TECHNOLOGY TRANSFER VS. TRADE SECRETS: IS INDIA'S LEGAL FRAMEWORK ADEQUATE FOR FOREIGN COLLABORATIONS?

Isha Manchanda, CB&IL, Amity Law School, Amity University, Noida[1]

ABSTRACT

Technology transfer is a central feature of foreign collaboration, particularly where investment depends upon access to patents, proprietary know-how, manufacturing methods, software, technical data and business processes. Yet foreign technology suppliers frequently treat valuable know-how as trade secrets because secrecy can provide protection beyond the fixed term and disclosure requirements associated with patents. India has a mature patent regime and a substantial contractual framework for technology licensing, but it does not presently have a dedicated comprehensive trade-secret statute. This paper examines whether that combination is adequate for foreign collaborations. It argues that India's framework provides meaningful protection through contract, breach-of-confidence principles, intellectual property statutes, information-technology law and competition law, but remains fragmented when compared with the predictable remedial structure expected in sophisticated cross-border transactions. The paper analyses the Patents Act, 1970, Indian Contract Act, 1872, Competition Act, 2002, Information Technology Act, 2000, National IPR Policy, foreign-exchange rules and international obligations under TRIPS. It compares India with the United States, European Union and Singapore and proposes a targeted statutory framework that protects confidential know-how without allowing technology owners to use secrecy clauses to frustrate competition, employee mobility or legitimate technology diffusion.

Keywords: Technology Transfer; Trade Secrets; Foreign Collaboration; Intellectual Property; Know-How; India.

[1] CB&IL, Amity law School, Amity University, Noida

1. Research Problem

Foreign collaborations are often structured around a transfer of technological capability rather than a simple sale of goods. A foreign enterprise may contribute patents, technical drawings, manufacturing processes, source code, formulas, testing protocols, quality-control systems, confidential commercial information or specialised know-how to an Indian partner. The legal value of the collaboration therefore depends on two connected questions: whether the transferred technology can be used effectively in India, and whether the confidential elements of that technology will remain protected against unauthorised acquisition, use or disclosure. The first concern favours dissemination; the second favours secrecy. India has strong statutory protection for patents and several related forms of intellectual property, but trade secrets occupy a different legal position. There is no single comprehensive Indian statute dedicated to trade secrets. Protection is instead assembled from contract law, equitable principles concerning confidence, the Information Technology Act, 2000, intellectual property legislation and, in appropriate circumstances, competition law and criminal law. This fragmented structure can be adequate for ordinary domestic relationships but can create uncertainty in high-value international collaborations where parties expect clear definitions, predictable remedies, urgent injunctions and enforceable post-termination obligations.

The research problem is therefore not whether India protects confidential technology at all. It does. The harder question is whether its dispersed protections provide sufficient certainty for foreign technology suppliers while preserving the public interest in competition, employee mobility, innovation and access to technology. A legal framework that overprotects secrecy can lock Indian partners into restrictive arrangements; a framework that underprotects know-how can discourage foreign enterprises from transferring their most valuable technology. The appropriate standard is consequently calibrated protection rather than maximal protection.

2. Research Questions

- How does Indian law regulate technology transfer in foreign collaborations?
- To what extent do Indian laws protect trade secrets and confidential know-how?
- Does the absence of a dedicated trade-secret statute create material uncertainty for cross-border technology agreements?

- How should Indian law balance confidentiality with competition, employee mobility, innovation and technology diffusion?
- What reforms can improve legal certainty without creating excessive restrictions on access to technology?

3. Objectives

- To examine the legal framework governing technology transfer and confidential know-how in India.
- To evaluate contractual and non-contractual protection available to trade secrets.
- To analyse the interaction between intellectual property, contract, competition and foreign-exchange regulation.
- To compare India's approach with selected foreign jurisdictions.
- To propose reforms for more predictable and balanced foreign technology collaborations.

4. Hypothesis

The study hypothesises that India's existing framework is functionally capable of protecting trade secrets in many foreign collaborations, but its fragmented character reduces legal certainty and increases transaction costs. A dedicated but narrowly tailored trade-secret law would improve predictability if it preserved safeguards against overbroad secrecy claims, anti-competitive restrictions and unreasonable restraints on employees. The absence of a statute is therefore a significant institutional gap, but legislation should complement rather than displace contractual drafting and existing intellectual-property remedies.

5. Literature Review

Indian scholarship has identified the absence of a dedicated trade-secret statute as a recurring weakness. The existing approach relies heavily on contracts and the common-law action for breach of confidence. The National IPR Policy 2016 itself recognised the need to study protection of trade secrets and issues concerning technology transfer and know-how, indicating

that the policy framework has long acknowledged the subject as requiring further development (DPIIT, 2016). The Law Commission's 2024 Report on Trade Secrets and Economic Espionage subsequently recommended sui generis legislation, reinforcing the argument that the present framework may be insufficiently systematic.[2]

A second body of literature stresses that stronger IP protection does not automatically produce greater technology transfer. Excessive exclusivity can increase licensing costs and permit licensors to impose restrictive conditions. The Patents Act reflects this policy tension by recognising that patent protection should contribute to technological innovation and transfer and dissemination of technology, while preventing abuse and unreasonable restraints on trade (Patents Act, 1970, § 83). The literature therefore supports an approach in which protection and diffusion are treated as complementary objectives rather than opposing absolutes.[3]

6. Legal Framework

6.1 Technology Transfer and Intellectual Property

Technology transfer may involve assignment, licensing, franchising, joint ventures, technical-services agreements, research collaborations or combinations of these arrangements. Indian law does not create a single general technology-transfer contract. Instead, the legal character of each transaction depends upon the rights being transferred and the regulatory consequences of the arrangement. A patent licence may concern an exclusive or non-exclusive right to exploit a patented invention. A know-how agreement may transfer technical information without creating a registered intellectual-property right. A collaboration can combine patents, confidential information, trademarks, technical assistance and continuing services.[4]

The Patents Act, 1970 provides the core statutory framework for patents. Patent rights are territorial and time-limited, and patent disclosure is part of the bargain through which the legal monopoly is granted. Section 83 states policy principles concerning working of patents, technological innovation, transfer and dissemination of technology, public interest and prevention of unreasonable restraints on trade. This is significant for technology-transfer

[2] Department for Promotion of Industry and Internal Trade [DPIIT], 2016; Law Commission of India, 2024
[3] Patents Act, 1970, § 83; Agreement on Trade-Related Aspects of Intellectual Property Rights [TRIPS Agreement], art. 39; Law Commission of India, 2024
[4] Patents Act, 1970, §§ 68–69; Trade Marks Act, 1999, §§ 48–49; Copyright Act, 1957, §§ 18–19, 30; Indian Contract Act, 1872

analysis because Indian patent law is not conceptually indifferent to the social consequences of exclusivity.[5]

6.2 Contractual Protection of Trade Secrets

Because trade secrets are not registered rights, contractual protection is central to foreign collaborations. Parties commonly define confidential information, establish permitted uses, restrict disclosure, identify authorised personnel, impose security requirements, regulate subcontractors and establish return or destruction obligations after termination. Indian Contract Act principles permit parties to create binding obligations, subject to statutory limitations and public policy. A carefully drafted confidentiality clause can therefore provide a practical first line of protection.[6]

The weakness is that contract binds parties and legally connected persons, while misappropriation can involve third parties, former employees, consultants or downstream recipients. An international collaborator may consequently prefer a statutory cause of action capable of addressing acquisition or use of confidential information even where no direct contract exists. This is one reason why a dedicated statute can provide value beyond the mere existence of non-disclosure agreements.[7]

6.3 Breach of Confidence

Indian courts have developed protection for confidential information through equitable principles of breach of confidence. The claimant generally must establish that the information possessed the necessary quality of confidence, was communicated in circumstances importing an obligation of confidence and was subject to unauthorised use or disclosure causing or threatening harm. This doctrine is flexible because it is not restricted to information falling within a registered IP category. Its flexibility, however, can also produce uncertainty about the precise scope of protection and available remedies.[8]

The absence of a codified statutory definition means that parties often attempt to resolve

[5] Patents Act, 1970, §§ 48, 53, 83; DPIIT, 2016
[6] Indian Contract Act, 1872, §§ 10, 23; *American Express Bank Ltd. v. Priya Puri*, 2006; Law Commission of India, 2024
[7] Law Commission of India, 2024; *John Richard Brady v. Chemical Process Equipments Pvt. Ltd.*, 1987
[8] *John Richard Brady v. Chemical Process Equipments Pvt. Ltd., 1987; American Express Bank Ltd. v. Priya Puri, 2006*; Law Commission of India, 2024

uncertainty through contract. In cross-border agreements this increases drafting importance. The agreement should distinguish genuine confidential information from publicly available material, independently developed knowledge and general skill and experience. Without such distinctions, an overbroad clause may become difficult to enforce and may improperly restrict the Indian collaborator after the relationship ends.[9]

6.4 Information Technology Act, 2000

The Information Technology Act contains provisions relevant to unauthorised disclosure of information in specified circumstances, including section 72A concerning disclosure of information in breach of lawful contract. Its significance is greater where technology transfer involves digital records, databases, software or electronically stored know-how. However, it should not be treated as a complete trade-secret regime because its statutory elements and scope are narrower than a general cause of action for trade-secret misappropriation.[10]

6.5 Competition Act, 2002

Technology licensing can create competition concerns where contractual restrictions go beyond what is reasonably necessary to protect legitimate intellectual-property interests. The Competition Act prohibits anti-competitive agreements and abuse of dominant position, while the statutory framework recognises that intellectual-property rights may justify reasonable conditions. The Competition Commission of India therefore provides an additional control against licensing practices that substantially harm competition. This is important because trade-secret legislation should not become a mechanism for immunising restrictive licensing terms from competition scrutiny.[11]

6.6 Foreign Exchange and Foreign Collaboration

Cross-border technology arrangements can also involve royalty, technical fees, equity participation and remittances. Foreign-exchange regulation and the foreign direct investment framework determine the conditions under which financial aspects of collaboration may operate. Government guidance has historically addressed foreign technology agreements

[9] Indian Contract Act, 1872, §§ 10, 23; *American Express Bank Ltd. v. Priya Puri*, 2006; Law Commission of India, 2024
[10] Information Technology Act, 2000, §§ 43, 66, 72, 72A; Law Commission of India, 2024
[11] Competition Act, 2002, §§ 3–4, 3(5); Competition Commission of India [CCI], 2026

through approval mechanisms and limits applicable to certain forms of technical collaboration. Contemporary liberalisation means that many transactions can proceed through the automatic route, but sectoral restrictions and other applicable rules continue to matter. Legal due diligence must therefore treat the technology agreement as part of a wider investment structure rather than an isolated IP contract.[12]

7. Trade Secrets in Foreign Collaborations

7.1 What Qualifies as a Trade Secret?

A trade secret is ordinarily understood as information that is commercially valuable because it is not generally known or readily accessible, and that the holder takes reasonable steps to keep secret. Technical know-how may include manufacturing tolerances, source code, experimental results, formulations, engineering methods or production parameters. Commercial secrets may include pricing strategies, customer information, supplier arrangements and market plans. The central feature is secrecy combined with economic value and reasonable efforts at confidentiality.[13]

The distinction from patents is fundamental. Patent protection requires disclosure and generally lasts for a fixed statutory period. A trade secret does not require registration and can potentially remain protected for as long as secrecy is maintained. But secrecy protection is inherently fragile: once information becomes public through lawful disclosure, reverse engineering or independent development, the basis for protection may disappear. Foreign collaborators must therefore determine which elements should be patented and which should remain confidential.[14]

7.2 Contract Design and Risk Allocation

A sophisticated technology-transfer agreement should establish a hierarchy of information. Background technology owned before collaboration should be separated from foreground technology generated jointly or independently during the project. The agreement should specify ownership, licensing rights, territorial scope, permitted users, cybersecurity controls,

[12] Foreign Exchange Management Act, 1999; Foreign Exchange Management (Non-Debt Instruments) Rules, 2019; DPIIT, 2016

[13] TRIPS Agreement, art. 39(2); Defend Trade Secrets Act of 2016, 18 U.S.C. § 1839(3); Directive (EU) 2016/943, art. 2(1)

[14] Patents Act, 1970, §§ 48, 53; TRIPS Agreement, art. 39; Directive (EU) 2016/943, arts. 2–4

audit rights, subcontractor obligations and post-termination duties. It should also establish procedures for responding to suspected leakage and preserving evidence.[15]

The agreement should avoid treating every piece of information exchanged during collaboration as a permanent trade secret. Excessive definitions can generate disputes and impede ordinary business operations. A more defensible model identifies categories and requires reasonable security measures. The parties should also define exceptions for information already known, independently developed, lawfully obtained from a third party or required to be disclosed by law. These exceptions protect the legitimacy of the confidentiality regime.[16]

7.3 Employee Mobility

Employee mobility presents a difficult boundary. Employees inevitably carry general knowledge, skills and experience from one workplace to another. A trade-secret regime should prevent misuse of protected information without converting ordinary professional competence into the employer's proprietary asset. Indian contract law also places limits on restraints of trade, particularly through section 27 of the Indian Contract Act. Foreign collaborators should therefore rely on confidentiality, access controls and narrowly framed obligations rather than blanket post-employment prohibitions.[17]

7.4 Reverse Engineering and Independent Development

A modern statutory regime must distinguish unlawful acquisition from lawful discovery. Reverse engineering may, depending on circumstances and contractual terms, reveal technology without involving theft or breach of confidence. Similarly, independent development should not be treated as misappropriation merely because the resulting product resembles protected technology. Clear rules on these issues are necessary to prevent trade-secret protection from becoming a substitute for patent protection or a perpetual monopoly over technical ideas.[18]

[15] Indian Contract Act, 1872; Patents Act, 1970; Directive (EU) 2016/943, arts. 2–5; Law Commission of India, 2024
[16] Indian Contract Act, 1872, §§ 23, 27; TRIPS Agreement, art. 39; Directive (EU) 2016/943, arts. 2–5
[17] Indian Contract Act, 1872, § 27; *American Express Bank Ltd. v. Priya Puri*, 2006; Law Commission of India, 2024
[18] Defend Trade Secrets Act of 2016, 18 U.S.C. § 1839(6); Directive (EU) 2016/943, arts. 3–4; Law Commission of India, 2024

8. Technology Transfer and Access

Technology transfer serves a developmental function when foreign know-how strengthens domestic production capabilities, research capacity and local innovation. Yet a collaboration may transfer only limited operational knowledge while retaining strategic control over key components abroad. Indian partners can therefore face dependence if the agreement prevents independent adaptation or requires continuing purchases from the foreign supplier. Contractual restrictions should be evaluated against commercial necessity, competition law and the broader policy objective of technology diffusion.[19]

The National IPR Policy links technology transfer, know-how and licensing to India's innovation objectives and specifically identifies trade-secret protection as an area for policy development. The policy also recognises the importance of technology transfer in areas such as clean technology. This demonstrates that the policy objective is not simply stronger exclusion; it is an IP ecosystem capable of supporting innovation and dissemination.[20]

9. Comparative Analysis

9.1 United States

The United States provides a useful comparison because trade secrets are protected through a dedicated federal statute, the Defend Trade Secrets Act of 2016, alongside state law. The federal framework defines trade secrets and misappropriation and provides civil remedies, including injunctions and damages, subject to statutory conditions. It also contains exceptional procedures for seizure in narrowly defined circumstances. The American model illustrates the advantages of statutory clarity, especially for cross-border commercial disputes.[21]

For India, the lesson is not that every American remedy should be transplanted. Strong emergency remedies can be valuable where digital information can be copied instantly, but safeguards are necessary to prevent misuse. Indian legislation could provide clear civil remedies and evidentiary rules while preserving judicial discretion and proportionality.[22]

[19] Patents Act, 1970, § 83; DPIIT, 2016; TRIPS Agreement, art. 7
[20] DPIIT, 2016; Patents Act, 1970, § 83
[21] Defend Trade Secrets Act of 2016, 18 U.S.C. §§ 1836, 1839; Uniform Trade Secrets Act, §§ 1–4
[22] Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836(b); Law Commission of India, 2024

9.2 European Union

The European Union's Trade Secrets Directive harmonises protection against unlawful acquisition, use and disclosure of undisclosed know-how and business information. It also incorporates safeguards for lawful activities such as independent discovery and certain public-interest disclosures. The EU model is valuable because it attempts to reconcile strong commercial protection with legitimate exceptions. India could similarly define both the protected interest and the boundaries of protection rather than leaving the entire field to judicial development.[23]

9.3 Singapore

Singapore protects confidential information primarily through common law and contractual principles rather than a single comprehensive trade-secret statute. This makes it an especially relevant comparator for India because it demonstrates that a sophisticated technology economy can operate without a dedicated statute. [24]The comparison also shows, however, that legal certainty can arise from a mature body of commercial jurisprudence, strong contractual practice and predictable judicial remedies. India's concern is not simply the existence of a statute but the accessibility and consistency of remedies.[25]

9.4 TRIPS and International Standards

Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights requires protection of undisclosed information where specified conditions are satisfied. The obligation establishes an international minimum standard but leaves considerable discretion to members regarding legal form and enforcement.[26] India can therefore adopt a statutory trade-secret framework without being required to reproduce any single foreign model. The domestic challenge is to translate the international standard into procedures suitable for Indian courts and commercial realities.[27]

10. Contemporary Case Studies and Judicial Approach

10.1 American Express Bank Ltd. v. Priya Puri

The Delhi High Court's decision in American Express Bank Ltd. v. Priya Puri is frequently

[23] Directive (EU) 2016/943, arts. 2–5, 9–16
[24] Intellectual Property Office of Singapore [IPOS], n.d.; Law Commission of India, 2024
[25] IPOS, n.d.; Law Commission of India, 2024
[26] TRIPS Agreement, art. 39
[27] TRIPS Agreement, art. 39; Law Commission of India, 2024

discussed in Indian trade-secret jurisprudence. The dispute concerned confidential information and employee mobility. The Court's reasoning illustrates the importance of distinguishing genuinely confidential business information from general skill and knowledge acquired by an employee. The case remains useful because it demonstrates how Indian courts can protect confidential information without treating ordinary employment knowledge as proprietary.[28]

10.2 John Richard Brady v. Chemical Process Equipments

In John Richard Brady v. Chemical Process Equipments, the Delhi High Court considered confidentiality and know-how in a commercial context. The decision is significant for recognising the importance of protecting technical information communicated under circumstances of confidence. Its broader relevance to foreign collaboration lies in the proposition that equitable relief can protect valuable know-how even where the information does not fit neatly into a registered intellectual-property category.[29]

10.3 Indian Approach to Interim Protection

Trade-secret disputes can become practically irreversible because confidential information loses value once widely disclosed. Indian courts therefore use interim injunctions and other equitable remedies where the legal requirements are satisfied. The effectiveness of this approach depends on speed, evidence and precise identification of the information said to be confidential. A statutory regime should strengthen, not replace, this judicial capacity by providing clearer criteria for urgent relief and preservation of confidential evidence.[30]

11. Regulatory Gaps

11.1 Absence of a Dedicated Trade-Secret Statute

The most visible gap is the absence of a single statute defining trade secrets, misappropriation, available remedies, limitation rules and procedural safeguards. This fragmentation does not mean that confidential information is unprotected. It means that parties must construct protection from several legal sources. For foreign investors accustomed to statutory trade-secret regimes, that can increase uncertainty during negotiation and litigation. The Law

[28] *American Express Bank Ltd. v. Priya Puri*, 2006; Indian Contract Act, 1872, § 27
[29] *John Richard Brady v. Chemical Process Equipments Pvt. Ltd., 1987*; Law Commission of India, 2024
[30] John Richard Brady v. Chemical Process Equipments Pvt. Ltd.*, 1987; Code of Civil Procedure, 1908, Order XXXIX, rules 1–2; Specific Relief Act, 1963

Commission's 2024 recommendation for sui generis legislation is therefore a significant development in the reform debate.[31]

11.2 Fragmented Remedies

A claimant may need to rely on contractual remedies, injunctions, damages or other statutory provisions depending on the facts. Fragmentation can create uncertainty over jurisdiction, standards of proof and the treatment of third-party recipients. A dedicated statute could consolidate these principles while retaining access to existing contractual and equitable remedies.[32]

11.3 Evidentiary and Digital Challenges

Modern trade secrets are increasingly digital. Source code, cloud repositories, research data and engineering files can be copied without physical removal. Litigation therefore requires rules capable of protecting confidential evidence while allowing the defendant a fair opportunity to contest the claim. Indian courts have procedural tools for confidentiality, but a statutory framework could provide clearer mechanisms for sealed records, confidentiality clubs, forensic preservation and limited disclosure of sensitive material.[33]

11.4 Cross-Border Enforcement

Foreign collaborations can involve information moving among several jurisdictions. Indian protection may not prevent disclosure by a third party located abroad, while foreign courts may apply different standards. Contracts should therefore contain governing-law, jurisdiction and dispute-resolution provisions that reflect the location of assets and likely defendants. Arbitration can provide commercial flexibility, but emergency court relief may still be necessary to prevent disclosure before an arbitral tribunal is constituted.[34]

[31] DPIIT, 2016; Law Commission of India, 2024
[32] Indian Contract Act, 1872; Code of Civil Procedure, 1908, Order XXXIX; Specific Relief Act, 1963; Law Commission of India, 2024
[33] Information Technology Act, 2000, §§ 43, 66, 72A; Code of Civil Procedure, 1908, Order XXXIX; Law Commission of India, 2024
[34] Arbitration and Conciliation Act, 1996; Convention on the Recognition and Enforcement of Foreign Arbitral Awards, 1958; Law Commission of India, 2024

12. Recommendations

12.1 Enact a Targeted Trade Secrets and Economic Espionage Law

India should consider enacting a dedicated trade-secret statute along the lines proposed for consideration in the Law Commission's 2024 Report. The statute should define protected information by reference to secrecy, commercial value and reasonable protective measures. It should identify unlawful acquisition, use and disclosure while recognising lawful acquisition, independent development and other legitimate activities. The statute should expressly address third-party recipients who knowingly obtain misappropriated information.[35]

12.2 Preserve Contractual Flexibility

Legislation should establish a floor of protection rather than prescribe every contractual term. Parties should remain free to determine confidentiality periods, permitted uses, security standards, licensing scope and dispute-resolution mechanisms, subject to statutory and competition-law limits. This is especially important because technology collaborations vary significantly between pharmaceuticals, manufacturing, software, defence, biotechnology and emerging technologies.[36]

12.3 Provide Proportionate Remedies

The proposed statute should permit injunctions, damages, account of profits and other appropriate remedies. Emergency relief should be available where disclosure would cause irreparable harm, but safeguards should prevent tactical litigation against competitors or employees. Courts should consider the seriousness of the conduct, commercial value of the information, measures taken by the owner to preserve secrecy and the public interest in the remedy sought.[37]

12.4 Integrate Competition Law

Trade-secret protection should not create immunity for anti-competitive licensing. Agreements

[35] TRIPS Agreement, art. 39(2); Defend Trade Secrets Act of 2016, 18 U.S.C. § 1839(3); Directive (EU) 2016/943, art. 2(1)
[36] Indian Contract Act, 1872, §§ 10, 23, 27; Competition Act, 2002, §§ 3–4; Law Commission of India, 2024
[37] Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836(b); Directive (EU) 2016/943, arts. 10–16; Law Commission of India, 2024

should remain subject to the Competition Act where their conditions affect competition in Indian markets. A statutory provision clarifying the relationship between legitimate confidentiality restrictions and competition law would reduce uncertainty. Restrictions should be defensible by reference to the protection of the transferred technology and should not unnecessarily suppress independent innovation or market entry.[38]

12.5 Protect Employee Mobility

The reform framework should expressly preserve the distinction between confidential information and an employee's general knowledge, skill and experience. Post-employment confidentiality obligations can remain enforceable for genuine secrets, but broad non-compete restraints should not become the default mechanism for protecting know-how. This would align trade-secret protection with Indian contract-law principles and reduce the risk that foreign collaborations become vehicles for excessive restrictions on skilled workers.[39]

12.6 Create Clear Technology-Transfer Disclosure and Review Rules

Foreign technology agreements should be drafted with transparent allocation of background and foreground IP, ownership of improvements, royalty obligations, technical assistance, confidentiality and termination rights. Regulatory authorities should avoid unnecessary intervention in commercially negotiated arrangements but should maintain oversight where sectoral, foreign-exchange, competition, national-security or public-interest considerations are engaged. Clear guidance would reduce transaction costs and improve confidence for both foreign licensors and Indian licensees.[40]

12.7 Strengthen Institutional Technology-Transfer Capacity

Legal reform should be supported by institutional capability. Universities, research organisations and Indian enterprises need technology-transfer offices capable of evaluating patent portfolios, confidential know-how, licensing terms and freedom-to-operate issues. Government policy already recognises technology transfer as an innovation priority, and public research institutions have developed their own IP-management and commercialisation

[38] Competition Act, 2002, §§ 3–4, 3(5); Patents Act, 1970, § 83; Law Commission of India, 2024
[39] Indian Contract Act, 1872, § 27; *American Express Bank Ltd. v. Priya Puri*, 2006; Law Commission of India, 2024
[40] Patents Act, 1970, §§ 68, 83; Indian Contract Act, 1872; Foreign Exchange Management Act, 1999; DPIIT, 2016

guidelines. Wider adoption of professional technology-transfer practices would improve India's capacity to negotiate foreign collaborations on balanced terms.[41]

12.8 Promote Secure Digital Know-How Management

A legal right is only as effective as the security practices supporting it. Collaborators should implement access controls, encryption, audit logs, data classification, employee training and exit procedures. Agreements should allocate responsibility for cybersecurity incidents and require prompt notification of suspected compromise. Statutory protection should encourage reasonable security rather than impose technologically rigid requirements that become obsolete.[42]

13. Contemporary Regulatory Direction

India's policy trajectory indicates growing recognition of technology transfer and trade-secret protection as interconnected components of the innovation ecosystem. The National IPR Policy brought different intellectual-property rights into a common policy vision and expressly identified trade secrets and technology transfer as areas for continuing policy development. The Law Commission's 2024 Report represents a more concrete movement towards legislation. At the same time, the absence of an enacted comprehensive statute means that existing contractual and common-law mechanisms remain central to present-day collaborations.[43]

The practical adequacy of India's framework depends heavily on transaction design. Foreign collaborators can obtain meaningful protection through due diligence, confidentiality controls and precise contractual remedies. Indian counterparties can protect their interests by defining improvements, securing necessary technical information and negotiating fair termination arrangements. Law should facilitate this bargaining process rather than obscure it through uncertainty.[44]

14. Conclusion

Technology transfer and trade-secret protection should not be treated as competing legal

[41] DPIIT, 2016; Patents Act, 1970, § 83; Law Commission of India, 2024
[42] TRIPS Agreement, art. 39(2); Directive (EU) 2016/943, art. 2(1); Law Commission of India, 2024
[43] DPIIT, 2016; Law Commission of India, 2024, Report No. 289
[44] Indian Contract Act, 1872; *American Express Bank Ltd. v. Priya Puri, 2006;John Richard Brady v. Chemical Process Equipments Pvt. Ltd.*, 1987

objectives. They are complementary elements of a functioning innovation economy. Foreign firms are more likely to transfer valuable know-how when they can reasonably protect it; Indian enterprises are more likely to invest in absorption and adaptation when agreements provide predictable access and freedom to innovate. The legal problem arises when secrecy becomes excessive or when weak protection discourages the transfer of high-value knowledge.[45]

India's present framework contains substantial protective tools. The Patents Act provides a sophisticated system for registered technology rights and expressly recognises technology transfer as part of the broader public purpose of patent protection. Contract law allows parties to construct detailed confidentiality arrangements. Breach-of-confidence jurisprudence supplies equitable protection, while the Information Technology Act can address certain contractual disclosures of information. Competition law provides an external check where licensing conditions harm competition. These mechanisms demonstrate that India is not without trade-secret protection.[46] Fragmentation produces uncertainty. The absence of a dedicated statute leaves definitions, causes of action, remedies and procedural questions distributed across different sources. This becomes more consequential as foreign collaborations increasingly involve digital information, software, AI models, biotechnology and complex global supply chains. The Law Commission's recommendation for sui generis legislation provides a strong basis for reconsidering the present structure.[47]

The preferred reform is a focused trade-secret statute that defines the protected interest, codifies misappropriation, provides proportionate civil remedies and addresses digital evidence while preserving independent development, lawful reverse engineering where appropriate, employee mobility, public-interest disclosures and competition-law scrutiny. Such legislation should operate alongside, not instead of, the Patents Act, Contract Act, Competition Act and existing judicial principles. It should also recognise that technology transfer is ultimately a relationship involving continuing access, adaptation and learning rather than a one-time delivery of information.[48]

A balanced Indian framework would therefore protect secrecy sufficiently to make foreign

[45] Patents Act, 1970, § 83; TRIPS Agreement, arts. 7, 39; DPIIT, 2016
[46] Patents Act, 1970, §§ 48, 53, 83; Indian Contract Act, 1872; Information Technology Act, 2000, § 72A; Competition Act, 2002, §§ 3–4; *John Richard Brady v. Chemical Process Equipments Pvt. Ltd., 1987.*
[47] DPIIT, 2016; Law Commission of India, 2024, Report No. 289; TRIPS Agreement, art. 39.
[48] Law Commission of India, 2024, Report No. 289; TRIPS Agreement, art. 39; Directive (EU) 2016/943, arts. 3–5, 9–16.

collaboration commercially credible while ensuring that confidentiality does not become a substitute for perpetual intellectual-property rights or a device for restricting legitimate competition. The objective should be legal certainty with regulatory flexibility: foreign technology owners should know what protection they can obtain; Indian collaborators should know what they are entitled to receive and courts should have clear standards for resolving disputes. On that basis, India can strengthen confidence in cross-border technology transactions while advancing domestic innovation, competition and technological capability.[49]

[49] Patents Act, 1970, § 83; Competition Act, 2002, §§ 3–4; TRIPS Agreement, arts. 7, 39; Law Commission of India, 2024.

REFERENCES:

1. Indian Legislation

1. Arbitration and Conciliation Act, 1996 (India).
2. Bharatiya Sakshya Adhiniyam, 2023 (India).
3. Competition Act, 2002 (India).
4. Code of Civil Procedure, 1908 (India).
5. Copyright Act, 1957 (India).
6. Foreign Exchange Management Act, 1999 (India).
7. Information Technology Act, 2000 (India).
8. Indian Contract Act, 1872 (India).
9. Patents Act, 1970 (India).
10. Specific Relief Act, 1963 (India).
11. Trade Marks Act, 1999 (India).
12. Foreign Exchange Management (Non-Debt Instruments) Rules, 2019 (India).

2. Government Reports and Policy Documents

1. Department of Industrial Policy and Promotion. (2016). National intellectual property rights policy. Government of India.
2. Law Commission of India. (2024). Trade secrets and economic espionage (Report No. 289). Government of India.

3. Judicial Decisions

1. American Express Bank Ltd. v. Priya Puri, (2006) II LLJ 540 Del.
2. John Richard Brady v. Chemical Process Equipments Pvt. Ltd., AIR 1987 Delhi 372.

4. International Treaties and Instruments

1. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, 1869 U.N.T.S. 299.

2. Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, as revised at Stockholm on July 14, 1967.

5. Foreign Legislation and Comparative Legal Materials

A. United States

1. Defend Trade Secrets Act of 2016, 18 U.S.C. §§ 1836–1839.

2. Uniform Trade Secrets Act § 1–4 (Unif. L. Comm'n 1985, as amended 1985).

B. European Union

• 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.

C. Singapore

• Intellectual Property Office of Singapore. (n.d.). Trade secrets.

6. Institutional and Official Online Resources

1. Canadian Trade Commissioner Service. (n.d.). Trade secret protection: India. Government of Canada.

2. Intellectual Property India. (n.d.). National IPR policy and implementation documents. Government of India.

3. U.S. Department of Commerce, International Trade Administration. (n.d.). India: Protecting intellectual property.