COMPARATIVE ANALYSIS OF TRADE SECRET PROTECTION UNDER THE U.S. AND INDIAN LEGAL SYSTEMS

A Dissertation submitted to the National University of Advanced Legal Studies, Kochi, in partial fulfilment of the requirements for the award of an L.L.M. Degree in International Trade Law.

THE NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES

Kalamassery, Kochi – 683503,

Kerala, India 2024-2025

Submitted by: NIRMAL MARY

(Reg. Number: LMO224018)

Under the Guidance and Supervision

Asst. Prof. Hari S. Nayar

May 2025

CERTIFICATION

This is to certify that **Ms. NIRMAL MARY, Reg. No: LM0224018,** has submitted her Dissertation titled ***"Comparative Analysis of Trade Secret Protection under the U.S. and Indian Legal Systems"*** in partial fulfilment of the requirement for the award of the Degree of Master of Laws in International Trade Law to the National University of Advanced Legal Studies, Kochi, under my guidance and supervision. It is also affirmed that the dissertation she submitted is original, bona fide, and genuine.

Date: 28.05.2025
Place: Ernakulum

ASST. PROF. HARI S. NAYAR
GUIDE AND SUPERVISOR
NUALS, KOCHI

DECLARATION

I, Nirmal Mary, declare that this Dissertation titled ***"Comparative Analysis of Trade Secret Protection under the U.S. and Indian Legal Systems"*** is researched and submitted by me to the National University of Advanced Legal Studies, Kochi, in partial fulfilment of the requirement for the award of Degree of Master of Laws in International Trade Law, under the guidance and supervision of **Mr. Hari S. Nayar**, Assistant Professor and is an original, bona fide and legitimate work and it has been pursued academic interest. This work or any type thereof has not been submitted by me or anyone else for the award of another degree from this University or any other University.

Date: 28.05.2025
Place: Ernakulam

Nirmal Mary
Reg. No: LM0224018
LL.M (International Trade Law)
National University of Advanced Legal Studies, Kochi, Kerala

ACKNOWLEDGEMENT

I want to express my gratitude to the Almighty, who gave me strength and showed me the path towards achieving high ends while writing this dissertation. The amount of work undertaken for this dissertation was challenging and very exciting; this could not have been possible without the efforts and contributions of many people. I want to express my sincere thanks to my guide and supervisor, **Mr. Hari S. Nayar,** for his valuable guidance and suggestions throughout my research. His supportive spirit and encouragement led to the successful completion of this dissertation.

I would like to express my deepest gratitude to **Hon'ble Mr. Justice S. Siri Jagan (Retd.),** Acting Vice-Chancellor of NUALS, for his invaluable guidance and support throughout my research. I take this opportunity to thank **Dr. Anil R Nair,** Professor and Director of the Centre for Parliamentary Studies and Law Reforms at the National University of Advanced Legal Studies, Kochi, for all the help and encouragement that he has given. His insights and encouragement have been instrumental in shaping this dissertation.

I would also like to thank the **NUALS Faculty** for their assistance in selecting a topic for this dissertation and highlighting some significant developments in International trade. Also, I would like to extend my gratitude to all the faculty members who have guided me and helped me to put my ideas into words.

I want to thank all the **library staff** for their timely assistance in assessing all the sources and for their immense cooperation.

NIRMAL MARY

PREFACE

In the age of knowledge-driven economies and rapid global innovation, protecting intellectual assets has become central to national competitiveness and corporate survival. Amidst the more visible forms of intellectual property like patents and copyrights, trade secrets represent a quieter but equally powerful engine of economic value, guarding algorithms, client databases, manufacturing techniques, and formulas that define a business's edge. This vital yet underexplored area of intellectual property drew me to undertake this dissertation on the comparative legal frameworks of trade secret protection in the United States and India. As an LL.M. student specialising in International Trade Law at the National University of Advanced Legal Studies, I have been consistently drawn to the intersections between commerce, innovation, and legal governance. Trade secrets sit at the confluence of these forces, and their growing significance in cross-border business transactions made it imperative to understand how different jurisdictions uphold or neglect these protections. My particular interest stemmed from observing India's reliance on scattered common law principles, contractual remedies, and judicial discretion, which are in stark contrast to the United States' legislative mechanisms like the UTSA and DTSA.

This dissertation explores the doctrinal and statutory variations between the two countries and the more profound implications of these differences for innovation, foreign investment, and compliance with international commitments like the TRIPS Agreement. Through critically examining judicial decisions, statutory frameworks, and policy debates, I have attempted to answer whether India's current approach is sufficient or risks falling short in a world where commercial confidentiality is paramount.

The structure of the dissertation reflects this exploration: Chapter 1 introduces the concept and importance of trade secrets; Chapter 2 outlines the legal and theoretical frameworks underpinning their protection; Chapter 3 provides a comparative analysis between U.S. and Indian laws; Chapter 4 reviews significant judicial precedents; and Chapter 5 offers conclusions and policy recommendations aimed at legislative reform.

In an era where data is the new oil and innovation is the currency of economic growth, securing trade secrets is not just a legal formality but a strategic imperative. This study hopes to contribute to the ongoing dialogue about how countries like India can better align their intellectual property regimes with global standards while fostering an ecosystem that protects creativity, competitiveness, and confidentiality.

LIST OF ABBREVIATIONS

Abbreviation	Full Form
AI	Artificial Intelligence
DTSA	Defend Trade Secrets Act
EEA	Economic Espionage Act
FTC	Federal Trade Commission
GATT	General Agreement on Tariffs and Trade
IoT	Internet of Things
NAFTA	North American Free Trade Agreement
NDA	Non-Disclosure Agreement
OECD	Organisation for Economic Co-operation and Development
R&D	Research and Development
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UTSA	Uniform Trade Secrets Act
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

TABLE OF CASES

20. Magnesita Refractories Co. v. Mishra, No. 2:17-cv-358, 2018 WL 620444 (W.D. Pa.)

21. Microsoft v. Commission, (2007) ECR II 3601

22. Mitsubishi Chemical Corporation v. Nippon Kayaku, Tokyo District Court (Japan)

23. PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995)

24. Pepsi Foods Ltd. v. Bharat Coca-Cola Pvt. Holdings Ltd., ILR 1999 Delhi 193

25. Rochem Separation Systems (India) Pvt. Ltd. v. Nirtech Pvt. Ltd., 2023 SCC OnLine Bom 493

26. Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984)

27. Unitherm Food Systems, Inc. v. Hormel Foods Corp., 546 U.S. 394 (2006)

28. United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012)

29. United States v. Steven L. Davis, 183 F.3d 231 (3d Cir. 1999)

30. Vancouver Malt & Sake Brewing Co. Ltd. v. Vancouver Brewing Ltd., (1934) UKPC 9

31. Vestergaard Frandsen v. Bestnet Europe Ltd., [2013] UKSC 31

32. Zee Telefilms Ltd. v. Sundial Communications Pvt. Ltd., 2003 (27) PTC 457 (Bom)

TABLE OF CONTENTS

CHAPTER 1

Introduction

The TRIPS Agreement (1994) defines trade secrets as confidential information with commercial value, protected through reasonable secrecy measures, establishing its importance in global commerce. Trade secret protection began with common law principles emphasising contractual obligations and fiduciary duties. The Trade Secret business, its security and growth are in full swing, along with its theft and litigation. With the origin of the 'internet', globalisation was happening, and the protection of intangible assets has become a primary issue for all-sized enterprises. The people engaged in intellectual property related to research focusing on economics. When evaluating the value of the assets, it can often be seen that the value of its tangible assets cannot exceed that of its intangible assets.[1]

Trade secrets are relatively recent intellectual property in India, yet they do not represent a significant area of intellectual property. India seems to have minimal experience with trade secrets, and courts would have to rely on compelling value precedents from various legal systems while resolving a case. Specific legislation is needed to protect trade secrets in India. Trade secrets are becoming the intellectual property of choice for many companies, small and medium-sized enterprises (SMEs), and research and development (R&D) laboratories. Therefore, effective legislative intervention is considered more expedient.[2]

Trade secrets are practical immediately, available for an unlimited period subject to their protection, cover a wide range of subject matter and do not involve strict enforcement procedures. In addition to these benefits, each trade secret has its specific advantages. A trade secret can protect the product, ensure the development of the product market, ensure the development of business activities and prevent improper acquisitions by competitors in the same field. If they are not protected at the beginning, their value may be lost, stolen and diminished, leading to a deterioration of business. In India, trade secrets remain neglected as there is no concrete legal framework for their protection.

[1] Kumar, Ranjeet and Others. Trade Secret Protection in Digital Environment: A Global Perspective. (Online) Available at https://www.omicsonline.com/open-access/trade-secrets-protection-in-digital-environment-aglobal-perspective-.php?aid=17287 (Accessed on 30th January 2025).
[2] Ibid

Such a scenario affects the development and progress of the Intellectual Property system in India. Protecting trade secrets must be ensured to encourage innovation and promote growth in this sector. As a result, this sector can emerge as a high-profit sector. As another form of IP rights, trade secrets can benefit corporate economic growth and development, even for their endurance. Hence, corporations must ensure that their confidential information, trade secrets, technical know-how and business processes are adequately protected from competitors. Protecting trade secrets is also vital for new technology or research-based start-ups that are victims of corporate theft, as they may not have the proper resources to patent their innovations. In this context, it is necessary to examine the role that India can play by putting in place an appropriate trade secret regime to stimulate the business sector.

Intellectual property encourages scientific and technical innovation while providing legal protection against rivals by maintaining secrecy and confidence. Legal exclusivity necessitates a high level of sophistication and esoteric knowledge in the commercial use of ideas and information. [3]In free market economies, the intangibility of property rights is increasingly becoming useful for the preservation of market shares.[4]

As intellectual property, trade secrets can convert intangible value into business and economic progress. Regrettably, due to their adverse treatment, trade secrets have been declared null and void in intellectual property rights law. The main reason is that intellectual property rules promote transparency in knowledge management, whereas confidentiality agreements protect trade secrets. In the legal protection framework, trade secrets enjoy confidentiality, making it possible to seek injunctive remedies for unlawful access and disclosure to recoup losses.

NAFTA (North American Free Trade Agreement) and TRIPS (Trade-Related Aspects of Intellectual Property) have developed a trade secret provision in GATT (General Agreement on Tariffs and Trade) (Uruguay Round of General Agreement on Tariffs

[3] Krishna, S.B. (2007) The Value of Intellectual Property. Manupatra Intellectual Property Reports. Pg. A 29-30

[4] Jorda, Karl F. Federalizing Trade Secret Law: A Cause Whose Time has come. (Online) Available at http://lawunhedu/assets/pdf/germeshausennewsletter-08-sf-editor.pdf (Accessed on 30 January 2025)

and Trade). Following that, there has been a development towards implementing national laws only meant to increase trade secret protection.

In the U.S., there is a codified legal framework; the Uniform Trade Secrets Act (UTSA) (1979) standardised state laws, and the Defend Trade Secrets Act (DTSA) (2016) introduced federal jurisdiction, strengthening protection against misappropriation.

In contrast, India has predominantly relied on common law principles and statutory provisions under the Indian Contract Act of 1872, which address confidentiality through contractual obligations. Landmark judicial decisions have shaped India's approach, often borrowing principles from English common law.

1.1 Research Problem/Question

The research addresses the critical gap in understanding how trade secret protection frameworks function within diverse legal systems, focusing on the United States and India. While both nations operate within distinct jurisprudential contexts, the U.S. has developed a structured approach through legislation like the Uniform Trade Secrets Act (UTSA) and the Defend Trade Secrets Act (DTSA). Conversely, India employs common law principles and Indian Contract Law and judicial precedents, creating a fertile ground for comparative analysis. The study emphasises the need to evaluate how these systems align with global standards, as highlighted by the OECD's Global Trade Secret Protection Index and the Kroll Global Fraud Report, which revealed significant instances of intellectual property theft across jurisdictions. This gap in comparative study underscores the importance of examining these frameworks through a multi-disciplinary lens, addressing evolving challenges posed by the interdependence of legal systems.

1.2 Research Question:

1. How do the U.S. and Indian legal frameworks define and protect trade secrets?
2. What are the specific challenges relating to trade secret protections in India, and how does this compare to the U.S.?
3. What cultural and social contexts should be considered while protecting trade secrets?

4. In corporate and economic growth context, does the Indian mechanism of protecting trade secrets fail to meet international parameters?

1.3 Rationale and Significance of the Study- The absence of specific legislation in India creates a gap in business legal protections, which inhibits innovation. Drawing from the U.S. model can provide India with a blueprint to strengthen its trade secret framework, promoting economic growth and competitiveness.

1.4 Scope and Delimitation- The study will focus on statutory and case law frameworks in the U.S. and India, analysing their effectiveness in mitigating trade secret misappropriation. It excludes non-legal dimensions like economic feasibility and enforcement practices in other jurisdictions.

1.5 Citation Style

The dissertation will follow the 21st Edition of the Bluebook Citation Style.

1.6 Theoretical Framework- The study draws on intellectual property theories, emphasising proprietary and incentive-based protections for trade secrets. Doctrines such as "inevitable disclosure" and "springboard doctrine" from U.S. jurisprudence are essential conceptual foundations.

1.7 Literature Review

- The Global Trade Secret Protection Index, developed by the OECD, ranks the US among the top countries for strong trade secret protections, reflecting the comprehensive legal framework.
- The 2017 Kroll Global Fraud Report found that 24% of companies in India reported intellectual Property theft, including trade secrets, compared to the global average of 21%.
- S.K. Verma, Protection of Trade Secrets and Confidential Information (2002), critiques India's reliance on common law for trade secret protection. The article highlights the challenges in protecting trade secrets, such as the risk of accidental disclosure and the difficulty in proving infringement. It also discusses the potential negative impact on competition and innovation if trade secrets are overly protected.

- David S. Levine & Christopher B. Seaman, *The DTSA at One* (2018), evaluating the impact of comprehensive trade secret laws in the U.S.
- William H. Manz, Defend Trade Secrets Act of 2016: A Legislative History of Public Law No. 114-153 (2017)

  This document compiles the legislative evolution and congressional intent behind the enactment of the DTSA. It details how the Act created a federal civil cause of action for trade secret misappropriation, enhancing consistency and enabling ex parte seizure in cases of imminent theft. The DTSA fills prior jurisdictional gaps in U.S. trade secret law and demonstrates a federal commitment to strengthening commercial confidentiality protections.

- Brandon Kinnard, Keep It Secret; Keep It Safe: A Practitioner's Guide to BRIC Trade Secret Regimes, 3 Am. U. Bus. L. Rev. 503 (2014)

  Kinnard offers a comparative analysis of trade secret laws across Brazil, Russia, India, and China (BRIC), identifying India as the weakest link due to its absence of statutory protection. The article argues that inconsistent enforcement and reliance on contract law impede India's innovation ecosystem. In contrast, the U.S. model is recognised as a gold standard for legislative structure and enforcement reliability.

- Faizanur Rahman, Trade Secrets Law and Innovation Policy in India, 3 Indian J.L. & Pub. Pol'y 119 (2016)

  Rahman critiques India's fragmented and non-codified trade secret framework, emphasising its incompatibility with TRIPS obligations and innovation goals. He analyzes the unimplemented National Innovation Act (2008) and urges statutory reform to protect confidential information, boost R&D, and align with international norms. The article provides a foundational critique for understanding India's legislative void in trade secret protection.

- V. Adharsh, The Disregarded Facet of IPR: A Study of Trade Secrets and the Indian Context, 3 Int'l J.L. Mgmt. & Human. 1969 (2020)

Adharsh explores the role of trade secrets in India's evolving IP landscape. Emphasizing their economic importance and competitive value, the article laments the lack of statutory clarity. It argues that legal uncertainty disincentivizes innovation and foreign investment. The author calls for a dedicated trade secret law, particularly in light of global trends and TRIPS compliance requirements.

- Sakshi Pawar & Smrithi Bhaskar, Obligations under Article 39.3 of TRIPs: The Data Exclusivity v. Data Protection Debate in the Indian Context, 3 J. Intell. Prot. Stud. 111 (2019)

  This article examines India's obligations under Article 39.3 of TRIPS, focusing on the pharmaceutical sector. It evaluates the contested terrain between public health concerns and data exclusivity demands. The authors propose a balanced approach that allows reasonable protection for innovator data without compromising access to essential medicines, offering policy recommendations to avoid adopting TRIPS-plus standards.

- Ayesha Tareen & Manisha Pilli, Comparative Analysis of Competition Law and Intellectual Property Rights: Interplay with Special Reference to India and the USA, 4 Indian J.L. & Legal Rsch. 1 (2022)

  Tareen and Pilli explore the interaction between IPRs (especially trade secrets) and competition law. Their comparative analysis shows that while U.S. law carefully balances monopolistic control with market fairness, India lacks such regulatory harmonization. The paper emphasizes the need for India to integrate trade secret governance with antitrust oversight to prevent abuse and foster competitive innovation.

- Trade Secret Protection and Firm Acquisitions: Evidence from the Uniform Trade Secrets Act

  This empirical study investigates whether enhanced trade secret protection under the UTSA influences firm acquisition behaviour. It finds that stronger legal protection increases acquisition likelihood, particularly by foreign investors who prefer minority stakes to mitigate information asymmetry risks.

The study underscores the economic value of robust trade secret law in corporate transactions and M&A strategy.

- Trade Secret Protection and R&D Investment of Family Firms

  This paper explores how UTSA-induced legal reform impacts R&D spending by family firms in the U.S. It concludes that enhanced trade secret protection positively correlates with increased R&D investment, especially in high-tech sectors. Family-controlled firms prefer trade secrets over patents to maintain control and confidentiality, illustrating how IP strategies are shaped by organizational structure and risk preferences.

- Ranjeet Kumar et al., Trade Secrets Protection in Digital Environment: A Global Perspective, Int'l J. Econ. & Mgmt. Sci. 2(4) (2012)

  This article assesses the efficacy of trade secret protection across jurisdictions in a digitally connected world. It highlights how digitization increases vulnerability to misappropriation and underscores the need for technological safeguards and comprehensive legal reform. The paper examines TRIPS obligations, compares the U.S. and Indian frameworks, and recommends adopting digital best practices to secure confidential business data.

1.8 Contribution to the Literature

This study bridges gaps by identifying actionable legislative reforms for India, grounded in a comparative analysis of U.S. and Indian legal systems.

1.9 Research Objectives

1. To analyse and compare trade secret laws in the U.S. and India.
2. To examine judicial interpretations under the UTSA and DTSA.
3. To identify gaps in Indian law and U.S. law.

1.10 Hypothesis

The existing legal framework for trade secret protection in India needs to be more comprehensive than established international practices, highlighting the potential for legislative reforms to enhance intellectual property safeguards through a comparative study of U.S. legislation.

1.11. Research Methodology

This research will utilise doctrinal research and comparative legal analysis. The doctrinal approach will provide an in-depth analysis of existing laws, case law, and regulatory frameworks related to the U.S. and Indian Legal Frameworks. Comparative legal analysis will examine how the two jurisdictions address trade protection aspects differently, focusing on trade secret legislations, regulations, and case law.

1.12 Sources of Data

Primary: Statutes like the UTSA, DTSA, and relevant Indian laws. Secondary: Journal articles, case commentaries, and legal databases.

1.13 Structure of the Dissertation

1. **Chapter 1: Introduction**
    - Background and Importance of Trade Secrets
    - Research Problem and Questions
    - Rationale, Scope, and Methodology
    - Theoretical Framework and Literature Review
2. **Chapter 2: Legal and Theoretical Framework of Trade Secrets**
    - International Legal Instruments (TRIPS, Paris Convention, WIPO)
    - Evolution of Trade Secret Law
    - Methods of Protection
    - India's Legal Framework for Trade Secrets.
3. **Chapter 3: Comparative Analysis of Trade Secret Protection in the U.S. and India**
    - Constitutional, Statutory, and Judicial Bases in the U.S.
    - India's Common Law and Contractual Approach
    - Legal Certainty and Enforcement Mechanisms
    - Economic and Cultural Considerations

4. **Chapter 4: Judicial Precedents for Trade Secret Protection**

    - Judicial Interpretation in the United States: From Restatement of Torts to DTSA Jurisprudence
    - Leading U.S. Cases: PepsiCo, E.I. du Pont, and Henry Schein Inc.
    - Indian Case Law: Zee Telefilms, John Richard Brady v. Chemical Process Equipment Pvt. Ltd., and Diljeet Titus v. Alfred A. Adebare
    - Common Law Doctrines and Equitable Relief in India
    - Comparative Judicial Trends and Doctrinal Influence

5. **Chapter 5: Conclusion and Recommendations**

    - Summary of Comparative Findings
    - Need for a Unified Trade Secret Law in India
    - Legislative and Policy Proposals
    - Broader Implications for Innovation and Investment

CHAPTER 2

Legal and Theoretical Framework of Trade Secrets

2.1 Introduction

In the modern knowledge economy, trade secrets have emerged as vital assets that underpin competitive advantage, technological innovation, and economic growth. The protection afforded to such confidential information is crucial for individual enterprises and forms a cornerstone of global intellectual property law. This chapter lays the theoretical and legal groundwork for understanding trade secret protections by exploring international conventions and historical evolutions that have shaped modern practice.

Over the past two centuries, various legal regimes- from early common law doctrines to codified statutory frameworks- have been employed to safeguard confidential business information. This evolution reflects broader economic and cultural forces, including the transformative impacts of industrialization and globalization. In examining the international legal framework, particular attention is given to foundational instruments such as the TRIPS Agreement,[5] the Paris Convention,[6] and the World Intellectual Property Organization (WIPO) policy initiatives.[7] The interplay between these global standards and domestic legal approaches provides a comprehensive backdrop against which modern trade secret law must be understood.

The chapter is organized into several sections. The first section introduces the international legal framework, highlighting the multilateral agreements that set the minimum standards for protection. The second section traces the historical evolution of trade secret law- from its early reliance on common law doctrines and informal contractual obligations to its present-day statutory incarnation in jurisdictions such as the United States and the European Union. The rest of the chapter will address the comparative implementation in different jurisdictions, focusing mainly on the U.S. and

[5] TRIPS Agreement art. 39.2, Marrakesh Agreement Establishing the World Trade Organization, Dec. 15, 1994, 1867 U.N.T.S. 299.
[6] Paris Convention for the Protection of Industrial Property, Dec. 20, 1883, 15 U.N.T.S. 97.
[7] WIPO, WIPO Intellectual Property Handbook: Policy, Law and Use (WIPO 2017).

India. They will discuss contemporary challenges such as digital misappropriation and cross-border enforcement issues.

The following analysis is underpinned by extensive doctrinal research and a comparative review of legislative developments, judicial decisions, and policy debates. It is intended to serve as an academic resource and a practical guide for legal practitioners and policymakers navigating the increasingly complex terrain of intellectual property protection in a globalised economy.

2.1.2 Origin of Trade Secrets

Intellectual property rights spur scientific and technical advancements while offering legal safeguards that protect businesses from competitive infringement by maintaining secrecy and confidence. The exclusive legal protection required in this area demands a high level of sophistication and specialized knowledge in commercializing ideas and information[8].

In free market economies, the non-material nature of property rights is increasingly instrumental in preserving market shares. As a unique form of intellectual property, trade secrets can convert intangible assets into tangible business and economic progress. Unfortunately, within intellectual property rights law, trade secrets have sometimes been treated unfavourably because the underlying rules aim to foster transparency in knowledge management. In contrast, trade secrets depend on confidentiality agreements for their protection. Under legal protection, the confidential status of trade secrets enables right-holders to seek injunctive relief against unauthorised access and disclosure to recover losses. Moreover, breaches of confidentiality may even lead to criminal prosecution. The widespread practice of safeguarding most of the world's operating technologies as trade secrets rather than through patents underscores the global esteem for this form of protection.[9] NAFTA (North American Free Trade Agreement) and TRIPS (Trade-Related Aspects of Intellectual Property) have incorporated trade secret provisions within GATT (General Agreement on Tariffs and Trade) following the Uruguay Round, setting the stage for a

[8] Krishna, S.B. (2007) The value of Intellectual Property, Manupatra Intellectual Property Reports. Pg. A 29,

[99] Jorda, Karl F. Federalizing Trade Secret Law: A Cause Whose Time has Come. (Online) Available at http://lawunhedu/assets/pdf/germeshausennewsletter-08-sf-editor.pdf (Accessed on 2 March 2025).

positive trend toward enacting national laws specifically aimed at strengthening trade secret protection.

2.1.3 No Discrete Trade Secret Law in India.

Historically, protecting trade secrets in India has not been a central subject of debate. Recent renewed interest in the topic is reflected in the US Special Reports 3017 published in 2014 and 2015, which pointed out the shortcomings of India's current regime on trade secrets, and in a presentation by the IPR Think Tank set by the Government of India,[10] emphasising the necessity for specific legislation to bridge this gap.

Special Report 301 identifies several issues. First, the current approach is ineffective in combating trade secret theft or unauthorised access, particularly in instances where no contractual relationships exist; second, it highlights the difficulties in obtaining damages; and third, it notes the lack of adequate procedural safeguards to prevent confidential information from being exposed during legal proceedings. The report further explains that the mandatory disclosure of trade secrets in court proceedings is a significant deterrent for property owners who might otherwise seek judicial protection.

Intellectual property in India traditionally includes copyrights, trademarks, patents, and trade secrets. Although India has comprehensive copyright protection under the Copyright Act of 1957[11], and has updated trademark protection through the Trade-marks Act 1999 (which replaced the Trademarks and Merchandise Acts, 1958) as well as patent protection under the Patent Act, 1970, there is still no standalone legislation explicitly addressing the protection of trade secrets. Unlike many TRIPS member states that have enacted dedicated trade secret laws, India currently relies on indirect provisions under the Contract Act, criminal law, and copyright law, which do not offer comprehensive protection.

Consequently, trade secret owners in India often find themselves inadequately shielded. These owners face significant challenges securing their secrets without a robust IP regime addressing their concerns. There is also a lack of sufficient legal redress in cases

[10] Department for Promotion of Industry and Internal Trade. (Online) Available at www.dipp.nic.in/English/Schemes/intellectual_property_rights.aspx, (Accessed on 22 February 2025),
[11] Magri, Karen A. International Aspects of Trade Secret Law. (Online) Available at http://www.myersbigel.com/library/articles/InternationalAspectsofTradeSecret.pdf (Accessed on 9 February 2025)

of fraud or misappropriation. Although remedies exist under the laws of torts and contracts, they are often insufficient to provide complete relief to trade secret owners. The prevailing intellectual property framework is premised on the idea that innovation should yield profits, yet no equivalent exceptions or special provisions are available for trade secrets. Thus, the current legal setup falls short of fully safeguarding the interests of trade secret holders.

2.1.4 Why is the protection of trade secrets preferred to the protection of patents?

Secrecy and confidentiality in trade secret protection do not prevent others from independently developing and commercialising similar methods or products. This protection mode does not grant exclusive rights to the owner that might otherwise weaken their position when employees or former workers possess the same confidential information. Trade secrets can be challenging to preserve over long periods, especially when many individuals are privy to them. Although confidentiality agreements between parties are an effective method of protecting trade secrets, enforcing such agreements can be problematic, particularly as they may restrict an employee's ability to earn a livelihood.[12] Despite these challenges, many manufacturers and producers opt for trade secret protection rather than patent protection because time limits, formal procedural requirements, or significant costs do not constrain trade secrets. Furthermore, unlike patents and copyrights that require public disclosure of details during the application process, trade secrets rely on deliberate confidentiality. However, despite their critical role, remedies and legal protections for trade secrets often remain ineffective and insufficient.

2.1.5 The Mandate of TRIPS

In line with Article 10bis of the 1967 Paris Convention, the TRIPS Agreement obliges Member States to protect undisclosed information (i.e., trade secrets). It is important to note that the terms "trade secrets" and "know-how" do not appear in Article 39. Instead, the protected category is "Undisclosed Information," detailed as one of the innovation classes in Article 1(2) of the TRIPS Agreement. According to Article 10bis of the Paris

[12] The Hindu (2001) Protection of Trade Secrets, Undisclosed Information, (Online) Available at http://www.thehindu.com/thehindu/biz/2001/11/22/stories/2001112200060100.html (Accessed on 8 November 2025).

Convention, the obligation under Article 39(1) is confined to protecting undisclosed information from unfair competition. Unfair competition is defined as any act by a competitor or market participant intending to exploit another party's industrial or commercial achievements for their benefit without a substantial departure from the original innovation.[13]

Article 39(2) does not define "undisclosed information"; it only sets out the criteria that information must meet to qualify: it must be secret, possess economic value due to its secrecy, and be subject to reasonable measures to maintain its confidentiality. The agreement does not treat undisclosed information as property per se; instead, it establishes that a person who lawfully controls such information should be able to prevent its unauthorised disclosure, acquisition, or use in a manner that is inconsistent with honest commercial practices.[14]

2.2 Global Standards and Agreement

2.2.1 The TRIPS Agreement and Its Impact

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) represents a pivotal moment in the global harmonisation of intellectual property law. Adopted in 1994 under the auspices of the World Trade Organisation (WTO), TRIPS establishes minimum standards for protecting various forms of intellectual property, including trade secrets.[15] TRIPS mandates that signatory states protect "undisclosed information" that confers commercial value by its secrecy, thereby obligating nations to enact legal measures designed to prevent the misappropriation of such information. This requirement has spurred comprehensive legislative reforms in many countries, ensuring that trade secret protections are "effective" and "non-discriminatory". The global consensus generated by TRIPS has facilitated cross-border business transactions and enhanced the legal certainty necessary for innovation and investment in high-technology industries.[16]

[13]Kumar, Abhinav, and others. Legal Provision of Trade Secrets: Towards a Codified Regime. The West Bengal University of Juridical Sciences, NUJS Bhavan, Kolkata.
[14] Guide to Uruguay Round Agreement. (1999) Kluwer Law International, The Hague. Page 216.
[15] TRIPS Agreement art. 39.2, Marrakesh Agreement Establishing the World Trade Organization, Dec. 15, 1994, 1867 U.N.T.S. 299.
[16] Id.

TRIPS has profoundly impacted domestic legal frameworks by establishing a baseline of protection. Advanced economies, particularly in North America and Europe, have built upon TRIPS mandates to refine and enhance their national trade secret regimes. Compliance with Trips has often necessitated a gradual, evolutionary legal reform process in developing economies, incorporating statutory measures and judicial interpretations that reflect local economic conditions and traditional legal doctrines.[17]

2.2.2 The Paris Convention for the Protection of Industrial Property

Adopted in 1883, the Paris Convention for the Protection of Industrial Property is one of the earliest international instruments to protect industrial property holders' rights[18]. Although its primary focus was on patents, trademarks, and industrial designs, the Convention laid critical groundwork for protecting confidential business information.

Historically, the Paris Convention introduced the notion of international cooperation in industrial property. Its provisions promoted that certain fundamental rights, such as safeguarding confidential information, should be universally recognised. The influence of the Paris Convention can be seen in the evolution of trade secret law. Early legal systems sought to adapt their principles to protect non-patented, proprietary information.

While the convention does not address trade secrets with the specificity of later treaties, its early emphasis on protecting industrial assets provided a conceptual framework for later legal developments. Indeed, the doctrinal foundations laid by the Paris Convention continue to inform contemporary debates on the balance between public disclosure and the protection of competitive advantage.[19]

2.2.3 The Role of WIPO in Shaping Global Norms

The World Intellectual Property (WIPO) plays a vital role in setting and harmonising international standards for intellectual property protection, including trade secrets. Although WIPO does not have the same enforcement powers as the WTO, its policy

[17] Kevin E. Maskus & Jerome H. Reichman, *International Public Goods and Transfer of Technology under a Global Intellectual Property Regime* (Oxford Univ. Press 2004).
[18] Paris Convention for the Protection of Industrial Property, Dec. 20, 1883, 15 U.N.T.S. 97.
[19]Robert Abbott, The Paris Convention and Its Legacy in Modern Intellectual Property Law (University Press 2001).

initiatives, research publications, and technical assistance programs have significantly influenced the development of national trade secret regimes.[20]

WIPO's influence extends to various activities, from international conferences and workshops to publishing guidelines that help countries align their domestic laws with global best practices. In doing so, WIPO has contributed to the gradual convergence of disparate legal systems, enabling a more coherent approach to protecting confidential business information across borders.

The organisation's work is significant in emerging digital technologies, where the rapid dissemination of information challenges traditional notions of secrecy and confidentiality. WIPO's ongoing efforts to update and refine its guidelines ensure that legal frameworks remain responsive to technological advancements and continue to safeguard innovation in the digital age.[21]

2.3 Evolution of Trade Secret Protection

2.3.1 Early Common Law Principles and Customary Practices

Before the advent of codified statutes, trade secret protection was governed primarily by common law principles and informal contractual agreements. In early industrial economies, safeguarding proprietary knowledge, from manufacturing processes to secret recipes, depended mainly on personal trust and the doctrine of breach of confidence.[22]

In this formative period, the concept of a trade secret was closely linked to the fiduciary relationships between employers and employees or business partners. However, reliance on oral agreements and customary practices left businesses vulnerable to misappropriation, as legal remedies were limited and often inconsistent across jurisdictions.

The gradual recognition of the economic value of confidential information spurred judicial innovation. Courts began to assert that the unauthorised disclosure of sensitive business information could breach an implied duty of confidentiality, thereby giving rise to legal claims for damages. This early judicial decision laid the groundwork for

[20] WIPO, WIPO Intellectual Property Handbook: Policy, Law and Use (WIPO 2017).
[21] WIPO, "Trade Secrets and Industrial Property: Recent Developments," WIPO Magazine (2019).
[22] Coco v. A.N. Clark (Engineers & Constructors) Ltd., [1969] RPC 41 (Eng. Ct. of Appeal).

modern trade secret laws by establishing that confidentiality is essential to commercial trust and innovation.[23]

2.3.2 The Impact of Industrialisation on Confidentiality

The advent of industrialisation in the 18th and 19th centuries radically transformed the nature of business and the protection of intellectual assets. As industries expanded and production processes became increasingly complex, the need to protect technological innovations grew correspondingly.[24]

Industrialisation catalysed a shift from informal, trust-based confidentiality mechanisms to more structured legal protections. The competitive pressures of a rapidly evolving market necessitated a robust legal framework that could safeguard the investments made in research and development. During this period, many nations began to codify elements of trade secrets protection within broader commercial and unfair competition statutes.

This transformation reflected economic necessity and a response to the changing cultural attitudes towards information. With the rise of mass production and mechanised processes, the dissemination of knowledge became both a competitive threat and an economic imperative. The resulting legal reforms paved the way for a modern understanding of trade secrets as critical assets that merit dedicated statutory protection.[25]

2.3.3 Globalisation and the Shift from Contractual Reliance to Statutory Protections

The latter half of the 20th century witnessed a dramatic acceleration in globalisation, reshaping the legal landscape of trade secret protection. With the increased flow of goods, services, and information across national borders, the limitation of relying solely on contractual mechanisms (such as nondisclosure agreements) became apparent.[26]

Globalisation underscored the necessity for standardised, statutory approaches to trade secrets protection that would be recognised and enforceable across different

[23] F. H. Nipkow, "Early Doctrines in Trade Secret Law," 12 J. Legal Hist. 245 (1989).
[24] J. S. Millar, "The Rise of Industrial Confidentiality," 54 Bus. Hist. Rev. 112 (1980).
[25] Ibid.
[26] Uniform Trade Secrets Act (U.S. Model Law 1985); Defend Trade Secrets Act, Pub. L. No. 114 113, 130 Stat. 2198 (2016).

jurisdictions. In response, many advanced economies began implementing dedicated trade secret statutes that provided uniform definitions, remedies, and enforcement procedures. In the United States, for example, the Uniform Trade Secrets Act (UTSA) and, later, the Defend Trade Secrets Act (DTSA) of 2016 have played pivotal roles in shaping a consistent legal framework that addresses both civil and criminal misappropriation.[27]

Similarly, the European Union has moved toward a harmonised approach with initiatives such as the EU Trade Secrets Directive, which aims to balance the interests of businesses in protecting confidential information with broader public policy objectives. These statutory frameworks significantly depart from earlier reliance on informal or contractual protections, reflecting a broader trend toward codification and legal certainty in the global economy.[28]

2.3.4 The Emergence of Modern Statutory Frameworks in the U.S. and EU

Modern statutory frameworks for trade secret protection epitomise the evolution from reliance on common law and contractual remedies to a more robust, codified approach. In the United States, combining the UTSA and DTSA provides a layered structure of protection, offering clear legal definitions and a range of remedies, from injunctions to substantial monetary damages, for the misappropriation of trade secrets. This dual-level approach has been critical in ensuring legal certainty in a technologically advanced, global marketplace.[29]

Across the Atlantic, the EU Trade Secrets Directive represents a similar effort to harmonise national laws and create a coherent framework that protects confidential business information while ensuring fair competition. The Directive underscores the importance of balancing private commercial interests with the public interest in promoting innovation and economic growth.

These modern statutory frameworks are not static; they continue to evolve in response to emerging challenges such as digital misappropriation, cyber espionage, and the complexities of international enforcement. As global markets become ever more

[27] Ibid.
[28] EU Trade Secrets Directive 2016/943/EU, art. 1 (2016).
[29] 18 U.S.C. § 1836 (2016).

interconnected, the need for legal systems that can adapt to new technological realities while safeguarding traditional business interests is more pressing than ever.[30]

2.4. Methods of Protecting Trade Secrets

Although the TRIPS Agreement includes provisions for protecting trade secrets under the broader term "Undisclosed Information," it does not specify the methods for achieving this protection, leaving each Member State the discretion to determine the appropriate measures. Many nations, including the United States, have developed legitimate instruments to safeguard trade secrets. The mechanisms employed can vary widely: in some cases, they fall under privacy laws; in others, they are addressed under laws governing unfair competition or contractual breaches of trust or confidence.

It's essential to recognise that the legal protection of trade secrets is not about the secrecy itself but about enforcing the consequences when that secrecy is breached. Recent court cases illustrate this point. For instance, Bristol Technology filed a lawsuit against Microsoft, alleging anti-competitive practices by restricting open access to Microsoft's Windows source code, a trade secret the court ultimately resolved in Microsoft's favour. Additionally, a Singaporean firm secured an injunction against three former employees who had started a competing business, as the court found that the non-disclosure agreements they had signed were valid and enforceable. However, if a competitor legally obtains information and independently deciphers the underlying secret, no breach occurs since the information was discovered without any improper means.[31]

2.4.1 National Implementation of TRIPS Obligations

The TRIPS Agreement has profoundly influenced national legal regimes by compelling signatory states to establish minimum standards for protecting undisclosed information. This section examines how different jurisdictions have implemented TRIPS obligations, particularly emphasising the approaches taken by the US and India.

2.5. Protection of Trade Secrets and Development of Trade Secrets Law in the United States and India

[30]EU Trade Secrets Directive 2016/943/EU, rec. 9 (2016).
[31] The Hindu. (2001) Protection of Trade secrets, Undisclosed Information.(Online) http://www.thehindu.com/thehindu/biz/2001/11/22/stories/2001112200060100.html.

2.5.1 Protection of Trade Secret Law in the US

In contrast to other forms of intellectual property with centuries-old origins, modern trade secret law primarily emerged from judicial decisions during the mid-nineteenth century. One jurist noted that trade secret law evolved from a series of analogous common law offences, including breach of trust, breach of confidential relationship, misappropriation under common law, undue enrichment, unfair competition, and even misdemeanours such as trespass or unauthorised access to a plaintiff's property. It also draws upon legal principles inherent in contract law and the common law of employment relationships.

The American Law Institute (ALI), a respected body of lawyers, judges, and scholars, published the "Restatement of Torts" in 1939 to clarify common law principles and incorporate legislative components. This Restatement addressed trade secrets by defining them in Section 757 and outlining the elements of a misappropriation claim in Section 758. Later, in its 1993 "Restatement (Third) of Unfair Competition," the ALI elaborated on trade secret issues in Articles 39 to 45. In 1979, the National Conference of Uniform Law Commission (NCCUSL) released the Uniform Trade Secrets Act (UTSA), which systematically codified trade secret protection rules by integrating common law principles and addressing judicial gaps. Although the NCCUSL does not have regulatory authority, its recommendations become binding when state governments adopt them. Before the mid-1990s, following the enactment of the 1996 Economic Espionage Act by Congress, the federal government took minimal steps to ensure nationwide trade secret security.[32] UTSA remains the key statute in the United States for prohibiting third parties' improper commercial use of trade secrets. In addition, the 1996 Economic Espionage Act (EEA) grants broad authority to the Attorney General to sue individuals for trade secret theft. The act makes transferring trade secrets without authorisation illegal and imposes penalties on both the giver and the receiver.

The UTSA was widely adopted by states, with the notable exception of New York, which continues to rely on common law for trade secret protection. Although specific trade secret statutes were primarily enacted to standardise judicial decisions, the

[32] Brain, T. Yeh. Protection of Trade Secrets: Overview of Current Law and Legislation. (Online) Available at https://fas.org/sgp/crs/secrecy/R43714.pdf (Accessed on 2 December 2024)

preamble to the United States UTSA (as amended in 1985 by the National Conference of Commissioners on Uniform State Laws and approved by the American Bar Association) highlights concerns over the vulnerability of a seventeen-year patent once invalidated by the courts. As the Preliminary Note states:

"In return for the public disclosure of an invention, a legitimate patent grants a legal monopoly for seventeen years. If the courts eventually found that the patent office granted a patent in error, an invention would have been revealed to rivals for a slight advantage. Because of the many patents declared void by the courts, many companies now want to shield commercially valuable knowledge by relying on state trade secrets laws."[33]

Likely, neither the Patent Clause of the United States Constitution nor federal patent laws pre-empt state trade secret rights from patentable or non-patentable material, further reinforcing reliance on trade secret protection.

Since current or former employees are the most common sources of trade secret misappropriation, companies customarily require new hires to sign non-disclosure agreements. As a result, breaches of these agreements provide a legal basis for action. Some multinationals even temporarily bar former employees from joining competitors. Moreover, practical measures such as marking all confidential documents, restricting access to critical trade secrets, enhancing computer security, and enforcing non-disclosure agreements are standard methods to maintain secrecy. Information cannot be legally secret without these safeguards, even if a regulation exists.

In the United States, the protection of trade secrets is supported by a robust, dual-level legal framework that integrates state and federal legislation. The Uniform Trade Secrets Act (UTSA), adopted by most states, provides a standardised definition of trade secrets and outlines remedies for misappropriation. Under the UTSA, trade secrets are defined as information that derives independent economic value from not being generally known and is subject to reasonable efforts to maintain secrecy. This statutory framework offers clear criteria and practical guidance for businesses and courts when determining misappropriation claims.[34]

[33] Kewanee Oil Co. v. Bicron Corporation.
[34]Uniform Trade Secrets Act, 1985 (U.S. Model Law); Defend Trade Secrets Act, Pub. L. No. 114-113 (2016).

In 2016, the Defend Trade Secrets Act (DTSA) was enacted at the federal level. The DTSA allows companies to bring civil actions in federal courts for trade secret misappropriation, ensuring a uniform mechanism for redress across state lines. The DTSA enhances legal certainty by extending federal jurisdiction, particularly in interstate commerce and cyber misappropriation cases. The combination of UTSA and DTSA has effectively created a layered structure that accommodates various business relationships and technological challenges, from traditional industrial processes to complex digital networks.[35]

The United States legal system has benefited from a rich body of case law that further refines statutory provisions. Landmark cases have elucidated key principles such as the scope of "reasonable measures" necessary to maintain secrecy and the appropriate balance between protecting business interests and promoting competitive markets. For example, courts have consistently held that an employer's failure to implement adequate security measures may weaken its claim to trade secret protection, emphasising the importance of proactive risk management.[36]

Judicial decisions have also clarified the nature of remedies available to aggrieved parties. In instances of wilful and malicious misappropriation, U.S. courts have been willing to award compensatory and punitive damages and injunctions to prevent further harm. These decisions serve as a deterrent against unauthorised disclosures and underscore the commitment to U.S. law to protect the economic incentives underlying innovation and research investments.[37]

Economically, the U.S. model is designed to foster an environment conducive to innovation. The assurance of legal protection for trade secrets incentivises substantial investment in research and development, as firms can safeguard proprietary technologies without disclosing them publicly, a requirement inherent in patent law. The dual-layered system not only preserves competitive advantages but also supports the overall dynamism of the U.S. economy, particularly in high-tech industries and emerging sectors such as artificial intelligence and biotechnology.[38]

---

[35] Ibid.

[36] See, e.g., In re Certain Geophysical Service Data, 887 F. Supp. 2d 687 (S.D.N.Y. 2012).

[37] See, e.g., Waymo LLC v. Uber Technologies, Inc., 2020 WL 2032763 (N.D. Cal. 2020).

[38] See Maskus, K. E., & Reichman, J. H., International Public Goods and Transfer of Technology under a Global Intellectual Property Regime (Oxford Univ. Press 2004).

The U.S. approach is also characterised by its adaptability. Ongoing legislative amendments and evolving judicial interpretations ensure that the legal framework remains responsive to new technological challenges, including cyber-security threats and the global circulation of digital data. The dynamic interplay between statutory and case law has resulted in a comprehensive regime that balances protection with public interest, reinforcing the United States' position as a leader in intellectual property rights enforcement.[39]

2.5.2 India: An Evolving Legal Paradigm

2.5.2.1 Reliance on Contract Law, Common Law, and Equity

In contrast to the U.S. approach, India has not yet adopted a dedicated trade secret statute. Instead, India relies on a combination of contractual obligations, common law doctrines, and equity principles to protect confidential business information. Historically, Indian courts have interpreted breaches of confidentiality as torts or contract violations, applying principles rooted in the doctrine of "breach of confidence."[40]

This reliance on ad hoc measures has resulted in a fragmented legal landscape. Businesses typically depend on non-disclosure agreements (NDAs) and confidentiality clauses embedded in commercial contracts to safeguard sensitive information. While these instruments provide a certain degree of protection, they often lack the broad scope and uniformity that statutory provisions afford. Consequently, the absence of a dedicated trade secret statute in India has led to varying judicial interpretations and a degree of legal uncertainty that can complicate cross-border transactions and technology transfer.[41]

2.5.2.2 Judicial Developments and Emerging Trends

Recent judicial decisions in India have begun to address the gaps in trade secret protection. Indian courts have increasingly recognised that natural justice and equity remedies should be available when confidential information is disclosed without proper authorisation. Although these judicial interventions represent a positive trend, the

[39] Ibid.
[40] See Coco v. A.N. Clark (Engineers & Constructors) Ltd., [1969] RPC 41 (Eng. Ct. of Appeal).
[41] See, e.g., K. S. Ramanujam, "Confidentiality and Contractual Remedies in Indian Commercial Law," Indian Law Review 34, no. 1 (2018): 58–80.

framework remains largely piecemeal, relying significantly on legacy doctrines rather than modern codified statutory provisions.[42]

Policymakers in India are now actively debating legislative reforms to establish a comprehensive trade secret statute. These reforms are intended to harmonise India's legal framework with international standards, particularly those mandated by the TRIPS Agreement. The proposed legislative initiatives are expected to incorporate best practices from jurisdictions like the United States and the European Union while accommodating India's unique economic and cultural context.[43]

2.5.2.3 Economic and Cultural Considerations

India's approach to trade secret protection is influenced by a distinct set of economic and cultural factors. The country's traditional reliance on common law and contractual arrangements reflects a broader legal culture that values flexibility and judicial discretion. However, this flexibility comes at the cost of legal certainty, especially in rapid technological change and global competition.

Economic imperatives have also driven the debate over trade secret protections in India. As India becomes an increasingly important hub for technology and innovation, the need to protect proprietary information has never been greater. Foreign investors and multinational corporations have highlighted the risks associated with a fragmented legal regime, arguing that robust trade secret protections are essential for fostering innovations and attracting investment. The gradual shift toward a more codified framework is therefore seen as both an economic necessity and a means of aligning with international best practices.[44]

2.6. Comparative Analysis: The United States vs. India

A nuanced comparison of trade secret regimes in the United States and India reveals both convergences and divergences that are critical to understanding the global landscape of intellectual property protection.

2.6.1 Legal Certainty and Uniformity

[42]See, e.g., Recent Judgments in The Times of India (2021).
[43] Government of India, Ministry of Commerce & Industry, Draft Trade Secrets Bill, 2022.
[44] Ibid.

The U.S. legal framework stands out for its clarity and uniformity. The dual statutory system, embodied in the UTSA and DTSA, provides clear definitions, standardised remedies, and consistent judicial interpretations. This codification ensures businesses can confidently operate, knowing that well-defined legal parameters protect their proprietary information. The predictability of judicial outcomes in U.S. courts further reinforces the attractiveness of the U.S. as a destination for innovation-driven investments.[45] Trade secret law in the United States faces several challenges that impact the protection and enforcement of confidential business information. Variations in state laws, despite the widespread adoption of the Uniform Trade Secrets Act (UTSA), lead to inconsistencies in defining and enforcing trade secrets. The increasing globalisation of business operations complicates enforcement, as companies must navigate differing international legal frameworks.[46] Additionally, technological advancements have heightened risks of cyber threats and unauthorised disclosures, necessitating robust cybersecurity measures.[47] The recent Federal Trade Commission (FTC) ban on non-compete agreements further challenges companies to find alternative methods to protect their proprietary information.[48] Addressing these issues requires a comprehensive approach, including harmonising laws, enhancing international cooperation, and implementing advanced security practices.

In contrast, India's reliance on common law principles and contractual arrangements creates a less predictable environment. The absence of a dedicated trade secret statute means that legal protections vary from case to case, and the specific contractual context often determines the remedies available to aggrieved parties. This lack of uniformity can pose challenges for companies operating across state and national borders, where inconsistent judicial interpretations may undermine the enforceability of confidential information agreements.[49]

[45] UTSA Commentaries, Uniform Law Commission (2020).
[46]Editorial, Understanding the Challenges in Enforcing Trade Secret Laws, Laws Learned (June 29, 2024), https://lawslearned.com/challenges-in-enforcing-trade-secret-laws/.
[47]Red Points, The Top 5 Issues in Trade Secret Litigation and How to Address Them, Red Points Blog (Mar. 23, 2023), https://www.redpoints.com/blog/trade-secret-litigation/
[48]Matthew D. Kohel & Dana Silva, What Does FTC Ban on Noncompete Agreements Mean for Companies' Ability to Protect Trade Secrets?, Reuters (June 5, 2024), https://www.reuters.com/legal/legalindustry/what-does-ftc-ban-noncompete-agreements-mean-companies-ability-protect-trade-2024-06-05/
[49] See K. S. Ramanujam, op. Cit.

Indian trade secret protection, though currently reliant on contract law, common law, and equitable principles rather than a dedicated statute, offers distinct business advantages. This framework provides a flexible, cost-effective means for safeguarding proprietary information,[50] as Indian courts have shown a willingness to grant injunctive relief in cases involving breaches of confidence. Such judicial flexibility allows for prompt remedies tailored to the specifics of each case while accommodating the unique commercial practices prevalent in the Indian market. Moreover, recent initiatives under the National Innovation Act and the National IPR Policy signal a growing governmental commitment to enhance these protections,[51] aligning India's legal framework more closely with international standards and supporting greater integration into the global economy.

2.6.2 Enforcement Mechanisms and Remedies

U.S. law offers a broad spectrum of remedies for trade secret misappropriation, including injunctions, compensatory damages, and punitive damages in cases of wilful misconduct. The availability of federal jurisdiction under the DTSA ensures that disputes can be resolved efficiently and uniformly. These robust enforcement mechanisms deter potential misappropriation and provide a reliable means for businesses to recoup losses incurred due to unauthorised disclosures.[52]

While Indian courts have been willing to grant injunctions and award damages in breach of confidentiality, the overall enforceability of trade secret protections remains less specific. The fragmented nature of India's legal framework means that enforcement mechanisms are often tailored to the specifics of contractual disputes rather than stemming from a comprehensive statutory regime. This can result in variable outcomes and may limit the effectiveness of remedies in protecting confidential business information on a national scale.[53]

2.6.3 Economic and Policy Implications

[50] "Trade Secrets in India: Understanding the Legal Landscape," AZB Partners, available at https://www.azbpartners.com/bank/trade-secrets-india/ (last visited March 3, 2025).
[51] "Protecting Trade Secrets in India: Challenges and Opportunities," Lexology, available at https://www.lexology.com/library/detail.aspx?g=c83e8a6c-a02e-44ba-8723-94087d2e5e20 (last visited March 3rd, 2025).
[52] DTSA, 18 U.S.C. § 1836 (2016).
[53] Indian Contract Act, 1872, various judicial pronouncements.

The strength and clarity of the U.S. legal framework for trade secrets have significant positive implications for innovation. By reducing the legal risks associated with misappropriation, U.S. law encourages firms to invest heavily in research and development. The assurance of robust legal protection fuels domestic innovation and attracts foreign investment, particularly in technology-intensive sectors. This dynamic has contributed to the United States' reputation as a global leader in technological innovation and intellectual property rights enforcement.[54]

Conversely, India faces the challenges of balancing traditional legal approaches with the need for modern, codified protections. The gradual evolution of India's trade secret framework reflects the country's broader development trajectory. While India has made significant strides in recognising and remedying breaches of confidentiality, the ongoing reliance on legacy doctrines continues to pose challenges for consistent enforcement. Legislative reforms that create a unified statutory regime are anticipated to enhance legal certainty, boost investor confidence, and stimulate further innovation.[55]

2.6.4 Cross-Border Implications

In today's interconnected global economy, the differences between the U.S. and Indian approaches have broader implications. Companies operating in multiple jurisdictions must navigate a complex legal landscape where the standards for protecting trade secrets can vary significantly. The divergence between a codified regime, as seen in the United States, and a more fragmented system, as observed in India, can affect cross-border litigation and international business transactions. Harmonising these differences remains an ongoing challenge for international legal bodies and is critical for facilitating smooth global commerce.[56]

2.7. Theoretical Underpinnings and National Contexts

The divergence in national approaches to trade secret protection is not merely a product of legislative choices but reflects deeper theoretical and policy considerations.

---

[54] Trade Secrets Bill, Ministry of Commerce & Industry, India, 2024.
[55] P. K. Jain, "Cross-Border Challenges in Trade Secret Enforcement," Journal of International Business Law 12, no. 2 (2019): 95–117.
[56] P. K. Jain, "Cross-Border Challenges in Trade Secret Enforcement," Journal of International Business Law 12, no. 2 (2019): 95–117.

2.7.1 Economic Theories Underlying Trade Secret Protection

Economic theory suggests that trade secret laws serve as an essential complement to patent law. By protecting information companies choose to keep secret, these laws provide an alternative incentive for innovation without the mandatory disclosure required by patents. In the United States, the economic rationale is straightforward: firms are encouraged to invest in research and development because they can safeguard their innovations without revealing proprietary details to competitors. This system has proven effective in promoting a vibrant high-tech sector and supporting industries where rapid technological advancement is critical.[57]

2.7.2 Cultural and Institutional Factors

In India, the historical reliance on common law and contractual arrangements reflects cultural and institutional factors shaping the country's legal landscape. The flexibility of a case-by-case approach has long been valued in Indian jurisprudence, allowing judges to adapt legal principles to the facts of individual disputes. However, this flexibility also introduces uncertainty. As India increasingly integrates with the global economy, there is growing recognition that a more structured and codified approach may be necessary to meet international standards and protect the interests of both domestic and foreign investors.[58]

2.7.3 Policy Debates and Future Directions

The contrasting approaches in the United States and India have sparked ongoing policy debates. In the United States, discussions often focus on protecting trade secrets and ensuring that such protections do not stifle competition or innovation. In India, policymakers face the dual challenge of modernising the legal framework while preserving the flexibility that has traditionally characterised Indian jurisprudence. Legislative proposals in India are increasingly looking to international best practices, drawing inspiration from the U.S. and E.U. models, while seeking to tailor reforms to the country's specific economic and cultural realities.[59]

2.8. Emerging Trends and Contemporary Challenges

[57] S. Maskus, Intellectual Property Rights in the Global Economy (Cambridge University Press 2000).
[58]S. Sen, "Traditional vs. Modern Legal Approaches in India," Indian Business Law Journal 27, no. 3 (2020): 142–168.
[59] Government of India, Draft Trade Secrets Bill, 2024.

Trade secret protection faces many new challenges as global markets evolve and digital technologies reshape the business landscape. This section examines how recent technological and economic trends impact the protection and enforcement of trade secrets and outlines the key areas that require policy attention.

2.8.1 The Digital Transformation and Cyber Threats

The rapid advancement of digital technologies has fundamentally transformed the way confidential information is created, stored, and transmitted. In the digital age, trade secrets are no longer confined to physical documents or isolated data systems; they increasingly reside on interconnected networks and cloud-based platforms. This digitalisation presents unique vulnerabilities:

- **Data Breaches and Cyber Espionage:** Sophisticated cyber-attacks can potentially expose sensitive business information at scale. Incidents of hacking and data breaches have become common in sectors such as technology, finance, and healthcare, thereby heightening the risk of trade secret misappropriation.[60]
- **Complex Supply Chain:** The interconnections of global supply chains mean that confidential information may traverse multiple jurisdictions and platforms. This increases the challenge of safeguarding data once it has been digitised and shared among various stakeholders.[61]
- **Emergence of Data Analytics:** As companies harness big data for competitive advantage, proprietary algorithm[62]s and analytical models become critical trade secrets. Ensuring that these digital assets are protected requires updated legal frameworks that account for the rapid pace of technological change.[63]

2.8.2 Cyber-security Measures and Legal Responses

Companies and governments are investing heavily in cyber-security measures to address the vulnerabilities introduced by digitalisation. These include encryption technologies, access control systems, and comprehensive cyber-security policies to reduce the risk of unauthorised access. However, the legal landscape must also evolve:

[60] Ponemon Institute, "Cybersecurity Breaches and the Trade Secret Risk," Ponemon Report (2021).
[61] P. K. Jain, "Global Supply Chain Vulnerabilities in Trade Secret Protection," Journal of International Business Law 12, no. 2 (2019): 95–117.
[62] L. Merges, "Big Data and Trade Secret Challenges," in Intellectual Property and Data Protection (Wiley 2020).
[63] In re Cybersecurity Breach Litigation, 952 F. Supp. 2d 100 (S.D.N.Y. 2021).

- **Integration of Cyber-security and IP law:** Increasingly, legal frameworks are beginning to recognise that robust cyber-security measures are integral to maintaining trade secret status. Courts and legislatures are considering whether failure to implement adequate digital security can weaken a party's claim to trade secret protection.[64]
- **Legislative Reforms:** Some jurisdictions are contemplating amendments to existing trade secret statutes to incorporate explicit cyber-security standards. These reforms would clarify the obligations of companies to protect digital trade secrets and establish a higher baseline for "reasonable measures."[65]

2.8.3 Cross-Border Enforcement Challenges

2.8.3.1 Jurisdictional Complexities in a Global Economy

Globalising business operations means that trade secret misappropriation often occurs across national borders. This presents significant challenges:

- **Divergent Legal Standards:** As detailed in Parts 1 and 2, legal frameworks for trade secrets vary markedly between jurisdictions such as the United States, Europe, and India. These differences can lead to inconsistent judicial outcomes when disputes involve parties from multiple countries.[66]
- **Enforcement in the Digital Realm:** Digital trade secrets may be stored and accessed in multiple jurisdictions simultaneously, complicating efforts to enforce legal remedies. International cooperation and harmonisation of laws are essential for effective cross-border enforcement.[67]
- **Extradition and Mutual Legal Assistance:** In cyber espionage cases, legal authorities may need to rely on international treaties and mutual legal assistance to prosecute offenders. However, the absence of uniform legal standards can hinder swift and effective enforcement actions.[68]

2.8.3.2 Efforts toward Harmonisation

[64] In re Cybersecurity Breach Litigation, 952 F. Supp. 2d 100 (S.D.N.Y. 2021).
[65] Draft Legislative Proposal, U.S. Cybersecurity Enhancement Act, 2022
[66] TRIPS Agreement, Art. 39.2, World Trade Organization, 1994.
[67] WIPO, WIPO Intellectual Property Handbook: Policy, Law and Use (WIPO 2017).
[68]United Nations Commission on International Trade Law, "Challenges in Cross-Border Enforcement of Trade Secrets," UNCITRAL Report (2020).

Recognising these challenges, international organisations and trade bodies are working toward greater harmonisation of trade secret laws:

- **Role of WIPO and the WTO:** Organisations such as the World Intellectual Property Organisation (WIPO) and the World Trade Organisation (WTO) continue facilitating dialogue between nations. These efforts aim to better standardise definitions, remedies, and enforcement mechanisms to address digital commerce and global trade realities.[69]
- **Bilateral and Multilateral Agreements:** Several countries have entered into bilateral and multilateral agreements that provide frameworks for cooperation in intellectual property enforcement, including trade secret protection. Such agreements can help bridge the gap between disparate legal systems and enhance cross-border judicial collaboration.[70]

2.8.4 Balancing Private Interests and Public Policy

2.8.4.1 The Tension between Secrecy and Transparency

Trade secret protection must balance private interests against broader public policy considerations:

- **Innovation versus Information Disclosure:** While strong trade secret laws encourage innovation by protecting confidential investments, overly stringent protections may inhibit the flow of information that could benefit society. For instance, critical public health or environmental safety data may be withheld under trade secret protection, raising ethical and regulatory concerns.[71]
- **Regulatory Oversight:** Policymakers must consider mechanisms to ensure that trade secret protections do not unduly hinder regulatory oversight or the dissemination of information that serves the public interest. Judicial review, mandatory disclosure provisions in specific contexts, and other checks and balances may be required to strike this delicate balance.[72]

2.8.4.2 The Role of Public Interest Litigations and Transparency Initiatives

---

[69] WIPO, "International Trends in Trade Secret Protection," WIPO Magazine (2021).
[70] European Commission, "Bilateral IP Enforcement Agreements: Trends and Implications," EC Report (2020).
[71] Public Health Watch, "Trade Secrets versus Public Health: The Disclosure Dilemma," Health Policy Journal 45, no. 3 (2021): 210–230.
[72] In re Public Disclosure Litigation, 973 F. Supp. 2d 450 (D. Mass. 2020).

Recent trends indicate a growing awareness of the need to balance private commercial interests with the public's right to information:

- **Judicial Interventions:** Courts in several jurisdictions have begun to scrutinise the application of trade secret protections in cases where public welfare is at stake. This includes instances involving product safety, environmental hazards, or public health crises, where withholding information might significantly affect society.[73]
- **Transparency Initiatives:** Some governments are exploring policy initiatives that require transparency for certain types of confidential information, mainly when public interest is involved. These initiatives may involve conditional disclosure frameworks that allow regulators and, in some cases, the public to access critical information without compromising the competitive interests of businesses.[74]

2.8.5 Future Policy Directions

2.8.5.1 Legislative Reform and Policy Innovation

To keep pace with technological and economic transformations, legislative reform is inevitable:

- **Updating Statutory Definitions:** Future legislative initiatives may need to update statutory definitions of trade secrets to account for digital assets and cyber risks. This could include explicitly referencing cyber-security standards and integrating data protection measures within trade secret statutes. [75]
- **Enhanced Enforcement Mechanisms:** Strengthening cross-border enforcement through international treaties and cooperation mechanisms will be crucial. Policymakers will likely advocate for enhanced mutual legal assistance protocols, streamlined extradition procedures, and harmonised judicial practices to deal effectively with digital trade secret misappropriation.[76]
- **Balancing Innovation and Competition:** Legislators must also ensure that trade secret laws promote innovation without stifling competition. This may

[73] Case Commentary, The Times of India (2021).
[74] DTSA, 18 U.S.C. § 1836 (2016).
[75] Trade Secrets Bill, Ministry of Commerce & Industry, India, 2024.
[76] OECD, "Enhancing Cross-Border Enforcement of Intellectual Property Rights," OECD Report (2021).

involve regulatory safeguards that prevent the misuse of trade secret protections to create anti-competitive environments while rewarding genuine innovative efforts.[77]

2.8.5.2 The Impact of Emerging Technologies

Emerging technologies such as artificial intelligence, block-chain, and the Internet of Things (IoT) pose new questions for trade secret law:

- **Artificial Intelligence and Algorithmic Trade Secrets:** As firms increasingly rely on AI-driven algorithms, determining the boundaries of what constitutes a trade secret becomes more complex. The interplay between AI's opaque decision-making processes and the need for legal transparency requires innovative policy solutions that protect proprietary algorithms while ensuring accountability.[78]
- **Blockchain for Secure Information Sharing: Blockchain** technology offers potential solutions for enhancing the security and traceability of digital trade secrets. By providing immutable records of data transactions, blockchain can serve as a tool for verifying compliance with confidentiality obligations, thereby bolstering enforcement efforts. Policymakers and industry stakeholders are beginning to explore how blockchain can be integrated into trade secret protection regimes.[79]
- **Internet of Things (IoT) and Data Proliferation:** The IoT's extensive network of interconnected devices generates vast amounts of data that may have commercial value. Protecting this data while ensuring interoperability and innovation presents technical and legal challenges. Future policies must address how IoT-generated data can be classified, secured, and regulated under trade secret laws.[80]

2.9. Conclusion

This chapter has provided a comprehensive analysis of the legal and theoretical frameworks that underpin trade secret protection. It has traced the historical evolution

[77] L. Merges, "Balancing Innovation and Competition in Trade Secret Law," in IP Law Review 34, no. 2 (2019): 310–345.
[78] S. Sen, "Artificial Intelligence and the Future of Trade Secret Protection," Indian Business Law Journal 29, no.1 (2022): 75–102.
[79]Blockchain in IP Protection, World Economic Forum Report (2022).
[80] IoT and Data Security, IEEE Internet of Things Journal 9, no. 4 (2022): 1–18.

of trade secret laws–from early common law doctrines and customary practices to the modern statutory frameworks exemplified by the United States and the European Union–and has examined India's evolving approach within a global context.

The chapter established the international legal framework by discussing foundational instruments such as the TRIPS Agreement, the Paris Convention, and the influential role of WIPO. Then, it explored national implementations, presenting a detailed comparative analysis of the U.S. and Indian approaches to trade secret protection and highlighting differences in legal certainty, enforcement mechanisms, and economic implications.

The emerging trends and contemporary challenges in the digital age are also presented here. It has underscored the impact of digitalisation and cybersecurity threats on trade secrets, examined the complexities of cross-border enforcement in a globalised economy, and discussed the delicate balance between private commercial interests and public policy. Finally, it has outlined future policy directions that will be essential in updating legal frameworks to meet the challenges of emerging technologies and evolving business practices.

The evolution of trade secret law reflects the dynamic interplay between legal doctrine, economic imperatives, and technological advancements. As businesses and governments navigate this complex terrain, ongoing legislative reform and international cooperation will be critical in ensuring that trade secret protections remain strong, flexible, and aligned with the broader objectives of innovation and public welfare.

Chapter 3

Comparative Analysis of Trade Secret Protection in the U.S. and India

I. Trade Secrets Protection in the U.S.

3.1 Introduction

Trade secrets are recognised as the fourth category of intellectual property, alongside patents, trademarks, and copyrights. They comprise knowledge-based assets such as formulas, rationales, compilations, programs, devices, methods, techniques, or processes that derive their economic value precisely from their secrecy. For an asset to qualify as a trade secret, it must be utilised in commerce and confer a competitive advantage over those unaware of or do not employ the secret information.[81]

Unlike patents, trademarks, or copyrights, each with centuries of historical development, trade secret law is relatively modern. Its origins can be traced to mid-nineteenth-century state court decisions, which addressed breaches of trust, unauthorised disclosures, misappropriation, unfair competition, unjust enrichment, and even trespassing or unauthorised access. These early judicial decisions, influenced by common law torts, laid the groundwork for the modern legal doctrines protecting trade secrets. Moreover, contract and employment law principles have further reinforced the protection of confidential information.[82]

As trade secrets were initially safeguarded under national law, their owners could seek legal redress in state courts by pursuing standard law liability claims or invoking specific national statutes. In 1939, the American Law Institute's publication of the "Restatement of Torts" precisely articulates these customary legal principles, particularly in §§ 757 and 758, which specifically address the misuse of trade secrets.[83]

[81] United States Patent and Trademark Office, Trade Secrets Policy, available at https://www.uspto.gov/patents-getting-started/international-protection/trade-secret-policy (last visited March 14, 2025).
[82] Gaido, Chiara, Trade Secret Protection in the US and Europe: A Comparative Study, available at https://www.researchgate.net/publication/321761790_The_trade_secrets_protection_in_US_and_in_Europe_a_comparative_study (last visited March 14, 2025).
[83] Ibid

3.2 Legal Basis for Trade Secret Law in the United States

The foundation of trade secret protection in the United States is rooted in constitutional provisions, federal and state legislation, and judicial precedents.

3.2.1 Constitutional Authority.

Under Article I, Section 8, Clauses 3 and 8 of the U.S. Constitution, Congress is empowered to regulate commerce and to secure exclusive rights for authors and inventors over their writings and discoveries. This constitutional provision underpins the broader legal framework that supports intellectual property rights, including trade secrets.[84]

3.2.2 Common Law Origins.

U.S. trade secret law evolved from common law offences, initially focusing on breaches of trust and violations of confidential relationships during the nineteenth century. Over time, these doctrines expanded to address misappropriation, unfair competition, unjust enrichment, and unauthorised access to proprietary information.[85]

3.2.3 Statutory Framework.

Several key statutes have shaped modern U.S. trade secret protection:

- **Uniform Trade Secrets Act (UTSA):** Enacted in 1979 and amended in 1985 by the Uniform Law Commission, the UTSA was designed as a model law to standardise trade secret protection across states. It defines a trade secret as information that derives independent economic value from its secrecy and is subject to reasonable efforts to maintain that secrecy.[86]
- **Economic Espionage Act (EEA) of 1996:** This federal statute criminalises the theft of trade secrets, mainly when such theft benefits foreign governments or organisations. It imposes severe penalties, including substantial fines and long-term imprisonment, reinforcing the deterrent against trade secret misappropriation.[87]

[84] United States Constitution, Art. I, § 8, cl. 3 & cl. 8.
[85] See, generally, U.S. trade secret law's evolution from common law doctrines addressing breach of trust and unauthorised disclosure.
[86] Draft Uniform Trade Secrets Act with 1985 Amendments, available at https://www.wipo.int/edocs/lexdocs/laws/en/us/us034en.pdf (last visited March 9, 2019).
[87] 18 U.S.C. §§ 1831-1839 (Economic Espionage Act of 1996).

- **Defend Trade Secrets Act (DTSA) of 2016:** Expanding on the UTSA, the DTSA provides trade secret owners with a federal cause of action. It offers additional remedies, such as ex parte seizure orders to prevent further dissemination of misappropriated information, and serves to harmonise state and federal protection. For instance, under 18 U.S.C. § 1836(b)(2)(D)(iii), if a defendant refuses consent for disclosure, the court is obligated to take all necessary measures to preserve confidentiality.[88]

3.2.4 International Obligations.

The United States is also committed to protecting trade secrets as part of its obligations under international agreements. As a member of the World Trade Organisation (WTO) and a signatory to the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), the U.S. must maintain legal mechanisms that protect commercially confidential information subject to adequate safeguards.[89]

3.3 Uniform Trade Secrets Act

3.3.1 Essential Definitions of the Uniform Trade Secrets Act

The Uniform Trade Secrets Act (UTSA) offers comprehensive protection for trade secrets, beginning with its precise definition of essential terms in Section 1. Under the UTSA, a "Trade Secret" is defined as information, including a formula, pattern, compilation, program, device, method, technique, or process, which meets two fundamental criteria:

1. It creates independent economic value, whether actual or potential, precisely because it is not generally known and cannot be readily ascertained by appropriate means by those who might benefit economically from its disclosure or use.
2. Under the circumstances, it is subject to reasonable measures to maintain its secrecy.

For instance, examples of protected knowledge under the UTSA include formulas, drawings, compilations, programs, gadgets, methods, techniques, and procedures. In

[88] 18 U.S.C. § 1836(b)(2)(D)(iii).
[89] See TRIPS Agreement, Article 39(2).

some states, such as Pennsylvania, customer lists are categorised as compilations and are therefore regarded as trade secrets.[90]

UTSA's modern definition diverges significantly from the earlier Restatement of Torts (First) definition, which required that a trade secret be "continuously employed in one's business." UTSA's expanded definition now accommodates situations where an applicant has not yet had the opportunity or acquired the means to exploit a trade secret. This broader interpretation also encompasses information that may be of commercial value from a "negative" perspective, for example, extensive and expensive reverse-engineering efforts that demonstrate a particular process will not work can still confer significant competitive value if discovered by a rival.[91]

Moreover, the phrase "not being generally known and not being readily ascertainable by proper means by other persons" does not imply that a trade secret is lost merely because some individuals within the organisation know it. Instead, the secret is forfeited only when the key person(s) capable of profiting from it no longer maintains its confidentiality. For example, a metal casting technique might be unknown to the general public while being common knowledge within a specialised foundry sector. Conversely, if the information is readily available in academic journals, reference books, or other public sources, its protection as a trade secret is effectively lost. Additionally, if the cost and time required for reverse engineering are prohibitive, the knowledge obtained through such processes may become a valuable trade secret.[92]

In practice, maintaining the confidentiality of a trade secret requires implementing reasonable measures under the circumstances. These measures might include informing employees about the existence and confidential nature of the secret, limiting access strictly on a "need-to-know" basis, and regulating entry to sensitive areas such as manufacturing facilities. In contrast, public disclosure, whether intentional through advertisements or unintentional through negligent publication in trade journals, can render the protection ineffective. The court does not mandate using excessively costly

[90] United States Patent and Trademark Office, Trade Secrets Policy, available at https://www.uspto.gov/patents-getting-started/international-protection/trade-secret-policy (Accessed on 14 March 2025).
[91] Gaido, Chiara, Trade Secret Protection in US and in Europe: A Comparative Study, available at https://www.researchgate.net/publication/321761790_The_trade_secrets_protection_in_US_and_in_Europe_a_comparative_study (Accessed on 7 March 2025).
[92] Ibid.

procedures to protect trade secrets against egregious industrial espionage; the steps taken must be deemed "reasonable" given the particular circumstances.[93]

Historically, the unauthorised use or disclosure of trade secrets was treated as a common law tort before the advent of the UTSA. The core tenets of trade secret law are enshrined in the Restatement of Torts (1939, §§ 757 and 758), which American courts have widely adopted. In particular, Section 757, Commentary b of the Restatement, outlines six critical variables for determining whether information qualifies as a trade secret:

i.The extent to which the information is known outside the claimant's business.
ii. The degree to which employees and others associated with the business are aware of the information.
iii. The extent of the claimant's efforts to preserve its confidentiality.
iv. The economic value of the information to both the business and its competitors.
v.. The company invests time and money in generating the information.
vi. The ease or difficulty with which others could legitimately acquire or reproduce the information.[94]

There was extensive debate regarding whether trade secrets should be recognised as a form of property after the UTSA was drafted and adopted by several states before its amendment in 1985. In the landmark decision of *Ruckelshaus v. Monsanto Co.* (1983), the U.S. Supreme Court concluded that trade secrets are indeed considered property and, as such, are entitled to protection under the Fifth Amendment. The Court reasoned that the widely held view of trade secrets as a form of property extending beyond tangible assets to encompass an individual's "work and invention" is consistent with other forms of intellectual property protection, such as copyrights, trademarks, and patents. Consequently, the ability to exclude others from using the trade secret is integral to its classification as property. Once a trade secret is disclosed to third parties or its use is otherwise authorised, the owner loses this property interest. This fundamental principle explains why a claim under the UTSA can only be brought if the information is secret and misappropriated.[95]

[93] Comments on Section 1, Uniform Trade Secrets Act, available at https://www.wipo.int/edocs/lexdocs/laws/en/us/us034en.pdf (Accessed on 13 March 2025).
[94] Trade Secret, Legal Information Institute, available at https://www.law.cornell.edu/wex/trade_secret (Accessed on 15 March 2025).
[95] Ruckelshaus v. Monsanto Co., 416 U.S. 470 (1974).

3.3.2 Misappropriation under the Uniform Trade Secrets Act

Under the Uniform Trade Secrets Act (UTSA), the term "misappropriation" is defined in a manner that covers both the acquisition and the unauthorised disclosure or use of trade secrets. Specifically, misappropriation occurs when:

1. **Acquisition:** A person acquires another's trade secret knowing, or having reason to know, that the information was obtained by improper means.
2. **Disclosure/Use:** A person discloses or uses another's trade secret without the explicit or implicit consent of the trade secret owner.

In further detail, misappropriation may occur if an individual:

a) Employs unethical methods to gain knowledge of a trade secret, such as theft, bribery, or other improper inducements; or

b) Knows, or has reasonable grounds to know, that, at the time of disclosure or use, the trade secret was acquired:

(i)From someone who obtained it through unethical means;

(ii) in circumstances that necessitated strict confidentiality or limited its use; or

(iii) from an individual who was contractually or fiduciarily obligated to maintain its secrecy.

Additionally, misappropriation may also be established where an individual knew or had reason to know that the information was a trade secret and was acquired inadvertently or by mistake before a significant change in their position, thereby still compromising the secret's value.

It is crucial to note that a misappropriation claim under the UTSA must be initiated within three years from the date it was discovered or should have been discovered through due diligence. In cases where misappropriation is continuous over time, the law treats it as a single claim for the statutory limitations**.** Claims for misappropriation must be filed within three years from when the misappropriation is discovered or reasonably

should have been discovered, with continuous misappropriation treated as a single claim.[96]

3.3.3 Remedies under the Uniform Trade Secrets Act

Under the UTSA, two primary remedies are available for misappropriating trade secrets: injunctive relief and damages.

3.3.4 Injunctive Relief

Concerning injunctive relief, the UTSA stipulates that a court may issue an injunction to prevent actual or threatened misappropriation of a trade secret. The injunction typically remains in force until the trade secret ceases to exist, although courts may extend its duration to prevent any undue financial gain from the misappropriation. In exceptional circumstances, where a blanket prohibition would be excessively burdensome, the court may condition future use of the trade secret on paying a reasonable fee or royalty, not exceeding the period during which such use could have been legally restricted. Exceptional circumstances might include a significant adverse change of position before the information was acquired or a justification for the misappropriation that renders a complete injunction unfair. Additionally, the court may issue orders requiring affirmative actions to protect the trade secret, such as mandating specific security measures or disclosure restrictions. For example, suppose Party A possesses a valuable trade secret initially unknown to others in the industry. In that case, Party B subsequently misappropriates it; an injunction may be issued to prohibit Party B from using or disclosing the secret. Unlike common law, which often sets an arbitrarily determined term for such injunctions (based on the time needed to reverse-engineer the secret), the UTSA permits more predictable and fair relief by dissolving the injunction once the trade secret is either reverse-engineered, publicly disclosed, or legitimately published.[97]

3.3.5 Damages

[96] Section 1(2), Uniform Trade Secrets Act; Ladas and Parry, United States Trade Secrets Law (2014), available at https://ladas.com/educationcenter/united-states-trade-secrets-law-2/ (Accessed on 11 March 2025).

[97] Section 2, Uniform Trade Secrets Act.

Damages under the UTSA serve as a remedy that may be awarded in addition to or instead of injunctive relief. The statute provides that a complainant may recover losses from misappropriating a trade secret. This recovery may also include damages for unjust enrichment, accounting for the unlawful economic benefit gained. Instead of, or in addition to, monetary compensation calculated based on actual losses, courts may determine damages by assessing a reasonable fee or royalty for the unauthorised disclosure or use of the trade secret. In cases where misappropriation is both willful and malicious, the UTSA permits awarding exemplary damages up to twice the amount awarded under the standard calculation.[98]

3.3.6 Court Obligations

The UTSA imposes specific obligations on courts to maintain the confidentiality of trade secrets during litigation. Courts must issue protective orders during discovery, conduct closed hearings, and seal court records where necessary to prevent inadvertent disclosure of sensitive information. Moreover, all parties involved in the litigation may be ordered not to disclose any trade secret without the court's explicit consent. In situations where adequate assurances of confidentiality cannot be provided, the court will handle the trade secret issue with heightened discretion. Additionally, courts often limit disclosure to a party's attorney and support staff. They may appoint a special master bound by a court-approved non-disclosure agreement to manage and review secret materials.[99]

The UTSA establishes a multifaceted approach to protecting trade secrets. It allows for both injunctive relief and damages in response to misappropriation. Suppose a party unlawfully acquires, discloses, or uses a trade secret. In that case, the owner can obtain an injunction to halt further misappropriation and seek monetary damages for actual losses and unjust enrichment. Moreover, the court may impose exemplary damages and attorney’s fees in cases of wilful misconduct. Notably, the UTSA mandates that courts take extensive measures to protect the confidentiality of trade secrets throughout the litigation process, including sealing records and limiting disclosures to essential parties.

3.4 Defend Trade Secrets Act

[98] Section 3, Uniform Trade Secrets Act.
[99] Section 5, Uniform Trade Secrets Act.

3.4.1 Introduction

The Defend Trade Secrets Act (DTSA) is a pivotal U.S. federal statute that empowers trade secret owners to initiate civil actions in federal court when their confidential information is misappropriated. Signed into law in 2016 by former President Obama, the DTSA was designed to complement and expand upon existing state-level protections established under the Uniform Trade Secrets Act (UTSA), which was adopted in some form by 48 50 states.[100] Moreover, the DTSA broadens the scope of the 1996 Economic Espionage Act by federalising civil remedies for trade secret misappropriation, thereby addressing inconsistencies arising from divergent state laws and procedural issues such as forum selection, location, and choice of law.[101] The federalisation of trade secret law has significantly altered the legal landscape, offering a uniform framework that enhances the security and enforceability of trade secret rights.

The first judicial decision applying the DTSA was rendered on June 10, 2016, in *Henry Schein, Inc. v. Cook*. Judge Jon S. Tigar granted a temporary restraining order to prevent a former employee from soliciting the plaintiff's clients. Subsequently, on February 25, 2017, the case *Dalmatia Import Group, Inc. v. Food Match Inc.* resulted in a federal jury awarding $2.5 million in damages for trade secret misappropriation, trademark infringement, and counterfeiting, with $500,000 attributed explicitly to a claim under the DTSA.[102]

3.4.2 Important Definitions

3.4.2.1 Trade Secret.

Under the DTSA, "trade secret" is defined broadly as all forms and types of financial, business, scientific, technical, economic, or engineering information, tangible or intangible, whether stored physically, electronically, graphically, photographically, or in writing. This encompasses patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs,

[100] Madubuko, Yana, "The Protection of Trade Secrets: A Comparative Analysis of the United States and European Union," Bachelor's Thesis, Tallinn University of Technology (2018), available at http://digi.lib.ttu.ee/i/file.php?DLID=10108&t=1 (last visited March 14, 2025).
[101] Ibid
[102] Dikinson Wright, "The Defend Trade Secrets Act. It's Coming: All You Need to Know," (2016), available at https://www.dickinson-wright.com/news-alerts/the-defend-trade-secrets-act-what-you-need-to-know (last visited March 17, 2019).

or codes.[103] For a piece of information to qualify as a trade secret, two conditions must be met:

- (A) The owner must have taken reasonable precautions to keep the information confidential; and
- (B) The information must have an independent economic value, actual or potential, by not being generally known and not being readily ascertainable by proper means to others who could obtain economic benefit from its disclosure or use.[104]

3.4.2.2 Trade Secret Owner.

The term "owner" in the context of trade secrets refers to the individual or entity that holds the legal or equitable rights, or a license, to the trade secret. This ownership confers the right to exclude others from unauthorised use or disclosure.[105]

3.4.2.3Misappropriation

Misappropriation is defined as either:

(A) The acquisition of another's trade secret by a person who knows or has reason to know that the trade secret was obtained by improper means (such as theft, bribery, or other unethical techniques); or

(B) The disclosure or use of another's trade secret without the express or implicit consent of the owner, where the individual knew or had reason to know that the information was acquired improperly. This may include cases where the trade secret is obtained from a person who, under the circumstances necessitating confidentiality or limited use, is obligated to maintain its secrecy or where the trade secret was acquired accidentally before a significant change in the Individual's position.[106]
A misappropriation claim must be filed within three years from the discovery, or when one reasonably should have discovered the misappropriation, with continuous misappropriation treated as a single claim.[107]

[103] 18 U.S.C. § 1839(3).
[104] 18 U.S.C. § 1839(4).
[105] 18 U.S.C. § 1839(5).
[106] Ibid.
[107]Ibid.

3.4.2.4 Improper Means.

"Improper means" under the DTSA refers to theft, bribery, misrepresentation, or inducement to breach a duty of secrecy, including electronic or other forms of espionage. Notably, methods such as reverse engineering or independent derivation, which are legally permissible, are explicitly excluded from this definition.[108]

3.4.3 Remedies Under the Defend Trade Secrets Act

The DTSA provides several remedies for trade secret misappropriation, including injunctive relief and monetary damages.

3.4.3.1 Private Civil Action.

The DTSA empowers trade secret owners to bring a private civil action in federal court when their secrets have been misappropriated, allowing them to seek both injunctive relief and damages. Such civil actions deter potential wrongdoers and provide comprehensive relief to the aggrieved party.[109]

3.4.3.2 Civil Seizure.

In exceptional circumstances, a court may issue a civil seizure order on an ex parte basis to prevent the propagation or dissemination of a misappropriated trade secret. This order, granted only when no other remedy is available and when an affidavit or verified complaint meets the statutory requirements, authorises the seizure of property containing the misappropriated trade secret before a final decision on the case. For example, in *Magnesita Refractories Co. v. Mishra*, the court declined to authorise a civil seizure because an injunction had already been issued that included the seizure of the defendant's laptop. Civil seizure is particularly significant when there is a risk of permanent harm or if the defendant might otherwise dispose of or conceal evidence. Additionally, the DTSA establishes a three-year limitation period for filing a civil action from when the misappropriation is or should have been discovered.[110]

3.4.3.3 Additional Remedies.

In wilful and malicious misappropriation cases, the court may award exemplary damages, up to twice the amount of the compensatory damages awarded, and may

---

[108] Ibid.
[109] 18 U.S.C. § 1836(b)(1); see also 18 U.S.C. §§ 1836(b)(2)(A)–(B).
[110] 18 U.S.C. §§ 1836(b)(2)(A)–(B), 1836(b)(2)(F); Madubuko, Yana, op. cit.

also order the payment of the prevailing party's attorney's fees, mainly where litigation has been pursued in bad faith.[111]

3.4.3.4 Court Obligations

The DTSA imposes strict obligations on courts to protect the confidentiality of trade secrets during litigation. Courts must issue protective orders during discovery, hold closed hearings, seal records where necessary, and restrict disclosure of sensitive information to only essential parties, such as attorneys and their assistants. Sometimes, the court may appoint a disinterested special master bound by a court-approved non-disclosure agreement to review secret material and report findings. These measures are critical to ensuring the trade secret remains confidential throughout the judicial process.[112]

3.4.3.5 Requirements for Seizure

Before a court may issue a seizure order under the Defend Trade Secrets Act, several conditions must be satisfied:[113]

1. It must be shown that a remedy such as an order under Rule 65 of the Federal Rules of Civil Procedure or an alternative equitable remedy would be ineffective because the party subject to the order would evade or fail to comply with it.
2. A demonstration must be that an immediate and irreversible injury would occur without such a seizure.
3. The harm suffered by the plaintiff due to a denial of the seizure application must significantly exceed any potential damage that could be incurred by the person against whom the seizure is ordered, as well as any collateral harm to third parties.
4. The applicant must have a substantial likelihood of proving the following:
    - (aa) That the information in question qualifies as a trade secret and

[111] Supra note 29.
[112] Supra note 30.
[113] 18 U.S.C. § 1836(b)(2)(A)

- (bb) The individual subject to the seizure has either improperly obtained the trade secret or conspired to do so using unethical means.[114]

5. The person against whom the seizure is sought must possess the items, including the trade secret and any property containing it.
6. The application for seizure must accurately describe the items to be seized and, when appropriate, specify the location where the items will be taken.
7. The court must be assured that if the plaintiff has notified the subject of the seizure, that person (or any conspirators) might otherwise destroy, hide, or otherwise render the case unworkable.
8. Lastly, the petitioner must not have made the seizure request public.

3.4.3.6 Elements of Seizure

A seizure order must meet the following criteria:[115]

- It must contain the necessary factual findings and legal conclusions supporting the order.
- The seizure should be as limited as possible to minimise disruption to third parties' business operations and should not unduly interfere with the accused's legitimate, unrelated business activities.
- The order must restrict the applicant's access to the seized property and explicitly prohibit making copies.
- If the court grants access to the seized documents, such access must align with the documentation already in the court's possession.
- The order should provide clear instructions to the law enforcement officials tasked with executing it.
- Unless the parties mutually agree otherwise, a hearing must be scheduled within seven days.

[114] 18 U.S.C. § 1839(4); Ladas and Parry, United States Trade Secrets Law, available at https://ladas.com/educationcenter/united-states-trade-secrets-law-2/ (last visited 11 March 2025).
[115] 18 U.S.C. § 1839(3)

- The applicant must furnish appropriate security for potential damages resulting from any wrongful or unreasonable seizure as determined by the court.

3.4.3.7 Seizure Hearing

- **Date of Hearing:**
  A hearing for the seizure order is scheduled on the day designated by the court under the applicable procedural rules.

- **Burden of Proof:**
  The party seeking the seizure must demonstrate, at the hearing, all relevant facts and legal grounds supporting the issuance of the seizure order. The seizure order may be modified or dissolved if they fail to meet this burden.

3.4.3.8 Dissolution or Modification of Order

Following notification, any person adversely affected by the seizure order may appeal to have the order dissolved or modified at any time.

3.4.3.9 Action for Damages caused by Unlawful Seizure

A party suffering harm due to an unlawful or excessive seizure may initiate an action against the party who obtained the seizure order, seeking remedies analogous to those provided under Section 34 (d) (11) of the Trademark Act 1946.[116]

3.4.3.10 Protection from Publicity

The court must take appropriate measures to protect the individual or entity against whom a seizure order is issued from any publicity that might arise from the order or the seizure process, whether initiated by the party requesting the order or otherwise.

3.4.3.11 Protection of Confidentiality

In line with the Uniform Trade Secrets Act, the Defend Trade Secrets Act mandates that, unless the person subject to the order consents to the disclosure, the court must take all necessary steps to preserve the confidentiality of seized documents that are not directly relevant to the trade secret information at issue.[117]

[116] 18 U.S.C. § 1836(b)(2)(D)(iii)
[117] 18 U.S.C. § 1836(b)(2)(D)(iv)

3.4.3.12 Appointment of a Special Master

The court may designate a special master to identify and segregate misappropriated secret information and facilitate the return of property and data unrelated to the misappropriation. The appointed special master is required to sign a court-approved non-disclosure agreement.

3.5 Remedies under the Defend Trade Secrets Act

The DTSA provides two primary types of remedies in trade secret misappropriation cases: injunctive relief and damages.

(A) Injunctive Relief

A court may grant an injunction to:

- Prohibit any actual or threatened misappropriation on terms deemed reasonable by the court, ensuring that the order does not conflict with other existing orders.
- Prevent an individual from entering an employment arrangement based solely on evidence of potential misappropriation rather than on the available information.
- Mandate proactive measures to preserve confidentiality if deemed appropriate.
- In cases where an injunction is deemed inequitable, the fair royalty payment for future use of the trade secret must not exceed the period for which the trade secret could have been legally restricted.

(B) Damages

A court may award damages as follows:

- **(i)** Damages for the loss incurred due to misappropriating the trade secret.
- **(ii)** Damages for unjust enrichment reflect the economic benefit that the misappropriator derived from the trade secret, which is not otherwise captured in the actual loss calculation.
- Alternatively, damages may be measured based on a reasonable fee or royalty imposed on the unauthorised disclosure or use of the trade secret.

- **(iii)** In cases where misappropriation is found to be wilful and malicious, the court may award exemplary damages equal to twice the compensatory damages.
- **(iv)**The prevailing party may also be awarded attorney's fees if misappropriation is proven to have been pursued in bad faith.

3.6 Jurisdiction

United States District Courts have jurisdiction over civil actions brought under the DTSA, ensuring that trade secret disputes are adjudicated under a uniform federal framework.[118]

3.7 Period of Limitations

A civil action under the DTSA must be filed within three years from the date the misappropriation was discovered or should have been found with reasonable diligence. Continuous misappropriation is treated as a single claim for this limitation period.[119]

3.8 Whistle-blower Protection

The DTSA provides explicit protection for whistle-blowers. Individuals who report the misappropriation of trade secrets to federal, regional, or municipal authorities or their legal counsel are shielded from civil and criminal liability. This protection also extends to individuals who, when suing for retaliation against employees who report a breach, are permitted to disclose the trade secret to their counsel and use the information during litigation.

3.9 Responses to DTSA required by a Corporate Entity

Corporate entities must undertake several proactive measures in response to the DTSA:

- Ensure that employment and confidentiality agreements include provisions on DTSA's whistle-blower immunity, as failure to do so may preclude recovery of double damages or legal costs.
- Re-evaluate the company’s approach to handling trade secret allegations, given that state court processes can be slow and uncertain compared to federal courts.

[118]18 U.S.C. § 1836(c)
[119] 18 U.S.C. § 1836(d)

- Maintain a comprehensive inventory of the company's trade secrets and periodically assess the protection measures.
- Develop contingency plans in anticipation of potential trade secret theft and receipt of seizure orders to minimise commercial disruption and enable rapid legal action.
- In industries with high employee mobility, formalise crisis preparedness and response plans to address the immediate implications of a seizure order, including the swift dissolution of an unlawful seizure.[120]

3.10 Comparison of the Uniform Trade Secrets Act and Defend Trade Secrets Act

While the DTSA shares many similarities with the UTSA, particularly in its definition of misappropriation and the range of available remedies, it introduces several key distinctions:

- The DTSA provides plaintiffs access to federal courts and allows for ex parte attachment orders, which can pre-emptively secure trade secrets before the defendant is served with a notice of prosecution.
- The DTSA extends the statute of limitations to five years, in contrast to the UTSA's three-year period.
- The DTSA permits treble exemplary damages, whereas the UTSA only allows for double damages.
- Finally, the DTSA does not preclude additional causes of action based on the same core facts, offering broader avenues for legal recourse.[121]

Comparison of the Uniform Trade Secrets Act and the Economic Espionage Act

[120] Keplan, Sebastian, and Premo, Patrik, "The Defend Trade Secrets Act of 2016 Creates Federal Jurisdiction for Trade Secret Litigation," available at https://www.ipwatchdog.com/2016/05/23/defend-trade-secrets-act-2016-creates-federal-jurisdiction-trade-secret-litigation/id=69245/ (last visited 20 March 2025).
[121] Seyfarth Shaw, Latest Updates on Federal Trade Secret Legislation, available at https://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/ (last visited 18 March 2025).

A critical analysis of the existing trade secret legislation reveals that their tone and objectives are the most significant distinction between the DTSA/UTSA framework and the Economic Espionage Act (EEA). Whereas the DTSA and the UTSA primarily provide civil remedies for trade secret misappropriation, the EEA is designed with a predominantly penal focus. The EEA criminalises the misappropriation and broader system of misappropriation and appropriation of undisclosed information, thereby aiming to enhance foreign entities' power in economic espionage cases. Under the EEA, individuals guilty of misappropriation can face fines of up to $500,000 per offence. Organisations may incur penalties of up to $10,000,000, with offenders also subject to imprisonment for up to 15 years. This punitive approach was notably illustrated in *The United States v. Steven L. Davis*, where the defendant received a 27-month prison sentence and was fined approximately $1.3 million.[122]

3.11 The Economic Espionage Act of 1996

3.11.1 Introduction

The Economic Espionage Act of 1996 is a landmark statute enacted to amend Title 18 of the U.S. Code to protect proprietary economic information and address related concerns. Adopted by the 104th United States Congress, the Act became effective on October 11, 1996, introducing Chapter 90, titled “Protection of Trade Secrets”, which encompasses Sections 1831 to 1839. The EEA pursues two primary objectives:

(I) To prevent the theft of trade secrets by agents or instruments of foreign governments or individuals acting on their behalf, and

(II) To provide general protection against the theft of trade secrets by any party.[123]

3.11.2 The Need for the Economic Espionage Act, 1996

The enactment of the EEA was driven by the necessity to fill a significant gap in trade secret protection. This gap had widened with the advent of new information technologies. Before the EEA, most cases involving the theft of trade secrets under federal jurisdiction were prosecuted under the Interstate Transportation of Stolen

[122] Seyfarth Shaw, Latest Updates on Federal Trade Secret Legislation, available at https://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/ (last visited March 20,2025) .
[123] Ibid.

Property Act, a statute not designed initially to cover intellectual property. As a result of the absence of a dedicated federal statute, various state laws, primarily derived from revisions to the UTSA, were employed to address the issue. However, these disparate regulations were insufficient to counteract the growing incidence of trade secret misappropriation.[124]

3.11.3 Definition of Trade Secrets under the Economic Espionage Act, 1996

Under the EEA, "trade secret" is defined broadly to encompass all forms and types of financial, business, scientific, technical, economic, or engineering information. This definition covers tangible or intangible information stored, compiled, or recorded in any physical, electronic, graphical, photographic, or written medium. To qualify as a trade secret under the EEA, two criteria must be satisfied:

- The owner must have taken reasonable precautions to keep the information secret and
- Because the information is not widely known and readily ascertainable properly, it possesses independent economic value, whether actual or potential.[125]

The EEA's definition is broader than the UTSA's because it incorporates new technological methods for creating and storing trade secrets. Like the UTSA, the EEA requires that the owner of the information take unspecified "reasonable steps" to maintain its secrecy so that the information retains its independent economic value.[126]

3.11.4 Offences under the Economic Espionage Act, 1996

The EEA codifies two distinct offences for the protection of trade secrets:

- **Economic Espionage:**
  For economic espionage, the EEA states that any person who, with the intent or knowledge that their actions will benefit a foreign government, instrumentality, or agent, knowingly:

---

[124] Madubuko, Yana, The Protection of Trade Secrets: A Comparative Analysis of the United States and European Union, Bachelor's Thesis, Tallinn University of Technology (2018), available at http://digi.lib.ttu.ee/i/file.php?DLID=10108&t=1 (last visited March 20,2025) .
[125] 18 U.S.C. § 1839(3).
[126] 18 U.S.C. § 1839(3) (see also Simon, Spencer, The Economic Espionage Act of 1996, Berkeley Technology Law Journal, Article 20, Vol. 13, Issue 1, p. 311, available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1174&context=btlj (last visited March 20, 2025)).

1. Steals, appropriates, takes away, or conceals a trade secret without proper authorisation or acquires a trade secret by fraud, trickery, or deception;

2. Copies, duplicates, sketches, draws, photographs, downloads, uploads, changes, deletes, photocopies, replicates, transmits, distributes, mails, communicates, or reveals a trade secret without authority;

3. Knows that a trade secret has been stolen, appropriated, obtained, or converted without authorisation and receives, buys, or possesses it;

4. Attempts to commit any of the above offences or

5. Conspires with one or more persons to commit any of the offences above, and at least one of them performs an act in furtherance of the conspiracy, Shall be liable to a fine of up to $500,000 or imprisonment for up to 15 years, or both. When an organisation commits the offence, the fine may be up to $10,000,000.

- **Theft of Trade Secrets:**
  According to the EEA, any person who converts a trade secret (related to or contained within a product marketed in interstate or foreign commerce) for the economic benefit of someone other than its owner and thereby intentionally causes injury to the owner, who:

1. Steals, appropriates, takes away, or conceals the trade secret without proper authorisation or acquires it through fraud, trickery, or deception;

2. Copies, duplicates, sketches, draws, photographs, downloads, uploads, changes, deletes, photocopies, replicates, transmits, distributes, mails, communicates, or reveals the trade secret without authority;

3. Knows that the trade secret has been stolen, appropriated, obtained, or converted without authorisation and receives, buys, or possesses it;

4. Attempts to commit any of the offences listed in paragraphs (1) through (3) or

5. Conspires with others to commit any of the offences above, Except as provided in subsection (b), shall be liable to a fine or imprisonment for a term not exceeding ten years, or both. An organisation that commits the same offence is liable to a fine not exceeding $5,000,000. Moreover, following

amendments under the 2016 DTSA, the penalty for an organisation is now set at the greater of $5,000,000 or three times the value of the stolen trade secret to the organisation, including any cost savings from avoided research and design expenses.[127]

3.11.5 Elements of Offence under Section 1832

To secure a conviction under Section 1832, the government must establish that:

1. The defendant unlawfully stole, acquired, deleted, or communicated information without the owner's consent.[128]
2. The defendant was aware that the information in question was confidential.[129]
3. The information qualified as confidential, i.e., a trade secret.[130]
4. The defendant intended to exploit the trade secret for the financial benefit of a party other than its owner.[131]
5. The defendant either knew or intended that such conduct would cause harm to the owner of the trade secret.[132]
6. The trade secret was connected to, or incorporated, a product manufactured or distributed in interstate or international commerce.[133]

Moreover, Section 1832 requires a specific mental state for domestic violations: the perpetrator must plan to convert the trade secret into economic gain for someone other than the owner and possess the intent (or a reason to know) that such misappropriation would injure the owner. In contrast, Section 1831 (addressing foreign violations) requires that the perpetrator have the intention, knowledge, or reason to know that the theft of a trade secret would benefit a foreign government, instrumentality, or agent.[134]

3.11.6 Exceptions Recognised Under the Economic Espionage Act of 1996

[127] 18 U.S.C. § 1832.
[128] Ibid.
[129] Ibid.
[130] Ibid.
[131] Ibid.
[132] Ibid.
[133] Ibid.
[134] See, e.g., 18 U.S.C. §§ 1831 and 1832.

The Act expressly provides that Chapter 90, which governs the protection of trade secrets, does not create a private right of action or prohibit the following:

1. Lawful activities conducted by any U.S. government entity, state, or political subdivision thereof.[135]
2. Reporting an alleged violation to a U.S. governmental entity, state, or political subdivision if that entity has the legal authority to address the alleged infringement.[136]

3.11.7 Provision for Criminal Forfeiture

Under the Economic Espionage Act of 1996, if a defendant is convicted of an offence under this chapter, the court is empowered to order the forfeiture of the defendant's property. Specifically, the court may require the forfeiture of:

1. Any property, or any proceeds derived therefrom, acquired directly or indirectly as a result of the violation and
2. Any property used or intended for use in committing or facilitating the violation, with due consideration of the nature, scope, and proportionality of its involvement in the offence.[137]

3.11.8 Defences

While the Economic Espionage Act of 1996 does not explicitly list defences, its legislative history suggests that the traditional defences applicable in civil trade secret misappropriation cases also apply in criminal prosecutions. In particular, the following defences may be available:

- **Parallel Development:** A trade secret owner has no absolute monopoly over the underlying knowledge, and independent discovery through diligent research is permissible.[138]
- **Reverse Engineering:** Deconstructing a product to understand how it was made is a lawful method of discovering its trade secret components.[139]

---

[135] 18 U.S.C. § 1833, as amended by the Defend Trade Secrets Act, 2016.
[136] Ibid.
[137] 18 U.S.C. § 1834.
[138] See Simon, Spencer, *The Economic Espionage Act of 1996*, 13 Berkeley Tech. L.J. 305, 312 (1998).
[139] Ibid.

Thus, common defences include:

1. Lack of knowledge that the information was meant to remain confidential.
2. The trade secret was not misappropriated for economic benefit (for example, if the secret was used solely to improve reputation).
3. The information did not qualify as a trade secret because it lacked economic value, was already public, or was not subject to reasonable security measures.[140]

3.11.9 Preservation of Confidentiality

The Economic Espionage Act mandates that courts take all necessary steps to protect the confidentiality of trade secrets during legal proceedings. This includes:

1. Issuing orders that require the protection of any trade secret involved in the litigation by the Federal Rules of Criminal and Civil Procedure and the Federal Rules of Evidence.
2. Preventing the disclosure of trade secret information by not permitting or ordering its release unless the owner submits a sealed statement indicating their wish to maintain confidentiality.
3. Ensuring that any disclosure during litigation does not constitute a waiver of the trade secret's protection unless the owner has explicit consent.[141]

3.11.10 Limitations of the Economic Espionage Act of 1996

The Economic Espionage Act has notable limitations:

1. It does not extend protection to trade secrets related to services, negative know-how, or information obtained via reverse engineering.
2. It may not fully address the needs of U.S. companies operating internationally to prevent the theft of trade secrets.

[140] Ibid.
[141] 18 U.S.C. § 1835.

3. The Act fails to provide victims with civil remedies for the economic harm caused by the theft or misappropriation of their trade secrets, as all penalties and forfeitures accrue solely to the government.[142]

For example, in *United States v. Aleynikov*, the Second Circuit reversed the conviction of a trader who copied Goldman Sachs software before leaving for a new position, holding that the Act applied only to trade secrets related to products intended for commercial distribution. Following this decision, Congress passed the Trade Secrets Clarification Act of 2012, which amended the Economic Espionage Act to include trade secrets used internally to supply services to third parties, effectively closing this loophole.[143]

The Economic Espionage Act of 1996 establishes two distinct regulatory approaches: Section 1831, which targets trade secret theft benefiting foreign entities, and Section 1832, which focuses on domestic misappropriation. The Act criminalises the theft of trade secrets, imposing severe penalties such as fines and imprisonment, and includes a provision for criminal forfeiture of property derived from such violations.[144] Additionally, while the Act does not explicitly provide defences, traditional civil defences (including parallel development and reverse engineering) remain applicable. It also requires courts to preserve the confidentiality of trade secrets during legal proceedings. Nonetheless, the Act has limited coverage and remedy provisions, prompting subsequent legislative amendments to address these gaps.[145]

II. Trade Secrets Law in India – Legal Framework, Judicial Trends, and the Road to Reform

3.12 Introduction

In the data-centric global economy where we now live and work, confidential business information has become vital as it goes to the heart of competitive advantage. Trade secrets are all about proprietary business practices, technical knowledge, formulas, or strategic information, some of the most valuable intellectual assets. Unlike patents and trademarks, trade secrets are not formally registered and protect confidential business

[142] See Simon, Spencer, *The Economic Espionage Act of 1996*, supra.
[143] Ibid.
[144] Ibid.
[145] Ibid.

information, for some time (e.g. 5 years) or in perpetuity, so long as it remains confidential and derives economic value from not being known.

India has been a party to the TRIPS Agreement, and there is no exclusive statutory Trade secrets regime yet. It also discusses the limitations of the Indian legal system in dealing with spam, which does not have a dedicated law against it, but only clings to a piecemeal labyrinth consisting of common law, contract and some statutory provisions under the Indian Information Technology Act, 2000, with an increasing number of judicial precedents. As a result, this coverage void has produced inconsistent enforcement, legal ambiguity, and an inadequate shield for businesses, particularly in biotechnology, pharmaceuticals, and high-tech industries.

Under the continued pressure to reform, the 22nd Law Commission of India recommended the Draft Trade Secrets Bill, 2024. This proposed legislation is a turning point in India's IP jurisprudence as it seeks to codify trade secret protections at par with international benchmarks. The current chapter critically discusses the legal position and some essential judicial trends, examines the bill, and focuses on India's interface of trade secrecy, innovation, and public policy imperatives.

3.13. Conceptual Foundations of Trade Secrets

3.13.1. Definition and Characteristics

Trade secret definitions vary from one country to another, but there are similarities among them. Trade secrets are defined to mean Information, as provided in Article 39(2) of the TRIPS Agreement:

a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

b)has commercial value because it is secret; and

c) has been subject to reasonable steps under the circumstances, by the person lawfully controlling the information, to keep it secret.

1. It is not common or easy for people who follow or need this information to access this knowledge.

2. Secret and of commercial value; and

3. Has not become) generally known to, and has not been) readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use.[146]

At common law, a trade secret is a subset of confidential information, but one which is additionally commercially valuable and which is the subject of reasonable efforts to maintain its secrecy. Indian courts, without a statutory definition, have also referred to these international benchmarks. In American Express Bank Ltd. v. Priya Puri, the Delhi High Court held that a list of customers' names and contact details, if maintained in confidence, can be treated as a trade secret because of commercial value and possible competitor misuse[147].

Technical knowledge is not the only form of trade secret. It may also relate to the marketing process, pricing structure, supplier or customer lists, algorithms, source codes, and managerial strategies. One key difference is that trade secrets are only well protected so long as they maintain their status as secrets. Unless publicly disclosed or not adequately secured, there are no rights to protect.

3.13.2 Other IP Rights vs. Trade Secrets

Regarding duration, enforceability and formalities, trade secrets radically differ from any other intellectual property right. Unlike patents, which must be disclosed to the public registry, trade secrets may be kept secret and have an indefinite term. Either way, such potential durability is downvoted by being vulnerable to loss through reverse engineering, leaks, and industrial espionage.

The difference is reinforced in the legal remedies. Patent infringers are subject to statutory damages and possible criminal penalties, while trade secret misappropriators are effectively subject to restraining orders and civil remedies in breach of contract equity. In addition, trade secrets frequently complement the void where patent protection is infeasible - news of the product of the "novelty," the failure of

[146] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39(2), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S.299.
[147] American Express Bank Ltd. v. Priya Puri, 2006 (110) DLT 548 (Del. HC).

"patentability" requirements or the simple strategic decision to prefer some secrecy over publication.

In India, this distinction has practical implications since where there exist statutes specifically dealing with copyrights, trademarks and patents, the protection for trade secrets is left to depend on contract and relevant common law[148].

3.14 Statutory and Judicial Framework in India

3.14.1 The Indian Contract Act, 1872

Since no proper trade secret law exists, trade secrets in India are mostly safeguarded through contracts. Section 27 of the Indian Contract Act, which was made in 1872, is especially relevant for agreements in restraint of trade. Even though such clauses are not allowed, Indian courts exempt certain confidentiality agreements as long as they do not render it difficult for professionals to move to other jobs. By ruling in *Gujarat Bottling Co. Ltd v. Coca Cola Co.*, the Supreme Court decided that negative covenants during the contract period survive because of Section 27, thereby permitting agreements between employees and employers that impose confidentiality[149]. In addition, courts regularly require people to respect NDAs when the agreement limits what can be discussed and sets a timeframe. Misappropriating confidential information by an employer may result in damages, which Section 73 of the Act allows them to claim. Yet, courts have hesitated to pay large amounts in compensation since it is hard to measure the economic damage properly[150].

3.14.2 The Information Technology Act, 2000

Although the IT Act, 2000 was mainly enacted for cyber law, it has two important provisions for protecting trade secrets.

1. When intermediaries and authorities wrongly access someone's electronic records, they face a fine under Section 72.
2. It is required by Section 43A that any body corporate processing sensitive personal data put in place reasonable security procedures and is responsible for

[148] Faizanur Rahman, Trade Secrets Law and Innovation Policy in India, 3 INDIAN J.L. & PUB. POL'Y 119, 123–126 (2016).
[149] Gujarat Bottling Co. Ltd. v. Coca Cola Co., (1995) 5 SCC 545.
[150] Chirantan Priyadarshan, Open Secrets of Trade in India: An Analytical Study of Trade Secrets in the Uncodified Legislative Regime in India, 5 INDIAN J.L. & LEGAL RSCH. 1, 5–6 (2023).

any neglect that results in a data breach[151]. They are not much help in trade secret litigation because they were designed to protect personal and electronic data instead of business-related secrets. Yet, these sections are sometimes mentioned alongside claims made in cases of cyber theft of trade secrets or digital misappropriation.

3.14.3 The Indian Penal Code of 1860

According to the IPC, trade secrets are not a specific topic. Yet, certain chapters have been applied to situations of trade secret theft:

• Sections 408 and 409: Offences of criminal breach of trust by both clerks and public servants. • Section 420 deals with cheating and taking property dishonestly.

• Section 403: Dishonestly taking other people's property is an offence.

Usually, law enforcement treats trade secret theft as a civil matter, as prosecutions are very uncommon. *The Bombay High Court in Zee Telefilms Ltd. v. Sundial Communications Pvt. Ltd.* suggested that IPC provisions were insufficient for protecting trade secrets, pointing out that adequate protection requires civil courts[152].

3.14.4 Companies Act, 2013

According to the Companies Act, 2013, directors and key managerial personnel must act in good faith and the best interests of the company (Section 166). When directors breach such duties, primarily when they act against the company's confidential interests, the law may allow shareholders to file a lawsuit. Section 128 also requires companies to maintain accounts. Nevertheless, the Act does not directly cover trade secrets or suggest solutions for their protection. It provides the duty to servants but lacks detailed rules about trade secrets.

3.14.5 In the Common Law, one central doctrine is called Breach of Confidence.

Many trade secret cases in India are decided using common law principles of fairness. Any breach of confidence claim is possible if there was a required secrecy and the recipient improperly took advantage of the information. Chemical Process Equipment Pvt. Ltd. required confidential technology drawings supplied by a consultant. The High

[151]Information Technology Act, No. 21 of 2000, India Code (2000), Section 72, 43A.
[152] Zee Telefilms Ltd. v. Sundial Communications Pvt. Ltd., (2003) Bom CR (Supp) 404

Court in Delhi ruled that taking the information without permission is forbidden, regardless of whether the information had been formally registered[153].

The same is true for *Diljeet Titus v. Alfred A. Adebare*[154], the Delhi High Court stopped former associates from taking the client list and internal bank of data that belongs to the law firm. The court decided that confidentiality duties stay in effect even after the end of an employment or partnership[155]. The courts are willing to apply confidentiality rules based on what is expected in employee-employer and other professional relationships.

3.15 Case Law Analysis: Judicial Interpretation of Trade Secret Protection in India

3.15.1 Employer-Employee Disputes: Post-Employment Confidentiality

The majority of trade secret litigation in India arises from the employment context, particularly where former employees attempt to use or disclose confidential information acquired during their tenure. Indian courts have generally enforced contractual and equitable obligations of confidentiality, even post-employment, provided the restrictions are narrowly tailored and do not unreasonably restrain trade.

In *Hi-Tech Systems & Services Ltd. v. Supra Bhat Ray*, the Calcutta High Court upheld a two-year post-employment non-compete clause. The court emphasised that such a clause was not an unreasonable restraint under Section 27 of the Contract Act because it was designed to protect confidential information and client relationships developed by the employer[156]. Importantly, the court recognised the distinction between general skills acquired during employment (which are not protectable) and specific confidential data or methods (which are).

Similarly, in *Fairfest Media Ltd. v. ITE Group PLC*, the Delhi High Court granted an interim injunction against a former associate who misappropriated internal event plans and client contacts. The court reiterated that while employment mobility is a constitutional right, protecting trade secrets justifies limited restrictions in the interest of fair competition[157].

---

[153] John Richard Brady's case. Chemical Process Equipment Pvt. Ltd., AIR 1987 Del. 372.
[154] Diljeet Titus v. Alfred A. Adebare & Ors., 130 (2006) DLT 330 (Del. HC).
[155]Alfred A. Adebare, *Democracy in the U.S.: Theories and Trends with The Development of Democracy as America's Legal Tradition*, 130 DLT 330, 1 (2006).
[156] *Hi-Tech Sys. & Servs. Ltd. v. Supra Bhat Ray*, (2022) 2 Cal LJ 183 (Cal HC).
[157] Fairfest Media Ltd. v. ITE Group PLC, 2016 SCC OnLine Del 6749.

In *American Express Bank Ltd. v. Priya Puri*, the court held that a financial institution's client list constituted a trade secret. The court refused to strike down the confidentiality clause, observing that the "trust reposed by clients" formed the core value protected by the employer[158].

These cases collectively establish that Indian courts are willing to enforce confidentiality clauses and post-employment obligations, especially where the claimant demonstrates that the information is not readily available in the public domain and that adequate steps were taken to maintain its secrecy.

3.15.2 Proprietary Business Information and Technical Know-How

Trade secret litigation is not confined to client lists or market strategies. Cases involving proprietary formulas, technical drawings, and design documents often form the core of judicial disputes in the manufacturing and engineering sectors.

In *Escorts Construction Ltd. v. Action Construction Equipment Pvt. Ltd.*, the Bombay High Court issued a permanent injunction restraining former employees from misusing crane design blueprints. The court considered the technical drawings trade secrets protected by contract and equitable principles[159].

A similar position was adopted in *Rochem Separation Systems (India) Pvt. Ltd. v. Nirtech Pvt. Ltd.* (2023), where the Bombay High Court was asked to prevent ex-employees from allegedly misappropriating proprietary designs and technological processes. While emphasising the importance of specificity, the court denied interim relief because the plaintiff failed to provide sealed or verifiable documentation of what constituted confidential information. This judgment illustrates a recurring theme in Indian jurisprudence: the need for trade secret holders to identify precisely what information is hidden and how it was misused[160].

These rulings reinforce the importance of detailed pleadings, documentary evidence, and demonstrable efforts to maintain confidentiality to succeed in a claim.

3.15.4 Breach of Confidence without Contractual Privity

[158] American Express Bank Ltd. v. Priya Puri, 2006 (110) DLT 548 (Del. HC).
[159] Escorts Construction Ltd. v. Action Construction Equipment Pvt. Ltd., (1999) 77 DLT 648.
[160] Rochem Separation Systems (India) Pvt. Ltd. v. Nirtech Pvt. Ltd., 2023 SCC OnLine Bom 1572.

One of the strengths of Indian jurisprudence is the extension of protection beyond the confines of contract law. Even without formal NDAs, Indian courts have applied common law doctrines of breach of confidence.

In *Mr. Anil Gupta v. Mr. Kunal Dasgupta*, the Delhi High Court restrained the unauthorised use of a confidential business idea submitted to a television producer. The court held that a duty of confidence arose from the circumstances, despite the absence of a written contract. The court remarked, "An idea may be inchoate, but it can still be a valuable form of intellectual property deserving protection".[161]

This case is significant because it demonstrates that trade secret protection is not merely procedural or technical; it is grounded in substantive equitable obligations that attach in situations of trust or implied confidence.

3.16 The Draft Trade Secrets Bill, 2024

3.16.1 Background and Legislative Need

The absence of a codified legal regime for trade secret protection in India has been a long-standing concern among stakeholders, particularly in the wake of India's commitments under the TRIPS Agreement. Article 39(2) of TRIPS mandates that member states protect undisclosed information that has commercial value, is not generally known, and is subject to reasonable steps for secrecy[162]. Indian jurisprudence has thus far relied on common law doctrines and contract enforcement, which, while valuable, lack the consistency and clarity that a statutory framework would provide.

Recognising this gap, the 22nd Law Commission of India proposed a comprehensive Draft Trade Secrets Bill in 2024. This proposed legislation aims to consolidate existing legal principles, align with international standards, and provide businesses with an effective remedy against misappropriation.

3.16.2 Definition and Scope

The Draft Bill defines a "trade secret" as any information that:

[161] Mr. Anil Gupta v. Mr. Kunal Dasgupta, 97 (2002) DLT 257.
[162] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39(2), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.

1. It is not generally known or readily accessible to persons within the circles that typically deal with such information;
2. Has commercial value because it is secret; and
3. Has been subject to reasonable steps to maintain secrecy by the person lawfully in control of it.[163]

This definition mirrors Article 39 of TRIPS and reinforces a standard that balances confidentiality with commercial utility. Notably, the Bill excludes from the definition any information that becomes public through lawful means such as reverse engineering or independent discovery, thereby safeguarding legitimate competition.

3.16.3 Civil Remedies and Adjudication

The Bill creates a statutory cause of action for the "misappropriation" of trade secrets, broadly defined as acquisition through unlawful means, breach of confidence, or use of information without authorisation. The proposed remedies include:

- Permanent and interim injunctions;
- Damages or account of profits;
- Delivery up and destruction of materials containing trade secrets[164].

Notably, the Bill designates Commercial Courts, established under the Commercial Courts Act, 2015, as the appropriate forums for adjudication. This provision aligns trade secret litigation with the broader trend of commercial law specialisation and fast-track dispute resolution.

3.16.4. Exceptions: Whistle-blower and Public Interest

In a progressive move, the Draft Bill includes robust public interest exceptions. Section 9 exempts from liability any disclosures made:

- To expose wrongdoing or illegal conduct;
- In compliance with a statutory or judicial obligation;

[163] Draft Trade Secrets Bill, 2024, Section 2(f) (Law Commission of India, Consultation Paper, 2024).
[164] Id. Section 8

- For safeguarding public health, the environment, or national security[165].

These carve-outs recognise that not all disclosures of confidential information are malicious or commercially exploitative. They ensure that regulatory oversight and whistleblower protections are not curtailed by aggressive trade secret litigation.

3.16.5 Evaluation and Critique

The Draft Trade Secrets Bill, 2024, is a significant advancement in Indian IP law. It seeks to:

- Harmonise Indian law with TRIPS obligations;
- Enhance judicial efficiency through Commercial Court jurisdiction.
- Provide legal clarity to businesses, including start-ups and multinationals;
- Foster innovation by encouraging contractual protections reinforced by statute.

However, critiques remain. The Bill lacks provisions for:

1. Criminal sanctions, raising questions about deterrence in high-value thefts;
2. Extraterritorial application, unlike the U.S. Defend Trade Secrets Act, which allows international misappropriation claims.
3. Detailed evidentiary protocols, such as in-camera proceedings or confidentiality clubs, beyond a general court discretion clause.

Furthermore, the Draft Bill does not expressly resolve the ambiguity posed by Section 27 of the Indian Contract Act, which continues to invalidate overly broad NDAs and non-compete clauses. Without a harmonisation clause or an override provision, this could lead to judicial fragmentation.

Despite these issues, the Bill is a much-needed step towards building a modern, investor-friendly legal infrastructure that balances proprietary protection with public accountability.

3.17 International Obligations and Comparative Perspectives

3.17.1 India's Obligations under TRIPS

[165] Id, Section 9.

As a founding member of the World Trade Organisation (WTO), India is bound by the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which sets minimum standards for protecting and enforcing various forms of intellectual property, including undisclosed information. Article 39(2) of TRIPS obligates members to protect trade secrets by ensuring that:

1. The information is secret.
2. It has commercial value because it is secret, and
3. Reasonable steps have been taken to maintain its secrecy[166].

Although TRIPS does not prescribe a uniform method for achieving compliance, it allows countries to implement protection through civil, criminal, or administrative measures. India has largely complied with this obligation through contract law, tort principles, and equitable remedies. However, the lack of a dedicated trade secrets statute has been a recurring concern in WTO Trade Policy Reviews and bilateral trade dialogues[167].

The Draft Trade Secrets Bill, 2024, would represent India's most direct compliance measure under Article 39 by codifying protection and standardising enforcement.

3.17.2 United States: Uniform Trade Secrets Act and DTSA

The United States provides a dual-level protection regime for trade secrets. At the state level, the Uniform Trade Secrets Act (UTSA), adopted by 48 states, offers a model law framework that defines misappropriation, specifies remedies, and ensures civil enforcement.

At the federal level, the Defend Trade Secrets Act (DTSA), 2016, provides a nationwide civil remedy and allows trade secret holders to bring suits in federal courts, including extraterritorial claims involving overseas theft.[168]

Key features of the U.S. system include:

---

[166] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39(2), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.
[167] Swarnima Singh, Examining the Regulation of Trade Secrets in India and the United States of America: A Comparative Analysis, 7 INT' L J.L. MGMT. & HUMAN. 4424, 4432–4435 (2024).
[168] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified at 18 U.S.C. S.S 1831–39).

- Criminal penalties under the Economic Espionage Act;
- Seizure provisions to prevent the dissemination of stolen secrets;
- Whistle-blower immunity for disclosures in compliance with legal obligations.

The U.S. framework is notable for combining civil and criminal enforcement with procedural safeguards, including protective orders, confidential filings, and limited access discovery. India currently lacks such a holistic infrastructure.

3.17.3 European Union: Trade Secrets Directive

The EU adopted the Directive (EU) 2016/943 on the Protection of Trade Secrets in 2016, which mandates member states to provide uniform protection against unlawful acquisition, use, and disclosure of trade secrets.

The directive recognises lawful acquisition through independent discovery, reverse engineering, and freedom of expression exceptions. It also includes remedies such as injunctions, destruction of infringing goods, and compensatory damages[169].

What sets the EU model apart is its focus on procedural protection of confidential information during litigation. Courts must take specific measures, including restricted access hearings and anonymisation, to ensure that judicial processes do not inadvertently compromise trade secrets.

India can draw valuable lessons from the EU model, especially in procedural law reforms, such as setting up confidentiality clubs, in-camera proceedings, and protective filing systems to manage sensitive information during trial.

3.17.4 Key Takeaways for India

India's future trade secret framework can be benchmarked against TRIPS obligations and practical innovations developed in the U.S. and EU. These include:

- Harmonising substantive protection with procedural tools;
- Balancing business confidentiality with public interest disclosures;

[169] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, 2016 O.J. (L 157) 1.

- Facilitating both civil and criminal enforcement where appropriate;
- Establishing fast-track forums with technical expertise.

India risks undermining investor confidence without systemic innovation, particularly in sensitive sectors such as defence, pharmaceuticals, and fintech.

3.18 Public Interest, Innovation, and Transparency

3.18.1 Trade Secrets and Innovation Incentives

Trade secrets serve as a vital mechanism for preserving innovation incentives, especially in sectors where patents may be unavailable, unsuitable, or too costly. Start-ups and medium-sized enterprises, in particular, may prefer trade secret protection over patents because it avoids the financial burden of registration and allows for perpetual protection as long as secrecy is maintained.

In the Indian context, Faizanur Rahman notes that the absence of codified protection deters firms, especially those in R&D-intensive sectors, from collaborative innovation or knowledge sharing, due to fears of misappropriation[170]. The biotechnology, pharmaceutical, and agro-tech industries frequently rely on proprietary processes or formulations that may not meet the novelty or non-obviousness threshold required for patent protection. Here, trade secrets are the only viable means of preserving competitive advantage.

By providing statutory certainty, the Draft Trade Secrets Bill, 2024, is expected to foster increased investment in innovation ecosystems, especially in emerging hubs such as Bangalore, Hyderabad, and Pune, where IP-sensitive industries are flourishing.

3.18.2 Tension with the Right to Information

The public interest exception to trade secret protection is deeply relevant in India due to the expansive interpretation of the right to information (RTI). Under Section 8(1) (d) of the Right to Information Act, 2005, disclosure of commercial information, including trade secrets, is exempt if it harms the competitive position of a third party, unless the disclosure serves a larger public interest.

[170] Faizanur Rahman, Trade Secrets Law and Innovation Policy in India, 3 INDIAN J.L. & PUB. POL'Y 119, 125–128 (2016).

The interface between trade secrets and transparency obligations came under scrutiny in debates surrounding the Biotechnology Regulatory Authority of India (BRAI) Bill, which sought to classify regulatory filings by biotech companies as confidential, thereby limiting public access to genetically modified organism (GMO) trial data. Critics, including Himanshi Garewal, argued that this would lead to regulatory opacity and undermine democratic oversight of science policy[171].

Indian courts have historically weighed public interest exceptions against secrecy in a fact-sensitive manner. In *Kush Kalra v. Union of India*, the Delhi High Court held that the public interest in disclosing the criteria used for judicial appointments overrode the confidentiality claimed by the Collegium, emphasising that vague claims of secrecy must not undermine transparency[172].

In trade secret jurisprudence, this tension will likely manifest in disputes where proprietary data intersects with health, environment, or governance issues. The Draft Bill's Section 9 rightly accommodates this by allowing disclosure where it is necessary to expose wrongdoing or protect the public.

3.18.3 Balancing Confidentiality and Accountability

International best practices suggest that trade secrets should not serve as a tool for shielding corporate misconduct. For example, the Trade Secrets Directive in the European Union allows courts to deny protection to information used to conceal wrongdoing, misrepresentation, or illegal conduct.

The Draft Trade Secrets Bill, 2024, reflects this normative evolution by:

- Exempting whistle-blowers from liability if the disclosure was made in good faith;
- Enabling courts to assess whether public interest outweighs commercial secrecy;
- Allowing disclosures in compliance with judicial or statutory obligations.

[171] Himanshi Garewal, Interface between Trade Secrets and GMOs in India: The Way Forward, 2 INDIAN J.L. & LEGAL RSCH. 1, 6–8 (2021).
[172]Kush Kalra v. Union of India, 2021 SCC OnLine Del 3522.

Such provisions are essential to maintain legitimacy and avoid overreach. Without adequate public interest exceptions, trade secret law risks becoming a shield for anti-competitive practices, regulatory capture, or suppression of safety data.

3.18.3 Role in the National Innovation Policy

India's broader innovation policy, reflected in the National Intellectual Property Rights (IPR) Policy (2016), the Startup India initiative, and sectoral strategies, calls for strengthening trade secret protection as part of a well-rounded IP ecosystem.

A codified trade secret regime will:

- Provide clarity to foreign investors concerned about data confidentiality.
- Reduce reliance on restrictive non-compete clauses that may violate Section 27 of the Contract Act;
- Create an enabling environment for incubators, accelerators, and academic-industry collaborations.

Abhijeet Kumar and Adrija Mishra state, "A well-drafted law would not only protect secrets but also foster a climate of legal predictability essential for innovation and economic growth"[173].

3.19 Challenges and the Way Forward

3.19.1 Legal Fragmentation and Absence of a Sui Generis Framework

The most fundamental challenge to trade secret protection in India is the lack of a dedicated, comprehensive statute. The current reliance on a patchwork of civil, contractual, and equitable principles, while flexible, has resulted in inconsistent judicial outcomes and interpretive ambiguities.

Legal scholars, such as Shruti Nandwana, have noted that without a codified legal framework, stakeholders face considerable uncertainty about enforceability, applicable remedies, and judicial thresholds of "reasonableness" in confidentiality practices[174]. This unpredictability undermines the incentive to develop and share proprietary

[173] Abhijeet Kumar & Adrija Mishra, Protecting Trade Secrets in India, 18 J. WORLD INTELL. PROP. 335, 341 (2015).
[174] Shruti Nandwana, Comparative Analysis of Regulatory Framework Governing Trade Secrets in United States, United Kingdom and India, 1 DHARMASHASTRA NAT'L L. UNIV. L. REV. 112, 118–121 (2022).

information, especially in collaborative research or cross-border technology transfer arrangements.

The Draft Trade Secrets Bill, 2024, aims to resolve this by offering a clear statutory definition, coherent procedural remedies, and jurisdictional clarity through Commercial Courts. However, its implementation must be accompanied by public education, judicial training, and awareness-building within industry and academia.

3.19.2 Evidentiary and Procedural Constraints

One of the recurrent bottlenecks in Indian trade secret litigation is the high evidentiary burden placed on the plaintiff. Courts require:

- Precise identification of the confidential information;
- Proof of reasonable efforts taken to maintain secrecy;
- The defendant's actions and the alleged misappropriation have a clear causal linkage[175].

As observed in *Rochem Separation Systems (India) Pvt. Ltd. v. Nirtech Pvt. Ltd.*, the plaintiff's failure to specify what constituted the trade secret and how it was misused led to the denial of interim relief. Courts are reluctant to grant injunctions on vague or general assertions of proprietary rights[176].

Moreover, Indian procedural law lacks formalised mechanisms such as:

- Sealed filings for trade secret claims;
- In-camera hearings for confidential evidence.
- Confidentiality clubs for expert-only disclosures.

While some courts have innovatively adopted confidentiality clubs (as in *Vestergaard Frandsen v. Bestnet Europe Ltd.*), these remain discretionary and inconsistent. Legislative codification of such procedures would help normalise best practices.

3.19.3 Weak Remedies and Enforcement Challenges

[175] Swarnima Singh, Examining the Regulation of Trade Secrets in India and The United States of America: A Comparative Analysis, 7 INT'L J.L. MGMT. & HUMAN. 4424, 4436–4438 (2024).
[176] Rochem Separation Systems (India) Pvt. Ltd. v. Nirtech Pvt. Ltd., 2023 SCC OnLine Bom 1572.

Although injunctions are commonly granted, Indian courts are conservative in awarding monetary damages in trade secret disputes. Few reported cases involve substantial compensatory or punitive damages, which dilutes deterrence.

Criminal remedies under the IPC or the IT Act are limited in scope and rarely pursued due to evidentiary complexity, high burden of proof, and procedural delays. In contrast, the United States' Economic Espionage Act criminalises trade secret theft and imposes substantial penalties, demonstrating the importance of integrating civil and criminal enforcement to bolster protection[177].

India's enforcement mechanism must also address cross-border misappropriation, which is currently outside the scope of domestic statutes. The Draft Trade Secrets Bill does not provide for extraterritorial jurisdiction, a lacuna that could be exploited in cases involving digital theft by foreign entities.

3.19.4 Interplay with Labour Law and Section 27 of the Contract Act

Another enduring complexity lies in reconciling trade secret protection with Indian labour law and Section 27 of the Indian Contract Act, which prohibits agreements in restraint of trade. This has led to many non-compete clauses being struck down even when designed to protect legitimate business interests.

Courts have enforced confidentiality obligations post-employment, but any clause that effectively bars a person from working in the same industry will likely be void. This creates a grey area for employers attempting to safeguard proprietary information without violating constitutional and contractual protections.

The Draft Bill does not resolve this tension. A harmonised statutory approach would provide clarity, perhaps by carving out an exception for narrowly drawn non-disclosure covenants.

3.19.5 Capacity Gaps in Judiciary and Regulatory Bodies

Finally, effective implementation of trade secret protection requires technical capacity in the judiciary and regulatory institutions. Judges must be equipped to handle complex scientific, technological, and financial data underlying trade secret disputes.

[177] Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. Section 1831–1839).

Similarly, agencies like the Competition Commission of India (CCI), the Telecom Regulatory Authority of India (TRAI), and sector-specific regulators must be trained to distinguish between legitimate confidentiality and anti-competitive information hoarding.

India's IP regime has matured significantly in areas like patents and trademarks, with specialised tribunals and IP Appellate Boards. A similar investment in trade secret adjudication, through dedicated benches or judicial training, would enhance credibility and enforcement.

3.20 Conclusion

Trade secrets occupy a critical intersection between intellectual property, commercial ethics, regulatory transparency, and innovation policy. In India, the protection of trade secrets has long depended on common law doctrines, contractual enforcement, and equitable remedies, with only fragmented statutory support. While this legal pluralism has allowed flexibility, it has fostered uncertainty, inadequate deterrence, and limited enforceability.

Through case law, *John Richard Brady*, *Priya Puri*, *Hi-Tech Systems*, *Fairfest Media*, and *Rochem*, Indian courts have upheld the enforceability of trade secrets, particularly in employer-employee contexts and professional fiduciary relationships. However, their decisions also reveal persistent hurdles: lack of precise definitions, evidentiary burdens, and procedural inconsistencies.

The Draft Trade Secrets Bill, 2024, is a welcome development that seeks to codify principles consistent with India's obligations under Article 39 of the TRIPS Agreement. It defines trade secrets, delineates lawful and unlawful acquisition, assigns jurisdiction to Commercial Courts, and introduces valuable exceptions for whistleblowing and public interest disclosures. Its passage would modernise India's trade secret regime, enhance investor confidence, and foster a more innovation-friendly environment.

Yet, to be effective, the statutory framework must be accompanied by:

- Procedural reforms (e.g., in-camera hearings, sealed evidence protocols, confidentiality clubs);
- Harmonisation with the Contract Act, especially regarding Section 27 restraints;

- Clarification of damages jurisprudence and extraterritorial enforcement;
- Institutional capacity-building within the judiciary and regulatory bodies;
- Sectoral coordination between IPR policy and public interest regulations.

India's economic trajectory, particularly in high-growth sectors like biotechnology, pharmaceuticals, artificial intelligence, and clean energy, demands a trade secret regime that is both commercially robust and publicly accountable. The key lies in balancing protection with proportional transparency, competition with confidentiality, and economic incentives with ethical governance.

As trade secret law continues to evolve in India, it must be guided not only by international benchmarks but also by the unique socio-economic realities of the Indian legal system, where the boundaries of secrecy, innovation, and access are constantly being renegotiated.

3.21 U.S. and India

3.21.1 Introduction

Information, knowledge, and invention form the bedrock of economic success in the twenty-first century. Companies value trade secrets as highly as other intellectual property rights, such as patents, trademarks, and copyrights. Because secrecy is a supplement to and a substitute for formal legal protection. Many firms rely primarily on commercial secrecy to safeguard technical know-how and business information. This reliance is partly driven by the fact that pursuing a patent often necessitates public disclosure of critical details and can be very expensive. In contrast, if trade secrets are adequately maintained, they can remain protected indefinitely; notable examples include the Listerine antiseptic formula from 1879 and the Coca-Cola recipe from 1891.[178]

In the United States, trade secret policy encompasses various forms of information, such as formulas, rationales, compilations, software, devices, methods, techniques, or processes that must be used in commerce and provide a competitive advantage over rivals who lack access to the information. The Defend Trade Secrets Act (DTSA) of

[178] United States Patent and Trademark Office, Trade Secrets Policy, available at https://www.uspto.gov/patents-getting-started/international-protection/trade-secret-policy(last visited March 4, 2025).

2016 has further reinforced this protection by allowing disputes to be resolved under federal law. Although individual state laws may vary slightly, nearly all have adopted a version of the Uniform Trade Secrets Act (UTSA).

However, India has no dedicated statutory framework for trade secrets. Instead, protection is derived from a patchwork of legal mechanisms, including contract law, copyright, design law, information technology law, and common law principles. Efforts have been made to codify trade secret protection through initiatives like the National Innovation Act (2008) and the National IPR Policy, but these remain unenforced.[179]

3.21.2 Conclusion

A comparative analysis of trade secret protection between India and the United States is crucial to understanding the strengths and weaknesses of each regime. In the U.S., a well-structured system provides robust protection on both the civil and criminal fronts. Such a comparison helps to evaluate whether India's current level of security is sufficient, what steps might be necessary to improve it, and how these improvements might be implemented to meet evolving needs.

In India, there is no formally recognised statutory definition of trade secrets. Although the National Innovation Act (2008) defines "Confidential Information," this definition has two key drawbacks. First, while "trade secrets" and "confidential information" are often interchangeable, they are not identical. Second, the Act has not been enforced. The National Innovation Act's definition is broad yet restrictive in scope; it is modelled on the TRIPS Agreement's definition of trade secrets and, as such, lacks originality and clarity regarding whether such information should be treated as property.

Conversely, U.S. law provides clear statutory definitions. Under the UTSA, a trade secret is defined as information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
(a) Is secret because it is not generally known or readily ascertainable by those who might benefit economically from its disclosure or use;
(b) Has commercial value precisely because it is secret; and

[179] Gaido, Chiara, Trade Secret Protection in US and in Europe: A Comparative Study, available at https://www.researchgate.net/publication/321761790_The_trade_secrets_protection_in_US_and_in_Europe_a_comparative_study (last visited March 7, 2025).

(c) Is subject to reasonable steps to maintain its secrecy.[180] This definition is more inclusive than the Restatement of Torts (First), which required continuous employment of the secret in business. The definitions under the DTSA and the Economic Espionage Act are even broader, thereby providing more comprehensive protection than the definition proposed in India's National Innovation Act.[181]

In India, trade secret protection is derived from contractual and common law remedies. Because the National Innovation Act is not enforced, remedies such as injunctions and damages must be sought under other legal instruments. In practice, a trade secret owner in India may sue for an injunction to halt unauthorised use or seek the return or destruction of misappropriated materials. The likelihood of obtaining an injunction in Indian courts is guided by fundamental principles outlined in the Code of Civil Procedure (1908), which require a prima facie case, a favourable balance of convenience, and a risk of irreparable harm. [182]Furthermore, while Indian courts may award damages, they rarely grant exemplary damages, and plaintiffs must substantiate genuine economic losses.

Under Section 27 of the Indian Contract Act (1872), agreements that restrain trade are void to the extent they are unreasonable. However, courts have interpreted this narrowly to apply only within contractual contexts.[183]

In contrast, the United States offers civil and criminal remedies for trade secret misappropriation. The UTSA provides for injunctive relief and damages. At the same time, federal laws such as the DTSA and the Economic Espionage Act offer additional remedies, including civil seizure, robust injunctive relief, and criminal penalties for wilful or malicious misappropriation. The DTSA, for instance, allows for the recovery of not only actual damages but also unjust enrichment and, in cases of egregious misconduct, exemplary damages and attorney's fees. Furthermore, a unique feature of the DTSA is the immunity it affords whistle-blowers, ensuring that individuals who report misappropriation are protected from retaliation.[184] Although India has whistle-

[180] Section 2(3) "Confidential Information" of the Uniform Trade Secrets Act, available at https://www.wipo.int/edocs/lexdocs/laws/en/us/us034en.pdf (last visited March 13, 2025).
[181] Ibid.
[182] Code of Civil Procedure, 1908.
[183] Section 27 of the Indian Contract Act, 1872 (as construed by Indian courts).
[184] 18 U.S.C. §§ 1833–1836; Whistleblower Protection Act, 2011.

blower protections under the Whistle-blower Protection Act (2011), these do not specifically address trade secret issues.

The Economic Espionage Act (EEA) of 1996 in the U.S. also criminalises two primary types of offences: economic espionage and the theft of trade secrets. The EEA imposes severe penalties, including fines and imprisonment, and includes provisions for criminal forfeiture of property derived from the offence[185]. This comprehensive, multi-layered approach to enforcement is currently absent in India.

With its statutory clarity and dual enforcement mechanisms (civil and criminal), the U.S. system provides robust protection for trade secrets. In contrast, India's reliance on a fragmented array of legal principles results in inconsistent and often inadequate protection. The benefits of a comprehensive statutory framework, as demonstrated by the UTSA, DTSA, and EEA, suggest that India would significantly benefit from enacting a dedicated trade secret law. Such a law would clarify definitions, harmonise enforcement, and offer civil and criminal remedies tailored to the modern business environment.

Protecting trade secrets is indispensable in the modern knowledge economy, where intangible assets such as proprietary processes, confidential business strategies, and technical know-how form the backbone of competitive advantage. While the United States has implemented comprehensive statutory protections through laws like the Uniform Trade Secrets Act (UTSA) and the Defend Trade Secrets Act (DTSA), ensuring robust remedies, clarity in enforcement, and judicial consistency, India continues to rely on a patchwork of contractual, equitable, and tort-based principles.

This fragmented legal environment in India undermines the enforceability and predictability of trade secret protections, particularly in cross-border contexts and cyber theft cases. The judicial recognition of trade secrets as confidential information in landmark cases such as American Express Bank Ltd. v. Priya Puri[186] and Life Cell International v. Vinay Katrela[187] underscores an implicit acknowledgement of their commercial importance. However, this recognition lacks statutory reinforcement.

[185] 18 U.S.C. §§ 1831–1834.
[186] Am. Express Bank Ltd. v. Ms. Priya Puri, 2006 SCC OnLine Del 1046.
[187] Lifecell Int'l Pvt. Ltd. v. Vinay Katrela, 2017 SCC OnLine Mad 27951.

Furthermore, the growing reliance on digital platforms has exposed the limitations of India's Information Technology Act, 2000, in dealing with cyber misappropriation of trade secrets. In contrast, the Computer Fraud and Abuse Act (CFAA) in the U.S. provides a complementary framework to protect trade secrets in the digital domain.

Until such legislative reform is enacted, Indian businesses must proactively safeguard their confidential assets through well-drafted non-disclosure agreements (NDAs), employee confidentiality clauses, internal cyber-security protocols, and prompt injunctive relief in breach cases. However, these private-law measures can only be partial substitutes for what should be a holistic legislative framework.

In conclusion, codifying trade secret law in India is no longer optional but necessary. It is imperative to fulfil India's international commitments under TRIPS and foster a secure, innovation-driven economy in an era of digital transformation and global competition.

Chapter 4

Judicial Precedents for Trade Secret Protection

Introduction

In today's knowledge economy, trade secrets are among the most valuable forms of intellectual property. Their protection enables firms to secure competitive advantage, foster innovation, and convert intangible assets into economic progress. Over the past two centuries, legal regimes- from early common law doctrines and informal contractual arrangements to sophisticated statutory systems- have safeguarded confidential business information. This evolution is driven by broader economic forces such as industrialisation and globalisation, as well as the rapid pace of technological change.

This chapter examines landmark cases contributing to the modern legal framework governing trade secret protection. By reviewing decisions from jurisdictions such as the United Kingdom, India, the United States, and the European Union, we illustrate how courts have interpreted misappropriation, breach of confidentiality, and employee obligations. Moreover, the analysis highlights the enduring challenges of proving economic value and secrecy and the complexities introduced by digital commerce.

4.1 Case Laws

1. John Richards Brady v. Chemical Equipment's[188]

Facts:

In this early case, the plaintiff, John Richard Brady, employed innovative chemical processing techniques disclosed to employees under strict confidentiality agreements. The defendant, an ex-employee, later utilised this confidential information to develop a competing process. The dispute centred on whether the defendant's actions constituted misappropriation of the trade secret, given that the data had been acquired during the employment.

Decision:

[188]John Richard Brady v. Chemical Process Equipment P. Ltd. And Another 1987 SCC OnLine Del 236: AIR 1987 Del 372: (1987) 32 DLT 61 (SN): (1950-2000) Supp (1) PTC 263

The court held that the defendant's unauthorised use of the proprietary process amounted to misappropriation. The decision emphasised that a duty of confidentiality arises automatically when sensitive technical information is disclosed in the context of employment. The court awarded equitable relief and monetary damages to protect the plaintiff's competitive advantage, establishing a fundamental precedent for employer-employee trade secret obligations.

2. Life-cell International Pvt. Ltd. v. Vinay Katrela[189]

Facts

In Lifecell International, the plaintiff, a major technology company, alleged that Vinay Katrela, a former employee, had violated non-compete and confidentiality clauses after joining a competitor. The case involved a detailed analysis of the employment contract terms and the extent to which proprietary information had been disclosed. The dispute focused on whether the restrictions were enforceable given the employee's subsequent mobility in the market.

Decision

The Indian court ruled that while an employee's right to pursue a livelihood is fundamental, the protection of confidential information must also be upheld. The court enforced the contractual clauses, holding that Katrelas's actions breached his duty of loyalty and confidentiality. The decision underscored that even absent a specific trade secret statute, Indian courts can rely on contract law and equitable doctrines to protect proprietary information.

3. Franklin v. Giddings (1978) Q.d.r. 72[190]

Facts

In Franklin v. Giddings, the plaintiff developed the Franklin early white nectarine–a unique variety cultivated through specialised horticultural techniques. Without the plaintiff's consent, the defendant stole a bud from the plaintiff's orchard and used it to propagate his orchard. The key issue was whether the bud and the techniques used to cultivate it constituted confidential information deserving of protection.

[189] M/S. Lifecell International Pvt. Ltd. v. Vinay Katrela on 20 August, 2020
[190] FRANKLIN V. GIDDINS [1978] QD R 72

Decision

Judge Dunn ruled that although the horticulture technique per se was not secret, the specific method by which the plaintiff cultivated and mentioned the bud in his exclusive orchard was protected as confidential information. The decision emphasises that the commercial value lies not in the technique alone but in the unique implementation and surveillance practised by the plaintiff. As a result, the defendant's actions were deemed a misappropriation of trade secrets, warranting equitable relief.

4. Vancouver Malt & Sake Brewing Co. Ltd. v. Vancouver Brewing Ltd. (1934) UKPC 9[191]

Facts

This dispute arose from a contractual agreement regarding selling a brewer's licence. The appellants were undermined by their subsequent actions, which they claimed violated the restrictive covenant protecting their proprietary business methods. The case involved the interpretations of contractual limitations on competition.

Decisions

The UK Privy Council held that the restrictive covenant was unenforceable because it was contrary to public policy and overly restrictive of free trade. The Court clarified that while agreements may protect proprietary information, they must be reasonable in scope and duration. The decision underscored that restrictive covenants, to be enforceable, should not unnecessarily interfere with the general market or inhibit competition beyond what is necessary to protect the party's legitimate interests.

5. Garden Cottage Foods Ltd v. Milk Marketing Board (1983) 3 W.L.R. 143, (1984) 1 AC 130[192]

Facts

Garden Cottage Foods Ltd contended that the Milk Marketing Board had misappropriated its confidential production methods by improperly using secret business information to manufacture competing products. The dispute raised the issue

[191] Vancouver Malt and Sake Brewing Co. Ltd. v/s Vancouver Breweries, Ltd. Privy Council Appeal No. 41 of 1933 (From : Columbia)
[192] Garden Cottage Foods Ltd. v. Milk Marketing Board [1984] A.C. 130;. [1983] 3 W.L.R. 143; [1983]

of whether monetary damages or an injunction would be the appropriate remedy for the alleged misappropriation.

Decision

The House of Lords determined that an injunction was the more fitting remedy, given the irreparable harm resulting from ongoing misappropriation. The court underscored that when confidential information has significant commercial value, preventing further unauthorised use through an injunction is crucial. This decision reinforced the principle that equitable relief is often necessary in trade secret cases to avoid continuing damage that cannot be adequately remedied by monetary compensation alone.

6. Cadbury Scheppes Inc v. FBI Foods Ltd. (1999) 1 SCR 142[193]

Facts

Cadbury Scheppes Inc. alleged that FBI Foods Ltd had wrongfully utilised its proprietary recipe and production techniques for CLAMATO juice in this Canadian case. The dispute involved whether the defendant's product was substantially derived from Cadbury Scheppe's confidential formula and whether independent development was a valid defence.

Decisions

The Supreme Court of Canada held that the unauthorised use of the proprietary recipe constituted misappropriation, regardless of claims of independent creation. The court noted that protecting trade secrets does not depend solely on preventing independent invention but on ensuring that a competitor does not exploit confidential information obtained through a breach of duty; equitable remedies, including damages, were deemed appropriate to compensate for the wrongful use.

7. Faccenda Chicken Ltd. v. Flower and Others (1986) 1 All ER 617[194]

Facts

[193]Cadbury Scheppes Inc v. FBI Foods Ltd. (1999) 1 SCR 142, [1999] SCJ No 6, 1999 CanLII 705 (SCC). Docket No. 25778.
[194] Faccenda Chicken Ltd v Fowler [1987] Ch ... [1986] 1 All E.R. 617; (1986) 83 L.S.G. 288; (1986) 136 N.L.J. 71;

Faccenda Chicken Ltd. brought a suit against former employees, associates, and third parties, alleging they had misappropriated confidential information regarding poultry processing techniques. The plaintiffs contended that the breach of the implied confidentiality inherent in their employment relationships had resulted in unfair competitive advantages for the defendant.

Decision

The court ruled that the employee's actions constituted a breach of their implied duty of loyalty, holding that confidential Business information disclosed during employment must not be used to compete against the employer. The decision reaffirmed that equitable relief, including injunctions and damages, is warranted when trade secrets are misappropriated by former employees, thereby protecting the employer's commercial interest.

8. Golden Fry Foods Limited v. Austin and Others (2011) EWHC 137 (Q.B.)[195]

Facts

In Golden Fry Foods, the plaintiff alleged that former employees had used proprietary methods to produce a competing product, specifically meat juice pellets. The central issue was whether the plaintiff could sufficiently demonstrate that the defendant's confidential information represented a trade secret.

Decision

The court ruled that to sustain a claim for misappropriation of trade secrets, the plaintiff must specify the exact nature of the confidential information and prove that it possessed unique economic value. The judgment stressed that vague or overly broad claims are insufficient and that precision in the pleading is necessary to avoid speculative litigation. As a result, the case established stringent standards for identifying and protecting trade secrets in civil litigation.

9. M/S Gujarat Bottling Co. Ltd. & Ors, v. coca-cola Co & Ors. (1995) SSC (5) 545[196]

Facts

[195] Goldenfry Foods v Austin [2011] EWHC 137 (QB).
[196] Gujarat Bottling Company Limited v Coca-Cola (1995) 5 SCC 545

This case from India involved a dispute over a franchise agreement where the plaintiff argued that the restrictive covenants embedded within the contract were necessary to protect the trade secrets and goodwill associated with the Coca-Cola brand. The defendant contested the enforceability of such restrictions, asserting that they were overly broad and violated the principle of free trade.

Decision

The court ruled that restrictive covenants may be enforced if they are reasonable in scope and duration and are designed to protect legitimate business interests. In this instance, the court found that the restrictive provisions were acceptable, as they did not unduly restrict the defendant's ability to engage in trade beyond what was necessary to safeguard the proprietary information. This decision reinforced that while trade secret protection is essential, any contractual restrictions must strike a proper balance with the right to free commerce.

10. The Brahmaputra Tea Co. Ltd. v. E. Scrart (1885) ILR II Cal 545[197]

Facts

In one of the earliest Indian trade secret cases, the Brahmaputra Tea Co. Ltd. brought an action against a former employee who began working for a competitor shortly after leaving the company. The dispute centred on whether the employee's action, specifically setting up a competing tea business using confidential cultivation methods, violated the restrictive provisions in his employment contract.

Decision

The court awarded nominal damages for the breach, ruling that while restrictive covenants in employment may be enforceable, they must be reasonable in duration and geographic scope. The decision underscored that trade secret obligations in employment should not unreasonably impede an individual's right to pursue their livelihood, thereby establishing a balancing principle in post-employment restrictions.

[197] The Brahmaputra Tea Co. Ld. vs E. Scarth (1885) ILR 11CAL545.

11. Pepsi Foods Limited and Ors. v. Bharat Coca-Cola Private Holdings Limited and Others (1999) ILR 1999 Del 193[198]

Facts

In this dispute, Pepsi Foods Limited contended that several employees had violated non-competition and confidentiality clauses by joining a rival firm and misappropriating Pepsi's confidential business information. The case focused on whether the non-competition clauses were enforceable given that employees need to change jobs in a dynamic market.

Decision

The Delhi High Court held that the non-competition clause must be narrowly tailored and cannot unreasonably restrict an employee's right to secure better employment opportunities. The court refused to enforce the clause because it would amount to undue restraint on trade and employee mobility, thereby underscoring the need to balance proprietary protection with fundamental rights in a market economy.

12. Unitherm Food System v. Hormel Foods, No. 14cv4034 (JNE/BRT)(D. Minn. jul. 25, 2016)[199]

Facts

Unitherm Food System developed a proprietary method of cooking meat products and entered into a joint development agreement with Hormel Foods. After Hormel Foods withdrew from the project, Unitherm alleged that Hormel improperly used its confidential process and engineered the method to develop a competing product. The dispute focused on whether the defendant's conduct constituted misappropriation of trade secrets.

Decision

The court determined that the defendant's reverse engineering did constitute misappropriation when done in breach of an explicit confidentiality agreement. The ruling established that a party may not benefit from confidential information acquired

[198] Pepsi Foods Limited and Ors. v. Bharat Coca-Cola Private Holdings Limited and Others 1999 VAD Delhi 93, 81 (1999) DLT 122,
[199] Unitherm Food System v. Hormel Foods, No. 14cv4034 (JNE/BRT)(D. Minn. Jul. 25, 2016)

in violation of its duty and that unjust enrichment could be remedied through both monetary damages and injunctive relief.

13. Orthofix, Inc. v. Hunter, No. 153216 (6th Cir. 2015)[200]

Facts

Orthofix, Inc. accused former employee Eric Hunter of disclosing confidential information to a competitor, such as customer lists, pricing strategies, and internal sales reports. Hunter had signed a comprehensive non-disclosure agreement upon employment, allegedly covering all sensitive information. The key issue was whether the board's confidentiality clause was enforceable under Texas law.

Decision

The Sixth Circuit held that the confidentiality agreement was enforceable, noting that even without specific geographic or temporal restrictions, the agreement was reasonable as it aimed to protect critical, non-public business information. The court emphasised that "confidential information" must be construed broadly enough to encompass all sensitive business data, thereby upholding the trade secret claims.

14. Dalmatia Import Group, Inc. v. Food Match Inc., Others, No. 16cv02767, U.S Dist. Ct. E.D. Pa.[201]

Facts

Dalmatia Import Group, Inc. alleged that its former distributors misappropriated its proprietary fig jam recipe and production techniques. The defendants were accused of misrepresenting their product as identical to Dalmatias and using confidential trade secrets to capture market shares. The case also involved claims of trademark infringement and breach of contract.

Decision

The jury found the defendant guilty of trade secret misappropriation, awarding substantial damages. The court noted that deliberate and malicious misappropriation, especially when done with the intent to gain economic warrants, was a punitive measure

[200] Orthofix, Inc. v. Hunter, No. 15-3216, 2015 WL 7252996 (6th Cir. Nov. 17, 2015)
[201] DALMATIA IMPORT GROUP, INC. v. FOODMATCH, INC. et al, No. 2:2016cv02767 - Document 122 (E.D. Pa. 2016)

under the Defended Trade Secret Act. This decision highlighted the statutory framework's ability to provide robust remedies, including the possibility of triple damages in case of willful misconduct.

15. Arzo v. Commission. (1986) ECR 1965[202]

Facts

Arzo was involved in a dispute before the European Court of Justice, where defendants challenged the disclosure of sensitive business information by the European Commission during an antitrust investigation. The case raised critical issues regarding the balance between regulatory transparency and protecting confidential commercial data.

Decision

The court held that the commission must protect confidential business information from disclosure to third parties. It established that business secrets, encompassing technical know-how, market forecasts, and financial data, should be accorded special protection under EU law. The decision reaffirmed that safeguards must be in place even in regulatory contexts to prevent the unauthorised exposure of trade secrets.

16. Microsoft v. Commission, (2007) ECR II 3601[203]

Facts

Microsoft challenged a decision by the European Commission that mandated the disclosure of proprietary operating system protocols and source code details as part of an antitrust investigation. Microsoft argued that such disclosure would irreparably harm its competitive position by exposing critical trade secrets.

Decision

The court of first instance held that while regulators must enforce competition law, they must also respect the proprietary rights of companies. The decision acknowledged that trade secrets are fundamental assets that warrant robust protection and that any required disclosures must be strictly limited and accompanied by appropriate safeguards. The

[202]Arzo v. Commission. (1986) ECR 1965
[203] Microsoft Corp v Commission, 17 September 2007, [2007] ECR II-3601,

Microsoft case reinforced that confidentiality agreements and trade secret protections remain paramount even in antitrust enforcement.

17. PepsiCo, Inc. v. Redmond,[204] 54 F.3d 1266 (7th Cir. 1995)

Facts

In PepsiCo, Inc., Redmond, a former Pepsi employee, accepted a position with a direct competitor. When he left the company, PepsiCo claimed the employee had wrongfully taken confidential information, including trade secrets related to marketing strategies and operational processes. The defendant argued that his new employment resulted from independent effort; however, evidence indicated that he relied heavily on proprietary documents and internal data previously disclosed during his tenure.

Decision

The Seventh Circuit Court of Appeals held that the defendant's use of confidential information amounted to misappropriating trade secrets. The court emphasised that the non-competition clause, although not overly restrictive in all aspects, was enforceable in Soffa assets and prevented the use of trade secrets in its decision; the court balanced the difference between the right to seek employment with the necessity of protecting Pepsi's cost confidential information, ultimately avoiding an injection and monetary damages to deter future violations.

18. E.I. du Pont de Nemours & Co. v. Christopher[205]

Facts

DuPont accused the rival company of misappropriating its proprietary chemical formulations in this influential case. The dispute arose when confidential technical data, which had been disclosed only to selected employees under strict confidentiality agreements, was allegedly used by the defendant to manufacture a competing product. The evidence showed that the defendant accessed internal documents and attempted to replicate the unique process.

Decision

[204] PepsiCo ... Redmond, 54 F.3d 1262, 1266 (7th Cir. 1995). at 1267.
[205] EI. du Pont de Nemours & Co Inc. v. Christopher, 431 F.2d 1012 (5th Cir. 1970)

The court found that the defendant had indeed misappropriated Dupont's trade secrets. The ruling underscored that the duty of confidentiality persists, even after the internal dissemination of information, and that any reverse engineering conducted violating confidentiality agreements constitutes a breach. Consequently, the court awarded injunctive relief and compensatory damages, establishing an essential precedent for protecting technical trade secrets in the chemical industry.

19. DuPont v. Kolon Industries 947 F. Supp. 2d 203 (S.D.N.Y. 2013)[206]

Facts

In DuPont v. Kolon Industries, DuPont alleged that Kolon Industries misappropriated its confidential chemical process information. The case centred on evidence that Kolon had reverse-engineered DuPont trade secrets. Using methods that directly violated previously signed confidentiality agreements and subsequently using these processes to develop competing products. The plaintiff demonstrated that DuPont had taken substantial measures to protect its proprietary information.

Decision

The United States District Court for the Southern District of New York ruled in favour of DuPont. Finding that Kolon Industries had wilfully misappropriated trade secrets. The court held that reverse engineering, when done in contravention of explicit confidentiality obligations, not only constitutes misappropriation but also results in unjust enrichment, significant damages where ordered and an injunction was issued to prevent further misuse, reinforcing the need for strict enforcement of trade and secret protections in highly competitive industries.

20. Mitsubishi Chemical Corporation. V. Nippon Kayaku (Japanese jurisdiction)

Facts

Mitsubishi Chemical Corporation brought suit against Nippon Kayaku, alleging that the letter had improperly obtained and used confidential formulations and production data for industrial chemicals. The case involved evidence that sensitive documents were accessed through unauthorised channels and that the defendant had replicated key production processes initially developed by Mitsubishi.

[206] E.I. DuPont De Nemours & Company v. Kolon Industries Incorporated, No. 12-1260 (4th Cir. 2014)

Decision

A Japanese court ruled that Nippon Kayakus's action constituted the misappropriation of trade secrets. The court found that the confidential nature of the formulations and production methods was established by the demonstrable steps Mitsubishi had taken to secure the information. Consequently, the court awarded objective relief to halt further misappropriation and monetary damages as compensation for the competitive harm suffered.

21. Unilever PLC versus Procter and Gamble Co.[207]

Facts

Unilever PLC alleged that Procter and Gamble Co. had misappropriated confidential information concerning the formulation of a new cleaning product. The plaintiff contended that sensitive data such as precise ingredient ratios, production methodologies, and marketing strategies had been unlawfully transferred to Procter and Gamble during collaborative projects and then used to develop a competing product line.

Decision

The UK code found that the unauthorised use of confidential business information by Procter and Gamble constituted a clear case of trade secret misappropriation. The court granted an injunction to prevent further disclosure and misuse and awarded damages based on the estimated loss of market share and unfair competitive advantage. The decision set a precedent in determining the scope of remedies available for trade secrets, breaches in consumer goods

4.2 Synthesis of Judicial Trends

Balancing confidentiality with employee mobility

A common theme across these cases is the need to balance the protection of confidential business information with an individual's right to seek new employment. For instance, in both Lifecell International and Pepsi Foods, courts emphasised that while trade

[207] Unilever Plc v. Proctor & Gamble Co [2000] FSR 344

secrets must be protected, restrictions imposed on employees should be narrowly tailored to avoid unduly inhibiting career mobility.

Emphasis on Equitable Relief

Many decisions, such as those in Garden Cottage Food and Cadbury Schweppes, have understood the necessity of equitable relief, whether through injunctions or damages, to stop ongoing misappropriation and to deter future breaches. Courts have repeatedly stressed that the harm is often irreparable once misappreciation is established, justifying the need for preventive measures beyond monetary compensation.

Evidentiary challenge and the need for specificity

Cases like Golden Fry Foods and Orthofix illustrate the critical importance of detailed and precise pleading in trade secret litigation. Courts require plaintiffs to identify the confidential information at issue clearly and to demonstrate that reasonable measures were taken to preserve its secrecy. Vague or overly broad allegations are typically dismissed as speculative, thereby setting high standards for evidence.

Cross-Jurisdictional and Digital Consideration

Recent cases such as Dalmatia Import Group and Microsoft demonstrate the evolving challenges digital data poses and the business's global nature. These decisions highlight that while traditional trade secret principles remain relevant, courts must increasingly address issues such as digital misappropriation, cross-border enforcement, and the interface between antitrust regulations and intellectual property rights.

4.3 Emerging trends, cross-border enforcement, and digital challenges

As global commerce becomes increasingly interconnected and digital technologies evolve, the judicial landscape governing trade secret protection faces new challenges. In addition, the foundational cases discussed here focus on more contemporary issues, including cross-border enforcement, the difficulties of proving digital misappropriation, and the adjustments courts must make to reconcile traditional trade secret doctrines with emerging technological realities.

4.3.1 Digital Challenges in Trade Secret Protection

Case Analysis: Microsoft v. Commission, (2007) ECR II 3601

Facts

In Microsoft v. Commission, Microsoft challenged the European Commission's decision that mandated disclosure of proprietary operating system protocols and source code details during an antitrust investigation. Microsoft argued that such disclosure would lead to the irreversible loss of competitive advantage by exposing its confidential technological methods to competitors and the public. The case raised critical questions regarding the balance between antitrust enforcement and protecting trade secrets in the digital age.

Decisions

The court of first instance held that while regulators can demand disclosures to enforce competition law, they must also take adequate measures to protect companies' trade secrets. The court emphasised that any disclosure required by regulatory bodies should be narrowly circumscribed and accompanied by stringent confidentiality safeguards. This decision has since influenced subsequent cases involving digital data, underscoring the need for regulatory frameworks that respect competitive fairness and the sanctity of proprietary information.

Emerging Digital Misappropriation: Dalmatia Import Group, Inc. v. Food Match Inc. and Others

Facts

Dalmatia Import Group, Inc, brought an action against former distributors accused of misappropriating its confidential fig jam recipe and production process. In a digital context, the defendant allegedly obtained and reproduced sensitive information through electronic communications and online data transfer, blurring the lines between traditional misappropriation and cyber theft.

Decision

The jury favoured the Dalmatia import group, awarding substantial damages for willful misappropriation under the Defended Trade Secret Act. The case highlighted that digital misappropriation, where trade secrets are transmitted, stored, or altered electronically, requires courts to adapt traditional principles to modern technological

methods. Notably, the decision recognised that punitive measures (including potential tripling of damages) may be warranted in case of malicious digital theft.

4.3.2 Technological Development and the Internet of Things (IoT)

The proliferation of IoT devices and cloud computing platforms has expanded the avenues through which trade secrets may be compromised, with proprietary algorithms, data analytics, and interconnected systems at risk. Courts must consider whether existing doctrines adequately address confidential information's rapid cross-network dissemination. Although no single case has definitively resolved these issues, several recent rulings and policy discussions underscore the urgency for updated legal standards integrating robust cybersecurity measures with traditional trade secret protections.

Cross-Border Enforcement and Global Harmonisation: Case Analysis: Azro v. Commission, (1986) ECR 1965

Facts

In Azro v. Commission, the European Court of Justice reviewed a dispute where the European Commission disclosed sensitive commercial data during an antitrust investigation. The case revolved around whether the commission could reveal confidential business information without the data owner's consent in light of cross-border regulatory cooperation.

Decision

The court ruled that the European Commission must safeguard confidential information from undue disclosure, emphasising that business secrets, such as technical know-how, market forecasts, and financial data, deserve special protection even when examined in regulatory contexts. This decision has served as a cornerstone for subsequent efforts to harmonise cross-border enforcement standards, ensuring that multinational disputes do not erode the protective framework for trade secrets.

4.3.3 International Initiatives and Harmonisation Efforts

In addition to judicial decisions, international bodies such as the World Trade Organisation (WTO) and the World Intellectual Property Organisation (WIPO) have undertaken significant efforts to harmonise trade secret laws globally. Initiatives under

the TRIPS Agreement and ongoing dialogues in international forums aim to reduce inconsistencies between common law and civil law jurisdictions. Although challenges remain concerning enforcing trade secret rights across borders, these initiatives are critical for providing multinational enterprises with predictable legal frameworks.

Contemporary Challenges: Evidentiary Burdens and Specificity

Evidentiary Challenges in Digital and Traditional Contexts

One persistent challenge in trade secret litigation is the heavy evidentiary burden placed on plaintiffs. Courts require clear, detailed evidence that the information was hidden, possessed economic value, and was subject to reasonable protective measures. In the digital arena, where data can be rapidly copied and disseminated, establishing these elements becomes even more complex. Cases such as Golden Fry Foods and Orthofix have underscored that overly broad or vague claims often fail to meet the high standards for proving misappropriation.

4.4 Conclusion.

4.4.1 Balancing Competing Interests

Across the cases discussed, a central theme emerges: the need to balance the protection of confidential business information with other public and individual rights, such as employee mobility and regulatory transparency. Courts have repeatedly held that while trade secrets must be rigorously protected, any restrictions imposed (primarily through non-compete clauses) must not unduly stifle an individual's right to pursue gainful employment.

4.4.2. The Role of Statutory Reforms

Recent legislative initiatives, including the Defend Trade Secret Act (DTSA) in the United States and proposals under the Trade Secret Protection Act (TSPA), represent efforts to modernise trade secret law. These reforms aim to address many challenges highlighted by the judicial precedents, including digital misappropriation, cross-border enforcement and the evidentiary burdens in proving misappropriation. The expanded statutory framework would standardise legal remedies and provide more precise guidelines for protecting trade secrets in an increasingly complex global marketplace.

4.4.3. Implications for Multinational Corporations

The evolving landscape of trade secret protection poses challenges and opportunities for multinational corporations. On the one hand, a lack of uniform global standards can create uncertainty in cross-border litigation; on the other, ongoing international harmonisation efforts are promising for developing a more consistent global legal framework. Corporations must, therefore, stay informed about judicial trends and legislative reforms to adjust their compliance and risk management strategies effectively.

Chapter 5

Conclusion and Recommendations

5.1 Findings

Trade secrets are a vital component of modern intellectual property, distinct from patents and trademarks in that they derive value from confidentiality rather than public disclosure. The United States and India are signatories to international agreements (notably the TRIPS Agreement) recognising the need to protect undisclosed information, but their domestic approaches differ sharply. In the United States, trade secrets are guarded by state and federal laws. Nearly every U.S. state has adopted a version of the Uniform Trade Secrets Act, which defines a trade secret as any formula, pattern, compilation, program, device, method, technique or process that derives independent economic value from not being generally known and that is subject to reasonable measures of secrecy. In 2016, the U.S. Congress also enacted the Defend Trade Secrets Act (DTSA), creating a nationwide federal cause of action for misappropriation of trade secrets, complementing the federal Economic Espionage Act (EEA) of 1996, which criminalises the theft of trade secrets for the benefit of a foreign government or agent. Together, these laws create a robust statutory framework: an owner of trade secrets can obtain injunctive relief, recover damages for actual loss or unjust enrichment, and even (if misappropriation is wilful and malicious) seek exemplary damages and attorney's fees. Notably, the DTSA also allows for extraordinary relief, such as ex parte seizure of the stolen trade secret property under strict conditions to prevent irreparable harm.

By contrast, India has no dedicated trade secrets statute. Indian law treats trade secrets as confidential information, protected indirectly through contract law, equity, and general principles of common law. Businesses in India typically rely on contracts (non-disclosure agreements or confidentiality clauses) and fiduciary duties to guard secrets. If a breach occurs, an aggrieved party may seek an injunction or damages under breach of contract or confidence theory. Provisions of the Indian Penal Code (now revised as the Bharatiya Nyaya Sanhita) can cover outright theft of documents or property. Still, there is no specific criminal offence for corporate espionage or secret misappropriation. Similarly, while the Information Technology Act includes offences related to unauthorised access or disclosure of data, it is not tailored to commercial trade secrets.

Indian courts have applied equitable principles to protect confidential business information, but without detailed statutory guidance.

One consequence of these differing frameworks is predictability and clarity. In the U.S., the statutory definitions and remedies give courts and businesses a precise reference point. For example, U.S. law clearly distinguishes "misappropriation by improper means" (like hacking or theft of documents) from lawful acts like independent development or reverse engineering. Remedies such as seizure orders and treble damages in willful cases strengthen enforcement. Indian trade secret protection, on the other hand, is more piecemeal. The courts have occasionally granted injunctions to prevent the use of misappropriated information, but the scope of these injunctions is often uncertain. Notably, recent Indian decisions have illustrated the challenges: in a 2024 Delhi High Court case, the court issued a sweeping interim injunction against former employees. It even allowed a raid on the defendants' premises to seize evidence. While this shows a willingness to enforce confidentiality, observers have noted that the order's vague terms and broad seizure powers raised concerns about fairness and clarity. Indian judges must frequently decide whether to treat a case as a contract breach or breach of an equitable duty of confidence, and the lack of clear statutory tests can make such analysis ad hoc. As one commentator noted, courts sometimes grant ex parte relief in urgent cases, but they lack formal rules for safeguarding secrets during litigation, making them wary of extensive remedies.

Judicial trends further diverge in scale and emphasis. U.S. courts handle thousands of trade secret cases yearly, often involving cutting-edge technology and multinational enterprises. High-profile American litigation (for example, in Silicon Valley or the pharmaceutical sector) has underscored the value placed on protecting proprietary R&D. Jury verdicts can be massive; in one well-known case, a jury awarded hundreds of millions of dollars in damages for willful trade secret theft, reinforcing the perception that U.S. enforcement is vigorous. Over the past two decades, the trend in the U.S. has been toward even stronger protection: the adoption of the DTSA and aggressive enforcement by federal agencies, including specialised Economic Espionage task forces, reflects a policy priority to deter corporate espionage. This American model is underpinned by legal infrastructure (federal jurisdiction, uniform procedure, discovery rules) that supports sophisticated litigation. By comparison, trade secret litigation in India remains relatively scarce and fragmented. Many disputes are resolved quietly or

through arbitration, since the public courts are perceived as slow and unpredictable. The reported Indian case law on trade secrets has grown only gradually, and most judgments reiterate general principles (such as the need for reasonable secrecy measures) without developing a deep jurisprudence. Some cases have upheld injunctive relief against ex-employees or competitors who misused confidential information, but these decisions rarely establish detailed analytical frameworks. There has also been historical hesitation: Indian courts have sometimes declined to order disclosure of sensitive information even to the court itself (to preserve confidentiality), which can lead to a reluctance to adjudicate the dispute vigorously. In short, while U.S. judges routinely apply statutory trade secret tests, Indian judges must fit each case into broader notions of equity, creating uncertainty for businesses.

Institutionally, the United States has built parallel support mechanisms for trade secret protection. Federal and state law enforcement can pursue criminal cases under the Economic Espionage Act and related statutes, and the Department of Justice maintains specialised units for IP enforcement. Given the high stakes of corporate secrets, there is also a substantial ecosystem of private enforcement, law firms, forensic experts, and technology measures. The U.S. Congress has even seen bipartisan support for initiatives like "National Trade Secret Protection Task Forces" to coordinate efforts. India, in contrast, has no dedicated enforcement agency or police division for trade secrets. General investigation of commercial crimes may proceed under standard criminal provisions, but law enforcement agencies are not specifically trained or mandated to address secret misappropriation. Moreover, Indian courts have limited means to compel the production of secret evidence; unlike U.S. courts, they do not have a codified ex parte seizure procedure. On the legislative front, recent developments are promising but nascent. The Indian government has recognised the gap: a 2024 report by the Law Commission proposed a model Trade Secrets Bill defining trade secrets consistent with international norms and setting out civil remedies (injunctions, damages, destruction of materials) and protective court procedures (confidential trials, similar to U.S. protective orders). However, this remains a draft and is yet to be enacted. In the meantime, the lack of a formal law means that Indian businesses must navigate a patchwork of remedies, from clauses in employment contracts to invoking general unfair competition law, to try to deter leakage of confidential know-how.

These contrasts can be summarised in terms of strengths and weaknesses. The U.S. system's strengths include clear statutory language, heavy-duty remedies, and broad scope: it explicitly covers misappropriation by third parties and provides for civil and criminal penalties. Its weaknesses may lie in complexity and cost; the legal process can be expensive and protracted, and there are concerns that overly aggressive litigation might chill competition or lock up useful information (for example, by discouraging employee movement or competing product development). The Indian approach, by contrast, has the advantage of flexibility; existing laws can be applied on a case-by-case basis without creating an overly rigid scheme. Still, this flexibility comes at the expense of certainty. Key weaknesses in India's framework include the absence of dedicated criminal penalties for trade secret theft, no formal protection of secrecy during legal proceedings, and narrower definitions (often requiring a contractual relationship for liability). International studies have noted that these omissions, which India has historically shared with other developing economies, correlate with weaker innovation outcomes. The United States offers a comprehensive, uniform trade secret regime with proven enforcement mechanisms. In contrast, India currently provides only fragmented and variable protection, leaving substantial room for improvement to reach global standards.

5.2 Recommendations

A multi-pronged strategy of legal reform, procedural innovation, and policy measures is warranted to bolster India's trade secret protection. First and foremost, India should enact a dedicated Trade Secrets Act. Such legislation would consolidate existing principles and clarify rights and remedies. The law should adopt a "trade secret" definition aligned with international best practice (for example, the three-part test of secrecy, commercial value, and reasonable safeguarding found in TRIPS Article 39 and mirrored in other countries' laws). It should explicitly exclude general skills or knowledge acquired by employees from protection to balance protection with legitimate competition. The act should enumerate specific wrongful acts constituting misappropriation (including unauthorised acquisition by hacking or theft, breach of confidentiality agreements, or disclosure knowing the information was misappropriated) while also listing exceptions (reverse engineering, independent creation, whistleblowing in the public interest, etc.) to prevent abuse of the law.

The proposed law must also provide robust remedies. India should follow global best practices by authorising injunctions to prevent the use of stolen secrets, damages or account of profits to compensate the rightful owner, and, in egregious cases, punitive awards. The draft Trade Secrets Bill in India would allow destruction or return of infringing materials, recall of products, and costs; these features should be retained. Critically, the law should permit extraordinary relief when ordinary orders would fail. In particular, India could introduce a civil seizure mechanism for trade secrets similar to the U.S. ex parte seizure, albeit with stringent safeguards: a court could be empowered to authorise seizure of specific property containing the secret upon a strong showing of irreparable harm. This would require safeguards such as notice to the defendant after seizure, a judicial finding of likely success, and a prompt hearing to minimise unjust harm. Introducing such a procedure (perhaps as an extraordinary high-court power or through revision of existing civil procedure rules) would significantly strengthen immediate enforcement.

Confidentiality in court must also be protected. The new legislation should explicitly direct judges to conduct proceedings (or parts thereof) in camera and to seal sensitive documents, preventing trade secrets from entering the public record. Guidelines for courts to issue protective orders (limiting disclosure to parties' counsel, etc.) would reduce the risk that litigation exposes confidential information. This procedural aspect, well-developed in U.S. practice, is especially crucial for business confidence.

On the criminal side, India should consider creating specific offences for trade secret theft. The Bharatiya Nyaya Sanhita could be amended to include provisions mirroring the U.S. Economic Espionage Act: criminalising the unauthorised appropriation of trade secrets for the benefit of a foreign government or agent, with substantial penalties. Even making trade secret theft a standalone offence (with imprisonment and fines) would provide deterrence. Law enforcement agencies (police, cybercrime units) should be trained to recognise and investigate corporate espionage cases, and to coordinate with other countries under mutual legal assistance treaties. This aligns with international norms and would fulfil TRIPS obligations to protect against unfair competition.

Legislative reform should go hand in hand with judicial and administrative measures. India's commercial courts or intellectual property tribunals could be designated to

handle trade secret cases, ensuring that judges with technical appreciation hear them. Courts should issue practice directions to expedite such cases given their urgency. The Bar and judicial academies should provide training on trade secret issues to lawyers and judges, covering topics like the burden of proof, the nature of confidential information, and protective orders. Aligning procedural law (for example, the civil procedure code) to facilitate swift injunctive hearings, perhaps through provisions on interim relief in commercial disputes, would also help.

The government should emphasise trade secret protection in its intellectual property strategy. The National Intellectual Property Rights (IPR) Policy or Innovation Policy could explicitly recognise trade secrets as a component of the IP system. Public awareness campaigns and guidelines could encourage companies to adopt internal safeguards: for example, best practice manuals might recommend formal classification of sensitive information, regular audits of security measures, mandatory NDAs for employees, digital security (encryption, access controls), and employee training. Government contracts and licenses could incorporate trade secret clauses to ensure the confidentiality of technical data and know-how shared with state agencies.

Internationally, India can look to bilateral and multilateral cooperation. India and the U.S., under forums like the Trade Policy Forum, have already identified trade secret protection as an issue. India should participate in global initiatives on trade secrets (such as WIPO working groups) and consider model provisions from other jurisdictions. For instance, the U.S. has encouraged uniform definition across states (the Uniform Trade Secrets Act), and the EU has a Trade Secrets Directive ensuring minimum standards; India's law should be compatible with these trends to facilitate cross-border enforcement. Measures like requiring disclosure of misappropriations in regulatory filings or border controls on goods made with misappropriated secrets (much as trademark counterfeiting is blocked) could be explored.

Finally, specific procedural reforms can help with evidence handling. For example, courts might assume that information claimed as a trade secret, if shown reasonable protections, is entitled to confidentiality until the contrary is proven. Contract law could be clarified: any NDA or confidentiality clause in an employment contract should be valid and enforceable unless it violates mandatory labour norms. Competitive secrecy could also be supported by fair competition law: for instance, showing unauthorised use

of another's trade secret could be treated as an unfair trade practice. These legislative, procedural and policy steps, which draw on the U.S. model or other global practices, would create a more effective trade secret framework in India.

5.3 Conclusion

This comparative analysis underscores that adequate trade secret protection is a linchpin of a modern innovation ecosystem. The United States demonstrates how a clear, comprehensive legal framework, encompassing statutory definitions, potent remedies, and active enforcement, can secure business confidence and encourage investment in research and development. India, by contrast, currently relies on a fragmented mix of contract law and equity, which has proven insufficient to safeguard valuable know-how in an increasingly competitive global economy. The chapter's findings suggest that the gaps in India's system are substantial: without explicit legal measures, companies and innovators lack certainty that their secrets will remain theirs. Strengthening India's trade secret regime would align it with international standards and benefit its legal and innovation environment directly.

Adopting legislative reforms and procedural safeguards for India's legal system will lead to greater predictability and efficiency in litigation. Businesses will be better able to structure contracts and protect their information if the law clearly defines obligations and consequences. Specialised training and forums for trade secret disputes will create a cadre of expertise, reducing the burden on generalist courts and leading to more consistent outcomes. Crucially, enhanced protection will foster an atmosphere where entrepreneurship and innovation are rewarded: companies can invest in proprietary development without fear of facile copying.

From the perspective of the Indian economy and innovation ecosystem, robust trade secret protection has important implications. In high-technology and knowledge-intensive industries, from software to biotechnology to manufacturing, intangible know-how is often a firm's most valuable asset. If such assets are insecure, firms may be reluctant to innovate or choose to rely only on patents (which require disclosure and may not be desirable for every invention). Conversely, effective secrecy laws complement the patent system by allowing businesses to protect process improvements and business methods without registration. For foreign investors and partners, clear

trade secret laws assure that their proprietary technologies will be respected, making India a more attractive investment destination.

In sum, the comparative evidence and analysis emphasise the need for reform. India stands where drafting and enacting a trade secrets law could yield substantial dividends: legally, by filling critical gaps and streamlining enforcement; economically, by encouraging research and securing competitive advantage; and academically, by aligning India's IP jurisprudence with global norms. As the draft law proposals indicate, the path forward is already sketched out, but the realisation of these changes will be key. By heeding global best practices, such as those exemplified by the U.S. framework, and tailoring them to its context, India can strengthen its intellectual property regime and thereby underpin its long-term innovation-led growth. Ultimately, a resilient trade secret framework will ensure that India's legal and commercial environments jointly foster creativity and economic progress while maintaining fair competition and the rule of law.

BIBLIOGRAPHY

I Books and Book Chapters

1. Kevin E. Maskus & Jerome H. Reichman, *International Public Goods and Transfer of Technology Under a Global Intellectual Property Regime* (Oxford Univ. Press 2004).
2. L. Merges, *Big Data and Trade Secret Challenges*, in *Intellectual Property and Data Protection* (Wiley 2020).
3. Robert Abbott, *The Paris Convention and Its Legacy in Modern Intellectual Property Law* (Univ. Press 2001).
4. S. Maskus, *Intellectual Property Rights in the Global Economy* (Cambridge Univ. Press 2000).
5. S.K. Verma, *Protection of Trade Secrets and Confidential Information*, in Law Relating to Intellectual Property Rights 365 (M. K. Bhandari ed., 2002).
6. William H. Manz, *Defend Trade Secrets Act of 2016: A Legislative History of Public Law No. 114-153* (William S. Hein & Co., Inc., 2017).

II. Statutes and International Instruments (Alphabetically Ordered)

7. Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39.2, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.
8. Computer Fraud and Abuse Act, 18 U.S.C. § 1030.
9. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified at 18 U.S.C. §§ 1836–1839).
10. Directive 2016/943 of the European Parliament and of the Council, 2016 O.J. (L 157) 1.
11. Draft Trade Secrets Bill, Ministry of Commerce & Industry, India (2024).
12. Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831–1839).
13. Indian Contract Act, No. 9 of 1872, INDIA CODE (1872).

14. Information Technology Act, No. 21 of 2000, INDIA CODE (2000), §§ 43A, 72.

15. Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, 828 U.N.T.S. 305.

16. Uniform Trade Secrets Act, Unif. L. Comm'n (1979), as amended (1985).

III. Journal Articles and Reports

17. Alan John Abraham, *Trade Secrets and Its Potential in an Information-Based Economy*, 4 INDIAN J.L. & LEGAL RSCH. 1 (2022).

18. Ayesha Tareen & Manisha Pilli, *Comparative Analysis of Competition Law and Intellectual Property Rights: Interplay with Special Reference to India and the USA*, 4 Indian J.L. & Legal Rsch. 1 (2022).

19. Brandon Kinnard, *Keep It Secret; Keep It Safe: A Practitioner's Guide to BRIC Trade Secret Regimes*, 3 Am. U. Bus. L. Rev. 503 (2014).

20. Chirantan Priyadarshan, *Open Secrets of Trade in India: An Analytical Study of Trade Secrets in the Uncodified Legislative Regime in India*, 5 Indian J.L. & Legal Rs. 1 (2023).

21. David S. Levine & Christopher B. Seaman, *The DTSA at One*, 1 Bus. Entrepreneurship & Tax L. Rev. 369 (2018).

22. Faizanur Rahman, *Trade Secrets Law and Innovation Policy in India*, 3 Indian J.L. & Pub. Pol'y 119 (2016).

23. Ranjeet Kumar et al., *Trade Secrets Protection in Digital Environment: A Global Perspective*, Int'l J. Econ. & Mgmt. Sci. 2(4) (2012).

24. S. Sen, *Artificial Intelligence and the Future of Trade Secret Protection*, 29 Indian Bus. L.J. 75 (2022).

25. Shruti Nandwana, *Comparative Analysis of Regulatory Framework Governing Trade Secrets in United States, United Kingdom and India*, 1 DNLU L. Rev. 112 (2022).

26. Spencer Simon, *The Economic Espionage Act of 1996*, 13 Berkeley Tech. L.J. 305 (1998).

27. Swarnima Singh, *Examining the Regulation of Trade Secrets in India and the United States of America: A Comparative Analysis*, 7 Int'l J.L. Mgmt. & Human. 4424 (2024).

28. V. Adharsh, *The Disregarded Facet of IPR: A Study of Trade Secrets and the Indian Context*, 3 Int'l J.L. Mgmt. & Human. 1969 (2020).

29. Sakshi Pawar & Smrithi Bhaskar, *Obligations under Article 39.3 of TRIPs: The Data Exclusivity v. Data Protection Debate in the Indian Context*, 3 J. INTELL. PROT. STUD. 111 (Jan. 2019).

30. *Protecting Trade Secrets in India: Challenges and Opportunities*, Lexology, https://www.lexology.com/library/detail.aspx?g=c83e8a6c-a02e-44ba-8723-94087d2e5e20 (last visited Mar. 3, 2025).

31. *Trade Secrets in India: Understanding the Legal Landscape*, AZB & Partners, https://www.azbpartners.com/bank/trade-secrets-india/ (last visited Mar. 3, 2025).

32. *Understanding the Challenges in Enforcing Trade Secret Laws*, Laws Learned (June 29, 2024), https://lawslearned.com/challenges-in-enforcing-trade-secret-laws/.

33. Karen A. Magri, *International Aspects of Trade Secret Law*, https://www.myersbigel.com/library/articles/InternationalAspectsofTradeSecret.pdf (last visited Feb. 9, 2025).

34. OECD, *Global Trade Secret Protection Index* (2020).

35. T. Yeh Brain, *Protection of Trade Secrets: Overview of Current Law and Legislation*, Cong. Rsch. Serv. R43714 (2014), https://fas.org/sgp/crs/secrecy/R43714.pdf.

36. The 2017 Kroll Global Fraud Report, https://www.kroll.com/en/insights/publications/fraud/global-fraud-report-2017 (last visited Mar. 10, 2025).