trade secrets have emerged as crucial assets for corporations, often surpassing the value of patents and trademarks in certain instances. Trade secrets remain undisclosed, unlike other forms of intellectual property, and their economic value derives from their secrecy. They provide holders with a significant competitive advantage and encompass a broad spectrum of sensitive information, including designs, processes, calculations, client lists, and marketing strategies.

Different legal systems, economic goals, and approaches to intellectual property rights lead to major differences in how countries protect trade secrets. This study compares the legislative frameworks for trade secret protection in four significant jurisdictions: the United States of America, the United Kingdom, Australia, and India. These jurisdictions exemplify several legal systems: India's evolving legal framework, predominantly founded on common law; the United States, characterized by a robust statutory structure; and the United Kingdom and Australia, which depend on common law principles supplemented by specific legislation.(1)

- The main goals of this study are to provide a detailed comparison of the laws and rules that protect trade secrets in the United States, the United Kingdom, Australia, and India, and to identify the best practices for managing and protecting trade secrets used in these countries.
- To enhance India's trade secret framework, it is suggested that analogous principles be implemented. This entails examining significant case law and legal precedents that have influenced the interpretation and enforcement of trade secret rights in the USA, UK, and Australia.
- This study seeks to enhance comprehension of the international trade secret protection framework and

provide critical insights for enterprises operating in India, legal professionals, and policymakers. India can foster innovation, attract investment, and enhance equitable competition through a robust and well-delineated trade secret framework.

LEGAL FRAMEWORK FOR TRADE SECRET PROTECTION

This section provides a comparative overview of the legal frameworks governing trade secret protection in the USA, UK, Australia, and India.

INDIA

Since India doesn't have specific laws for trade secrets, courts have used general legal principles and interpreted restrictions in job contracts according to Section 27 of the Indian Contracts Act, 1872, to protect trade secrets. Judicial bodies have affirmed the constitutionality of secrecy and non-compete clauses, determining that these restricted agreements are permissible. (2)

Negative covenants that prohibit commerce, trade, or self-employment are not considered trade restrictions unless they are too severe, unethical, biased, or unreasonable. Employee limitations should not be too burdensome or severe, nor should they exceed what is necessary to safeguard the employer's interests. Employees who acquire sensitive information during their employment and subsequently violate their confidentiality agreements have faced court-issued injunctions. Courts have imposed injunctions and penalties on parties for breaches of confidence and equitable principles concerning the misuse of sensitive information in the absence of a basic contract between employer and employee.

In instances where workers or third parties have unlawfully acquired trade secrets under coercion, the Supreme Court has issued injunctions as a remedy. The Supreme Court has safeguarded trade secrets from unavoidable exposure in legal proceedings. The court asserts that public trials must be regulated to guarantee that the involved parties obtain genuine justice, and maintaining the confidentiality of trade secrets during legal processes does not contravene Article 19. (3)

India lacks a comprehensive statute safeguarding trade secrets. Common law standards on breach of confidence and contractual obligations generally govern the protection of trade secrets and private information. Since there are no specific laws about trade secrets in India, courts have used common law rules and interpreted restrictions in employment contracts to protect trade secrets. Judicial bodies have affirmed the constitutionality of secrecy and non-compete clauses, determining that these restricted agreements are permissible. Negative covenants that prohibit commerce, trade, or self-employment are not considered trade restrictions unless they are too severe, unethical, biased, or unreasonable.

Employee limitations should not be too burdensome or severe, nor should they exceed what is necessary to safeguard the employer's interests. Employees who acquire sensitive information during their employment and subsequently violate their confidentiality agreements have faced court-issued injunctions. Courts have imposed injunctions and penalties on parties for breaches of confidence and equitable principles concerning the misuse of sensitive information in the absence of a basic contract between employer and employee. In instances where workers or third parties have unlawfully acquired trade secrets under coercion, the Supreme Court has issued injunctions as a remedy.

The Supreme Court has safeguarded trade secrets from unavoidable exposure in legal proceedings. The court asserts that public trials must be regulated to guarantee that the involved parties obtain genuine justice, and maintaining the confidentiality of trade secrets during legal processes does not contravene Article 19.

India lacks a comprehensive statute safeguarding trade secrets. The protection of trade secrets and private information is generally governed by common law standards on breach of confidence and contractual obligations.(4)

Definition of Trade Secret (Implied):

In accordance with English common law, Indian courts acknowledge the necessity of safeguarding secret information. The primary factors are the confidentiality of the material, whether the conditions of its transmission suggested an obligation of confidentiality, and if the owner experienced detriment due to its unauthorized use or distribution. India lacks an established definition of a trade secret.

Violation of Confidentiality:

In India, equitable principles and contractual duties form the foundation of the concept of breach of confidence. Contracts such as non-disclosure agreements (NDAs) may explicitly articulate a duty of confidentiality, or it may be inferred from the connection between the parties (e.g., employer-employee, business partners). Indian courts may provide remedies for breach of trust, including damages to compensate for losses, injunctive action to prevent further disclosure or use, and, in certain instances, an account of profits. The implementation of these remedies is sometimes obstructed by ambiguous regulatory requirements and procedural delays.

Limited Statutory Recognition:
Although there is no explicit trade secret legislation, certain Indian regulations now address elements of sensitive information. The Information Technology Act of 2000 defines data security and protection, which may be indirectly associated with safeguarding digital trade secrets. Moreover, contractual obligations are enforceable under the Indian Contract Act of 1872, specifically regarding confidentiality and non-compete provisions in employment agreements. The proposed National Innovation Act, if enacted, may establish a more extensive framework for safeguarding intellectual property, potentially extending beyond patents and trademarks to encompass trade secrets.

The Bombay High Court stated in ***VFS Global Services Pvt. Ltd. v. Mr. Suprit Roy***(5) that the use of trade secrets during or after termination of employment is not protected by section 27. In a significant decision, the Delhi High Court set certain requirements for filing a lawsuit for trade secret infringement. These requirements include illegal disclosure, asking an employee to divulge information, and a licensee breaking a condition. Usually, the owners have access to injunctions, damages, and compensation as remedies. A secret is no longer a secret once it is revealed.
Due to a lack of specific laws and an excessive dependence on antiquated common norms, the Indian market has become unduly vulnerable for multinationals, especially those in the chemical and pharmaceutical industries. Many multinational corporations have shown a strong reliance on trade secret protection laws in the fiercely competitive environment. This is the main cause of the sharp drop in significant foreign direct investments in India.

UNITED STATES OF AMERICA (USA)

The Uniform Trade Secret Act (UTSA) and the Economic Espionage Act of 1996 (EEA) are significant statutes regulating trade secrets in the United States. The UTSA forbids the unauthorized commercial exploitation of trade secrets, whereas the EEA empowers the Attorney General to initiate criminal proceedings against people for misappropriation. The UTSA and EEA are the principal legislation regulating trade secrets in the United States, with more than 25 states enacting their own criminal laws pertaining to trade secrets. Remedies for misappropriation encompass injunctions, damages, and legal fees. The EEA enforces fines and incarceration as sanctions under criminal law. Civil and criminal proceedings are established to protect trade secrets, with courts offering comprehensive discovery processes.(6)

Definition of Trade Secret:
The DTSA comprehensively characterizes trade secrets as "all forms and types of financial, business, scientific, technical, economic, or engineering information, encompassing patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, regardless of their tangible or intangible nature, and irrespective of the manner in which they are stored, compiled, or memorialized—physically, electronically, graphically, photographically, or in writing—if (A) the owner has implemented reasonable measures to maintain the confidentiality of such information; and (B) the information possesses independent economic value, either actual or potential, by virtue of not being generally known to, or readily ascertainable through proper means by, another individual who could derive economic benefit from its disclosure or utilization." This notion emphasizes the economic worth of information alongside its confidentiality.
Misappropriation:
Under the DTSA, misappropriation encompasses acquiring a trade secret through unethical methods, disclosing or utilizing it without authorization by an individual who was aware or should have been aware of its unethical acquisition, in situations that imposed an obligation to uphold confidentiality or limit its use, or from an individual who employed such unethical methods. (7)
The DTSA provides various remedies for trade secret misappropriation, including monetary damages (actual loss and unjust enrichment), both preliminary and permanent injunctive relief, and exemplary damages up to twice the actual damages, along with legal fees in instances of willful and malicious misappropriation. The DTSA has a specific "whistleblower" provision that protects individuals from legal consequences for lawfully disclosing a trade secret to an attorney or government official solely for the purpose of reporting or investigating a potential legal violation.
State legislation: State laws, mostly based on the UTSA, significantly impact trade secret litigation, notwithstanding the federal protection provided by the DTSA. The DTSA and UTSA possess analogous definitions of misappropriation and trade secret.
The principle that improper means of obtaining a trade secret, such as aerial photography of a competitor's plant under construction, constitute misappropriation even in the absence of a breach of a confidential relationship was established in the case of ***E.I. du Pont de Nemours &***

Co. v. Christopher,(8) This emphasizes how crucial it is to defend trade secrets against industrial espionage. Possible Adoption in India: A similar strategy might be used by Indian courts to acknowledge that obtaining trade secrets by illegal or unethical means—even in the absence of an established confidential relationship—represents a breach of trade secret rights.

Digital Transactions, Inc. v. Integrated Cash Management Services, Inc.,(9): This case made it clear that the owner of a trade secret must take reasonable steps to keep it hidden. The court ruled that a product's public presentation without confidentiality constraints may render trade secret protection null and void. Possible Adoption in India: Similar emphasis should be placed by Indian courts on the need for trade secret owners to actively safeguard their proprietary data using appropriate security methods in order to qualify for legal protection. ***Waymo LLC v. Uber Technologies, Inc.(10)***: Allegations of trade secret theft pertaining to self- driving car technology were at the center of this well-known case. Even though it was resolved, it demonstrated the importance of trade secrets in innovative fields and the possibility of large losses in cases involving misappropriation.

Possible Adoption in India: This case emphasizes how Indian courts must be prepared to deal with intricate trade secret issues involving cutting-edge technologies and to acknowledge the possibility of serious financial loss due to misappropriation.

UNITED KINGDOM (UK)

The United States possesses the most sophisticated codified legislation governing trade secrets, with the Uniform Trade Secrets Act of 1970 establishing unified regulations for states. Trade secrets possess commercial value, are known to a restricted group, and are maintained in confidentiality. Nevertheless, because to interstate and international challenges, federal legislation was enacted, including the Defence Trade Secret Act of 2016 and the Economic Espionage Act of 1996. These regulations penalize the misappropriation or theft of proprietary information while permitting individuals to investigate it through their abilities and diligence.(11)

The European Union abides by the Directive on the Protection of Trade Secrets in addition to the TRIPS Agreement and the Paris Principles. 2016 saw the approval of a new Directive pertaining to the protection of confidential information and know-how, which established a uniform definition of "Trade Secrets." This phrase is very similar to what is offered in TRIPS and UTSA. The order outlines damages and compensation, taking into consideration the owner's losses as well as the offender's unfair profits overall. In order to serve as a social deterrent, further legal remedies include injunctions that forbid the use of information, the destruction of trade secret documents or records, and the public announcement of decisions. Unintentional acquisition of concealed information is permitted by English law. The Commission's Draft Bill's Clause II (I) ignores the defendant's responsibility in situations when the disclosure of private information creates problems for the public interest. Similar to this, a defendant may provide information to a legitimately interested party as a result of a legal requirement or in the interest of national security.

Confidentiality clubs are essential in the UK for preventing unwanted publication of private information. The idea is to restrict access to sensitive information to a small group of opponents. One well-known example is the External Eyes-Only Club, which limits the sharing of secrets to specific people, like supporters or experts from the opposing side. Only in exceptional situations are these extremely stringent EEO Clubs permitted to be implemented.(12)

There isn't a specific law in the UK that addresses trade secret protection entirely. Common law laws, particularly the tort of breach of confidence, are primarily responsible for protecting trade secrets.(13)

Definition of Trade Secret: The judiciary has developed a three-part standard for information to be considered confidential and possibly protected as a trade secret, despite the lack of a statutory definition:

- The information must have the necessary quality of confidentiality;
- It must have been disclosed under circumstances imposing a duty of confidentiality; and
- There must be an unauthorized use of that information to the detriment of the disclosing party. Compared to the legislative definition in the US, this term is more flexible and fact-based. When a duty of confidentiality is in place and confidential information is disclosed or used without authorization, it is considered a breach of confidence tort.

This duty could result from a fiduciary relationship, a contractual relationship (such as employment contracts or non-disclosure agreements), or the nature of the information itself. In the UK, remedies for breach of confidence include an account of profits, compensatory and

often aggravated damages, and injunctive remedies. The specific facts of the case will determine the availability and scope of these remedies.

Regulations on Trade Secrets (Enforcement, etc.) 2018: Through the Trade Secrets (Enforcement etc.) Regulations of 2018, the UK implemented the EU Trade Secrets Directive. These rules define trade secrets more uniformly and lay out minimal requirements for remedies in cases where trade secrets are acquired, used, or disclosed illegally. The word closely resembles the DTSA, which stipulates that the information must be exclusive, have commercial value because of its proprietary nature, and be safeguarded by reasonable steps taken by the possessor to keep it secret.

AUSTRALIA

Australia, the smallest and lowest-lying continent globally, possesses a common law legal system akin to that of England. Australian law safeguards all commercially significant trade secrets, irrespective of their classification as technical or non-technical business information. The term "trade secrets" is shaped by significant English judicial rulings, notably ***Coco v. A.N. Clark (Engineers) Ltd.,***(14)which delineates three criteria for a breach of confidence: the information must be misappropriated to the detriment of the disclosing party, possess the requisite quality of confidentiality, and be revealed under conditions suggesting a duty of confidentiality.

Trade secrets denote more specialized, detailed, and proprietary information than "know-how." Trade secrets and many forms of corporate information, including data on medications, contraceptives, customer histories, building fit-out specifications, test findings, informant identities, and plant cuttings, are rigorously safeguarded by Australian law. Courts assess the plaintiff's attempts to get information and the plaintiff's degree of awareness within the organization, both domestically and globally.

No explicit criminal penalties exist for safeguarding "trade secrets." Disclosing information in breach of a legal obligation constitutes a felony, irrespective of the discloser's intent or the damage inflicted upon the claimant. Like the UK, Australia lacks a comprehensive federal statute that explicitly governs trade secrets. The principles of common law, especially the equitable doctrine of breach of confidence, serve as the primary source of protection.

Definition of Trade Secret (Implied): Australian courts align with the UK approach, necessitating that the knowledge exhibits secrecy, is conveyed under circumstances that impose an obligation of confidence, and is vulnerable to unauthorized use or disclosure. Factors evaluated in establishing secrecy encompass the type of the information, the context of its communication, and the degree of its dissemination beyond the owner's enterprise.

Breach of Confidence: In Australia, the notion of breach of confidence safeguards confidential information that has been divulged or utilized in violation of a duty of confidence. This obligation may originate from contract, equity, or the inherent nature of the relationship between the parties.

Remedies: Available remedies for breach of confidence in Australia encompass injunctive relief, damages, account of profits, and the return or destruction of confidential materials. The courts possess extensive discretion in awarding various remedies contingent upon the particular facts of the case.

Limited Statutory Provisions: Although there is no comprehensive trade secret legislation, certain specific statutes, such as the Corporations Act 2001 (Cth), include provisions that may indirectly safeguard confidential information in particular contexts, especially regarding employee behavior and the misuse of corporate information.

COMPARATIVE ANALYSIS: STRENGTHS AND WEAKNESSES(15)

A comparative analysis of the trade secret protection frameworks in the USA, UK, Australia, and India reveals distinct strengths and weaknesses in their respective approaches.

Strengths:

USA: The DTSA provides a clear federal statutory framework, offering greater predictability and uniformity in trade secret protection across states. The explicit definition of trade secret and misappropriation reduces ambiguity. The whistleblower provision offers a unique balance between protecting trade secrets and encouraging reporting of unlawful activities. The availability of federal jurisdiction can streamline litigation in cases involving interstate misappropriation.

UK: The common law principle of breach of confidence offers flexibility in adapting to various factual scenarios. The implementation of the EU Trade Secrets Directive through the 2018

Regulations provides a more harmonized definition and minimum standards for remedies, aligning it closer to statutory frameworks.

Australia: Similar to the UK, the equitable doctrine of breach of confidence provides a flexible mechanism for protecting confidential information. The courts have demonstrated a willingness to adapt the principles to address evolving business practices.

India: The reliance on established common law principles of breach of confidence provides a foundational basis for protecting trade secrets. The enforceability of contractual confidentiality clauses offers a degree of protection, particularly in defined relationships.

Weaknesses:

USA: While the DTSA provides federal protection, the interplay with state laws based on the UTSA can sometimes lead to complexities. The broad definition of trade secret requires careful application by courts.

UK: The reliance on common law can lead to less predictability compared to statutory frameworks. The definition of confidential information can be fact-dependent and less precise. Enforcement can sometimes be challenging without specific statutory provisions.

Australia: Similar to the UK, the absence of a comprehensive trade secret statute can result in less clarity and predictability. The application of equitable principles can be discretionary.

India: The lack of a specific statute dedicated to trade secrets creates significant uncertainty and inconsistency in enforcement. The definition of trade secret is not clearly codified. Remedies can be less robust and enforcement can be slow and cumbersome. The existing legal framework may not adequately address the complexities of modern business practices and cross-border misappropriation.

BEST PRACTICES IN TRADE SECRET MANAGEMENT AND PROTECTION(16)

Regardless of the specific legal framework, implementing robust best practices is crucial for effectively protecting trade secrets. This section highlights some key best practices adopted in the USA, UK, and Australia that could be particularly relevant for businesses operating in India.

- ***Identification and Classification of Trade Secrets:*** Businesses should proactively identify and classify information that constitutes trade secrets. This involves conducting audits to map valuable confidential information across different departments and systems. Clear labeling and documentation of trade secrets are essential.
- ***Implementing Reasonable Security Measures:*** Taking reasonable steps to maintain the secrecy of trade secrets is a fundamental requirement for legal protection in most jurisdictions, including the USA (under DTSA and UTSA), the UK (under the Trade Secrets Regulations 2018), and implicitly under the common law in the UK and Australia. These measures can include:
- ***Physical Security:*** Limiting access to premises, secure storage of sensitive documents, and implementing visitor management protocols.
- ***Cybersecurity:*** Implementing strong password policies, encryption, firewalls, intrusion detection systems, and data loss prevention tools.
- ***Document Control:*** Restricting access to sensitive documents (both physical and electronic), using confidentiality markings, and implementing document destruction policies.
- **Establishing Confidentiality Agreements (NDAs):** Utilizing well-drafted Non- Disclosure Agreements (NDAs) with employees, contractors, business partners, and other third parties who may have access to trade secrets is crucial. NDAs should clearly define the confidential information, the obligations of the receiving party, and the duration of the confidentiality obligations.
- ***Employee Training and Awareness:*** Educating employees about the importance of trade secrets, the company's confidentiality policies, and their obligations regarding confidential information is essential. Regular training can help prevent accidental disclosure or misuse of trade secrets.
- ***Access Control and Need-to-Know Basis:*** Limiting access to trade secrets on a need-to- know basis within the organization is a fundamental security principle. Implementing role-based access controls in IT systems and physical access restrictions can help achieve this.
- ***Monitoring and Auditing:*** Regularly monitoring employee access to sensitive information and conducting periodic audits of security measures can help detect potential breaches or vulnerabilities.
- ***Exit Interviews and Post-Employment Obligations:*** Conducting thorough exit interviews with departing employees to remind them of their confidentiality obligations and ensuring that they return all confidential information is crucial. Enforceable post-employment restrictive covenants (e.g., non-compete, non-solicitation clauses), where legally permissible, can also provide additional protection.
- ***Incident Response Plan:*** Developing a clear incident response plan to address potential trade secret misappropriation incidents is essential for minimizing damage and ensuring timely and effective action. This plan should outline procedures for investigation, containment, notification, and legal action.

REFERENCES

1. Zubair Ahmed, “Protection of Trade Secrets in India A Study of the Legal Framework”. Available at: https://shodhganga.inflibnet.ac.in/handle/10603/291861
2. F. Schultz and Douglas C. Lippoldt, “Approaches to Protection of Undisclosed Information (Trade Secrets): Background Paper”, Paper No. 162, 2014 OECD Trade Policy, OECD Publishing, Paris, p.298.
3. Mukesh Shukla, “Non Regulation Of Protection Of Trade Secrets In The Indian Corporate Sector A Comparative Analysis With USA Through The Lens Of Global IPR Regime”, https://shodhganga.inflibnet.ac.in/handle/10603/362381
4. Mark F. Schultz and Douglas C. Lippoldt, “Approaches to Protection of Undisclosed Information (Trade Secrets): Background Paper”, Paper No. 162, 2014 OECD Trade Policy, OECD Publishing, Paris, p. 215.
5. James McQuade, Kayvan Ghaffari and Andrea Nicole Greenwald, Can You Keep A Secret? The European Union’s New Directive on Trade Secrets and its Impacts on Whistleblowers, Trade Secrets Watch.
6. Chandni Raina Trade Secret Protection in India: The Policy Debate , Centre for WTO Studies, Indian Institute of Foreign Trade New Delhi , Working Paper CWS/WP/200/22 (2015).

a. peal Number 533 of 1998 79 Base International Holdings v. Pallava Hotels Corporation Limited , C.S. No. 802 of 1996, Original Application Nos. 653 and 654 of 1996 and 104 of 1997 and Application No. 1464 of 1997 (1998)

7. 431 F.2d 1012 (5th Cir. 1970).
8. 920 F.2d 171 (2d Cir. 1990)
9. (N.D. Cal. 2018), Case No. C 17-0939 WHA
10. Saltman Engineering Co., Ltd. v. Campbell Engineering Co., Ltd 3 All E.R. 413,415. (1963)
11. Sreenivasulu N S, TRIPS complaint intellectual Property Regime in India: Implication of TRIPS in modifying the cantors and canons of our system, Manupatra Intellectual Property Reports, 3 (2) 2007 A-79- 80.
12. T.Q. Delta LLC v. Zyxel Communications U.K. Ltd., 2018 EWHC 1515.
13. Niranjan Shankar Golikari v.Century Spinning and Manufacturing Co. Ltd., 1967 AIR 1098.
14. VFS Global Services Pvt. Ltd. v. Mr. Suprit Roy, 2008 (2) BomCR 446.