PROTECTION OF TRADE SECRETS: THE NEED FOR A BALANCED STATUTORY FRAMEWORK

Nivethitha M & Rishabh Manoj, BBA LL.B., VITSOL, VIT Chennai

ABSTRACT

Trade secrets are the only intellectual property right on which Indian companies can hold without registration, without disclosure and without any grant from the state, yet India does not have a specific statute for trade secret. What we have is a patchwork: confidentiality covenants under the Indian Contract Act, 1872, the equitable action for breach of confidence, and general criminal provisions that have been enacted on the assumption that tangible property is at risk. This paper asks whether the fragmented view is a sufficient justification for a standalone legislation and, if it so, whether the Protection of Trade Secrets Bill, 2024, attached to the Law Commission of India's 289th Report, adequately balances business confidentiality with employee mobility and public interest. This is a doctrinal and comparative study that examines dominant Indian judgements and a comparative study of the Bill against the EU Trade Secrets Directive 2016/943 and the US Defend Trade Secrets Act, 2016. The paper identifies three weaknesses in the present law: absence of settled definition, an undefined borderline between enforceable confidentiality and the restraint of trade prohibited by Section 27 of the Contract Act, and no statutory protection for a secret during litigated. The Bill covers these shortcomings through a four-limb definition, a closed set of lawful ways of acquisition, a statutory duty of confidentiality in proceedings and a commercial court forum, and a defensible repeal of criminal sanctions. It is less convincing overall. The employee skills exclusion is a narrowly drafted definitional carve-out that allows remedies to be unlimited, the whistleblower provision is a defence rather than the immunity the Commission itself proposed, and the compulsory licensing section has uncertain triggers and no procedural floor. The paper concludes that the need for a specific statute is justified, provided that four minor changes are made before enactment, each taken from provisions already working in the EU or the United States and capable of being absorbed into the Bill's statutory structure. It recommends against two changes that the literature often proposes: amending Section 27 and importing the inevitable disclosure doctrine.

Keywords: *Trade Secrets; Protection of Trade Secrets Bill, 2024; Breach of Confidence; Employee Mobility; Whistleblowing; Law Commission of India*.

1. INTRODUCTION

Trade secrets are information that is confidential and has commercial value due to its confidentiality and is subject to appropriate measures to preserve its confidentiality. The international standard is set out in Article 39(2) of the TRIPS Agreement which requires members to protect "undisclosed information" against "unfair commercial use".[1] The value of secrecy is in that which a registered right does not provide. A patent must be fully disclosed, and expires after twenty years; a trade secret does not need to be registered, and lasts for as long as the secret itself. For start-ups unable to afford patent prosecution and know-how not yet patentable, secrecy is often all that there is.

Secrecy too is not invulnerable. Once disclosed, no court can re-establish it. And since firms must also disclose their secrets to their employees, contractors, licensees and investors, the real risk may come more from the insider than the outsider. Protective measures can mitigate that risk but cannot eliminate it; law can deter but, more importantly, it can also prevent many disclosures of information from coming before the court at all. But that same information also lives in the minds of the employees whose freedom to practice their trade is secured by Article 19(1)(g) of the Constitution, and in the minds of those with good reasons to reveal wrongdoing. For this reason, legal protection for business trade secrets can only be justified to the extent that it is balanced against labour mobility, market competition and the public interest.

India has no such specific legislation. Protection is derived from the law of contract, subject to Section 27 of the Indian Contract Act, 1872, which says agreements in restraint of trade is void; from equity for breach of confidence received from English law; and from criminal law provisions on theft, breach of trust and cheating, now found in the Bharatiya Nyaya Sanhita, 2023 (BNS), together with the Information Technology Act, 2000. Courts determine the definition, elements and remedies case by case, a process critics call inconsistent. In March 2024 the 22nd Law Commission recommended a *sui generis* statute in its 289th Report and annexed a draft Protection of Trade Secrets Bill, 2024.[2] The Report records that an earlier failed attempt, the National Innovation Bill, 2008, which was never introduced in Parliament.[3] In the

[1] Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, art. 39(2).
[2] Law Commission of India, Report No. 289: Trade Secrets and Economic Espionage ¶¶ 8.2–8.4, 8.38 (Mar. 5, 2024) [hereinafter Report No. 289].
[3] Report No. 289, *supra* note 2, ¶ 7.4.

author's knowledge, the Bill has not since been introduced and still remains a Commission draft.

Research problem and gap

The research problem is whether India's fragmented position requires a new statute and, if so, whether the Bill achieves a workable compromise between business confidentiality, employee mobility and the public interest. Most of the Indian scholarship's, mostly before 2024, is in favour of a broad codification. It has not evaluated the Bill's attempts to strike a balance against specific failures of Indian case law or against existing protections in foreign systems. This paper addresses that gap.

Research questions

(1) What are the major failures of the current Indian regime? (2) Does the Bill address them without creating undue burden upon employees and public interest? (3) To what extent can Indian policy aspire to incorporate those features of the EU Trade Secrets Directive 2016/943 and the US Defend Trade Secrets Act, 2016 that are relevant? (4) Is a specific statute needed and if yes what minimum changes does the Bill require?

Objectives

The objectives are to map the existing framework and its failures, to scrutinise the Bill and suggest a few amendments that fit its existing structure.

Hypothesis

A dedicated statue is justified, and the Bill remedies the most important structural flaws of the common law position. However, its provisions relating to employee mobility, whistleblowing and compulsory licensing are not yet specified well enough to provide the stated balance.

Scope, limitations and methodology

The paper is doctrinal. It analyses statutes, reported decisions, the Commission's Report and the secondary literature, and compares the Bill with the EU Directive and the DTSA. In doing so, it excludes economic espionage, protection of regulatory test-data under Article 39(3) TRIPS and the interplay between the Digital Personal Data Protection Act, 2023 and trade-

secret protection.[4] Three limitations follow. The Bill is unenacted and may be amended before enactment. There is not enough empirical data about trade-secret litigation in India, which most of the academic consultees explained to the Commission.[5] Thus, the findings are based on reported decisions, and most cases involve interstate trade secret disputes that have reached the stage of interim relief. Lastly, national transpositions of the Directive and differences between US states are not considered.

2. LITERATURE REVIEW

Indian writing on trade secrets concern three things: whether to codify, how to treat employees, and an evaluation of the 2024 proposal. When read together, they suggest a gap between the case for a statute and its draft.

The codification argument

Nomani and Rahman note that Indian law is based on outdated common law theories that courts have variably imposed. They suggest, as do Kumar and Mishra, that India should impose legislation based on the model of the Uniform Trade Secrets Act.[6] Kumar and Mishra also make a useful proposal for the legislation and make the interesting point that the 2008 draft would have made little difference as it would have simply had the parties negotiate terms in a contract leaving the Section 27 problem untouched. Nomani and Rahman similarly criticise the draft on the lack of clarity of the public-interest exception and the clause that would allow continued use in return for a royalty, which they identify as a kind of a compulsory licence.[7] Both raise obvious design issues that the 2024 Bill will have to address itself.

Dwivedi's contribution is doctrinal. He demonstrates that contract, equity and criminal law are each, in their own way, inadequate, particularly because theft was seen as incapable of infringement of intangible information, and he points to India's treaty obligations as requiring legislation.[8] Priyadarshan reprises the argument, emphasizing the lack of a definition and the

[4] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[5] Report No. 289, *supra* note 2, ¶¶ 7.3–7.5.
[6] Md. Zafar Mahfooz Nomani & Faizanur Rahman, *Intellection of Trade Secret and Innovation Laws in India*, 16 J. INTELL. PROP. RTS. 341, 347–49 (2011).
[7] Abhijeet Kumar & Adrija Mishra, *Protecting Trade Secrets in India*, 18 J. WORLD INTELL. PROP. 335, 342 (2015)
[8] Dheeresh Kumar Dwivedi, Protection of Trade Secrets—Does India Need a Separate Legislation?, 3 RGNUL FIN. & MERCANTILE L. REV. 1, 2, 23–26, 30 (2016).

requirement for specialised courts and civil remedies.[9] His account of existing law, however, not reliable. He depends on a privacy case by *Niranjan Shankar Golikari*, which was a decision that turned on Section 27, and he at one-point claims that Indian law provides only criminal remedies, at another that there is no injunction at all, diametrically opposite to the practice of injunctions that Dwivedi notes. This paper therefore considers Priyadarshan for policy arguments only, and bases doctrinal propositions on primary sources. What brings these authors together is their shared approach that is, that each concludes the need for a statute because of the lack of one and because of the American precedent. That is an argument from alignment rather than from any harm.

Employee mobility and confidentiality

On this strand the four authors diverge the most. Nomani and Rahman, Kumar and Mishra and Dwivedi all tell how the Supreme Court manages to differentiate enforceable confidentiality from unenforceable post-termination restraints. The reforms they advocate, however, are to two different ends. Nomani and Rahman and Dwivedi would relax the standard by amending Section 27; Kumar and Mishra favour the US doctrine of inevitable disclosure.[10] Either would give employers a broader scope to restrain mobility, though Nomani and Rahman, Kumar and Mishra regard the Court's misgivings about post-employment restraints as good policy. Priyadarshan raises the alternative concern that trade-secret law can be used against whistle-blowers.

The 289th Report and the Bill

The scholarship here remains predominantly commentary. Byadwal interprets the Bill as a response to the nature of employer conduct. The absence of employees' experience, skills, and efforts from the definition, and the denial of remedies against groundless threats, relate to employers using criminal complaints to silence former employees - a problem he links to Prashant Reddy's scholarship[11]; he sees the Bill's criminal process as weakening that weapon. He reports that criminal remedies were agreed to after consultation, and that the compulsory

[9] 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, 4–7 (2023).
[10] Nomani, *supra* note 5, at 346; Dwivedi, *supra* note 7, at 31; Kumar, *supra* note 6, at 343; Priyadarshan, *supra* note 8, at 5.
[11] Prashant Reddy T., *The 'Other IP Right': Is It Time to Codify the Indian Law on Protection of Confidential Information?*, 5 J. NAT'L L. UNIV. DELHI 1, (2018).

licensing provision has few tools to coerce an unwilling holder.[12] Those critical distinctions are significant. The question post- 2024 is not only how to protect owners but how to prevent over-protection.

What remains unresolved

First, will the Bill's balancing devices hold in practice: where the line will lie between an employee's skill and his employer's secret, whether a whistleblower can rely on the exception to a defamation suit, and what stops mandatory licensing. Second, whether Section 27 needs to be retained in the absence of a separate safeguard of confidentiality. Third, whether the absence of criminal sanctions leaves a significant deterrence gap, since the literature in favour of criminal amendments was published in the period prior to the Commission's consultation. No study compares the Bill against the safeguards of the EU and US models. This paper therefore asks a narrower question than the codification debate: not whether India needs a statute, but whether the Bill's balance is sustainable and what minimal amendments would achieve this.

3. THE EXISTING INDIAN LEGAL FRAMEWORK

3.1 Absence of a dedicated statute

There is no Indian legislation which defines or bestows protection on trade secrets as a class. The Patents Act, 1970 covers inventions where there is an act of disclosure, the Copyright Act, 1957 covers expression and not information and the Trade Marks Act, 1999 protects marks and the trade secrets themselves do not fall in any of their purviews.[13] The protection provided by the courts, which build on the foundations laid by the principles of the law of contract, equity and sometime, copyright when the information happens to be stored in an article that is also protected by copyright. When it is not so stored, copyright protection is of no avail.

3.2 Contractual protection under the Indian Contract Act, 1872

Contractual protection works in three ways-non-disclosure agreements, non-compete covenants, and non-solicitation covenants. The upper limit of contractual protection is laid

[12] Yogesh Byadwal, *Law Commission's 289th Report—Trade Secret and Economic Espionage*, SPICYIP (Oct. 17, 2026, [11:35am]), https://spicyip.com/2024/05/law-commissions-289th-report-trade-secret-and-economic-espionage.html.

[13] Patents Act, 1970, § 10(4), No. 39, Acts of Parliament, 1970 (India); Copyright Act, 1957, § 13(1), No. 14, Acts of Parliament, 1957 (India); Trade Marks Act, 1999, § 2(1)(zb), No. 47, Acts of Parliament, 1999 (India).

down in section 27 of the Contract Act, which states that any agreement that any agreement that prevents someone from engaging in any type of authorized profession, trade or business is void to that extent. The single exception is when goodwill is sold. Distinguishing between covenants that apply during the course of employment and those that apply after termination, in the case of *Niranjan Shankar Golikari v. Century Spinning & Manufacturing Co. Ltd*., the apex court gave effect to a covenant that restricted a person from being employed elsewhere during his term in a company which held a duty of secrecy to a foreign collaborator, by granting an injunction.[14] By way of contrast, in *Superintendence Co. Of India Pvt. Ltd. V. Krishan Murgai*, the Court invalidated a restraint period post-termination, noting that the only permissible relief in circumstances of post-employment service is to prevent the disclosure of trade secrets, none of which were demonstrated.[15] The Court has reiterated that covenants that extend past the contract's duration are null and invalid. An employee has a duty of confidentiality at common law not to disclose trade secrets learned in his employment, and failure to have a written covenant in place does not necessarily prejudice the employer. The law is settled that an employer can legally bind an employee to non-disclosure of confidential information, but not to noncompetition once he ceases employment.

3.3 Breach of confidence, equity and judicial decisions

Where there is no contract, or in addition to a contract, the Indian courts recognize the action for breach of confidence. Under the rule laid down by Megarry J in *Coco v. A.N. Clark (Engineers) Ltd.*, the plaintiff has to demonstrate that the information was given in confidence, the circumstance of the communication demonstrates that it was given in confidence and the information has been used to the defendant's prejudice without the plaintiff's authorisation. The information can be given in confidence by the circumstances alone. In *Zee Telefilms Ltd. v. Sundial Communications Pvt. Ltd.*, the court granted an injunction to the television idea based on the information 'given in confidence', although no formal written contract not to disclose the idea was entered into.[16] In *John Richard Brady v. Chemical Process Equipments Pvt. Ltd.,* the court also restrained the use of know-how, drawings and specifications supplied as confidential information, considering the obligation to keep the information confidential to

[14] *Niranjan Shankar Golikari v. Century Spinning & Mfg. Co., AIR 1967 SC 1098.*
[15] *Superintendence Co. of India (P) Ltd. v. Krishan Murgai, AIR 1980 SC 1717 (India); see also Percept D'Mark (India) Pvt. Ltd. v. Zaheer Khan, AIR 2006 SC 3426 (India).*
[16] *Coco v. A.N. Clark (Eng'rs) Ltd., [1969] RPC 41, 47–48 (Ch.) (U.K.); Zee Telefilms Ltd. v. Sundial Commc'ns Pvt. Ltd., (2003) 27 PTC 457 (Bom.) (India).*

be founded on equity or on the common law action.[17]

The employee cases demonstrate where the protection does not extend. As the Delhi High Court observed in *American Express Bank Ltd. V. Priya Puri*, trade secrets are, for instance, formulae, technical know-how or a peculiar method of business, not known to the public; the Court rejected the belief of an employee that general knowledge could be protected (as it was in the US) and *Diljeet Titus v. Alfred A. Adebare* relied on the principles in Coco in respect of client data and documents taken from a law practice but focused on the misuse of such material instead of the clients' right to practise.[18] Remedies are interim and permanent injunctions under Order XXXIX of the Code of Civil Procedure, 1908 and the Specific Relief Act, 1963, satisfied by the familiar triad of prima facie case, balance of convenience and irreparable injury, together with damages or an account of profits. As equitable relief is discretionary, a delay in applying for or partial knowledge of the information will debar a claimant from it. Courts look for each element and refuse injunctions where secrecy cannot be proved, with third parties who know information is confidential being equally liable-this exposes a new employer to third-party damages even where it has no contract of its own with the employer.

3.4 Provisions of other statutes

Movable property is required for theft to be established, and it was long doubted that whether information could be included. In *Birla Corporation Ltd. v. Adventz Investments and Holdings Ltd.,* the Supreme Court decided that documents, even photocopies of documents, constitute corporeal movable property and therefore information recorded in a document may be stolen; but it struck the complaint, because those documents used in court proceedings did not show the wrongful intent necessary for theft.[19] The case concerns information that is embodied in a tangible form in a document or copy. It does not plainly include what an employee has merely memorised. Whether information is "property" for the offence of criminal breach of trust, now BNS section 316[20], has not been conclusively decided: in Pramod v. Garware Plastics and Polyester Ltd. The Bombay High Court declined to rule on this and advised against using the criminal law as a means of harassment.[21] The Information Technology Act, 2000 provides

[17] *John Richard Brady v. Chem. Process Equip. Pvt. Ltd., AIR 1987 Del 372, ¶ 24 (India)*
[18] *Am. Express Bank Ltd. v. Priya Puri, (2006) 3 LLJ 540 (Del.); Diljeet Titus v. Alfred A. Adebare, (2006) 130 DLT 330 (Del.).*
[19] *Birla Corp. Ltd. v. Adventz Invs. & Holdings Ltd., AIR 2019 SC 2390 (India).*
[20] Bharatiya Nyaya Sanhita, 2023, § 316, No. 45, Acts of Parliament, 2023 (India) (corresponding to Indian Penal Code, 1860, §§ 405–409, repealed).
[21] *Pramod Laxmikant Sisamkar v. Garware Plastics and Polyester Ltd., (1986) 3 Bom CR 411.*

compensation and penalties for unauthorised copying of data (sections 43 and 66), but these provisions are confined to taking through a computer resource.

3.5 Strengths and limitations

The framework has genuine strengths. Equity works without a contract and constrains third parties who are aware that the information will remain confidential; covenants permit protection to be variously customized; and the courts can swiftly issue interim injunctions. The oft-repeated proposition in the literature that Indian law provides no aid by way of injunctive relief is contradicted by the judgments above.

Its limitations are that no remedy has certainty, is rule-based or balances interests. Firstly, there is no definition, so the court determines whether information is secret, valuable and is reasonably protected on a case-by-case basis, and different decisions may result. Secondly, the line between an enforceable obligation and an unenforceable restraint under sec 27 is drawn by case-by-case analysis, and a mind-to-mind rather than a rule-based approach is encouraged. Thirdly, the protection of 'property' by criminal sanctions which are designed for tangible property, may prove to be neither effective nor appropriate. Fourthly, there is no statute protecting the secret from public exposure during legal proceedings: a plaintiff may need to reveal the information for which it claims a right to secrecy and confidentiality clubs and in camera proceedings are paternalistic. Fifthly, no specialist tribunal of prescribed time limits exists for information disputes. These five shortcomings, rather than a lack of remedies, provide the strongest argument for reform, and hit small business hardest.

4. CRITICAL ANALYSIS OF THE PROTECTION OF TRADE SECRETS BILL, 2024

4.1 Background and recommendations of the 289th Report

The Bill has originated in the 22nd Law Commission's Report No. 289, 5 March 2024. The Law Commission invited the judge of a High Court, academics, industry associations (ASSOCHAM, CII and FICCI) and the Department for Promotion of Industry and Internal Trade as consultees. Industry was consistent in its desire for a separate statute; among the academic consultees, opinions varied and several thought existing judicial balancing was adequate. Consultees rejected the idea of mandatory registration of secrets and several took a critical stand against criminal remedies for threats to employee mobility. The Law Commission

recommended a sui generis civil law, which codifies existing judicial principles, excluded criminal remedies, reserved economic espionage for specific legislation, and recognised that a trade secret is not property as it does not generate a monopoly and may be obtained freely by reverse engineering. The Bill comprises thirteen sections divided into four chapters.[22]

4.2 Definition and scope

Section 2(f) states the following four requirement for a trade secret: (a) it is not, in fact, easily accessible to or knowable by those involved in the trade of information; (b) it has commercial value to its proprietor because it is secret; (c) reasonable steps have been taken by the proprietor to keep it secret; and (d) its communication would be detrimental to the proprietor.[23] The first three follow Article 39(2) of TRIPS and provide courts with the statutory test they now lack – the Bill's most significant contribution. An explanation excludes information the disclosure of which would result in a breach of law and what an employee acquires in the course of his normal professional activities. Four issues remain. The fourth limb does not appear in TRIPS, the Directive or the DTSA, and the Commission only proposed the three TRIPS conditions; it is not clear whether "damage" is limited to tangible loss or includes competitive advantage, and lack of definition of "reasonable steps" fails to recognize the limited security budgets available to a start-up; the employee exception depends on the understanding of "normal professional practice".

4.3 Unlawful acquisition, disclosure and use

Section 2(d) defines misappropriation as: obtaining a secret without the consent of the owner through methods that are against to honest commercial practices, such as unauthorised access or copying of the secret, or other conduct that is against honest commercial practices; persuading a person to obtain, use or disclose the secret when that person knew or should have known that it was obtained through a breach of confidence or a violation of honest commercial practices; or obtaining, using or disclosing the secret when that person knew or ought to have known that it was derived from a person who obtained or used or disclosed it through a breach of confidence or a violation of honest commercial practices.[24] The provision is well-

[22] Report No. 289, *supra* note 2, ¶¶ 7.3–7.10, 8.2–8.9, 8.25; Protection of Trade Secrets Bill, 2024, Annexure-I to Report No. 289 [hereinafter Bill].
[23] Bill § 2(f); *cf.* Report No. 289, *supra* note 2, ¶ 8.10.
[24] Bill § 2(d); Directive 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

constructed. It is focused on conduct rather than property, extends to downstream recipients such as an employer who knowingly employs a former employee's computer files, and uses a "ought to have known" test similar to the Directive and somewhat broader than the gross-negligence standard in the TRIPS footnote.

Sec 4 outlines the ways you can obtain a trade secret legally: by independent discovery or creation; through observation, examination, reverse engineering, disassembly or testing of a public or lawful product by a person who has no obligation to restrict such purchase; and other lawfully consistent with good commercial practice. Statuting these makes them clear and puts a stop to trade secret as monopoly. Since Section 3(2) puts confidentiality agreements within Contract Act, many software licences include a reverse engineering restriction that will be subject to normal contract analysis, common in software licences, will be tested under ordinary contract principles.

4.4 Remedies and enforcement mechanisms

Section 7 provides reliefs-injunctions (including ex parte and ancillary relief such as discovery of and preservation of evidence), damages or account of profits (at the option of the plaintiff), delivery up or destruction of materials embodying the secret, and recall of goods substantially based upon the secret, with costs at the court's discretion. Section 8 provides for proceedings before commercial courts; section 9 provides that in proceedings for the disclosure of a secret, the court shall take measures to preserve the secret; section 10 provides a person at risk of spurious proceedings with a declaration and injunction; section 13 preserves other actions. These provisions address forum problems, secrecy of proceedings, and use of false threats that we identified in Part 3.

There are two issues to consider. Preserving the common law action gives claimants with information not captured in the four-limb definition access to a remedy, but it means there will be two routes, and a claimant who prefers the Bill's employee and whistleblower protections can simple plead breach of confidence. Secondly, other than the groundless-threats defence and section 7(3)'s costs discretion, the Bill takes insufficient steps to limit leverage: claimants need not specify a secret particular to the incident in which it was disclosed, and that excess has the potential to threaten free speech, given the Commission's own consultation, which

and Disclosure, art. 4(4), 2016 O.J. (L 157) 1 (EU) [hereinafter Trade Secrets Directive]; TRIPS, *supra* note 1, art. 39 n.10.

reveals that an academic consultee and the US Patent and Trademark Office, both identified claimants' inability to describe their secrets precisely as a barrier.[25] The EU and US regimes provide for both measures.

4.5 Criminal liability

The Bill makes no offence. Commission, citing the ongoing criminal prosecution of an information technology officer at the Ministry of Mines, recommended there should be no criminal offence and, as Part 2 recorded, once the draft of the Ministry had been consulted on the criminal remedies first proposed were dropped. The change can be justified. Reported cases show criminal proceedings being used to threaten ex-employees and Garware itself has warned against this. The scope of a veil-piercing threat of criminal proceedings is even less broad than the legal literature would suggest: there is a way, after *Adventz*, to remove documents or copies of documents that amounts to theft, and there are ways, after BNS, to cheat without any deposit of property or entrustment of property and with dishonest intention, as well as to exfiltrate data electronically after sections 43 and 66 of the Information Technology Act. A caveat is required. Section 13 explicitly states that criminal complaints are not affected and, as for whether section 10 will reach a threat of a criminal complaint, it is probably safer than commentators suggest to assume the Vice-Chancellor's expectation that threats will become dead letters is premature.

4.6 Exceptions, safeguards and potential ambiguities

Employee exclusion.

Excluding skills and experience obtained in "normal professional practice" is the solution in the Bill to the problem of mobility, and it rectifies *Golikari's* implication that an employee must reveal secrets if he wants to move to a rival. But it is a broadest possible definitional exclusion from the scope of the SCA, and employers will contend that the on-the-job acquired know-how itself constitutes a secret. An Indian text, with no protection for experience and skills acquired honestly in the regular course of employment, needs this line provided by the Directive and by a line in English law, which draws a fine distinction in *Faccenda Chicken Ltd. V. Fowler* between information that remains confidential during employment and actual trade secrets which outlive employment.[26] Nor does the Bill guard against an in effect interim

[25] Bill §§ 7(3), 10; Report No. 289, *supra* note 2, ¶¶ 7.5(d), 7.10(f).
[26] *Faccenda Chicken Ltd. v. Fowler*, [1986] 1 All E.R. 617 (C.A.) (U.K.).

injunction that keeps a claimant from working, section 13 provides a means of circumventing that provision. The Commission explicitly rejected the doctrine of inevitable disclosure; that is not included in the text.

Whistleblower exception.

Section 5 says that the import, use, or revealing of a secret is not misappropriation if done for the purpose of revealing an unlawful activity or professional or other misconduct, or in good faith for the purpose of safeguarding the public interest. This offers clarification of clause 11(a) of the 2008 draft, which relied on a court having determined that the revealed matter was in the public interest, and was regarded by Nomani and Rahman as too vague.[27] But it offers protection only ex post and it does not go as far as the Commission believed would be necessary, which is a immunity in addition to defences, so that a whistleblower would still have to foretell a court's decision to arrive at a good-faith and public-interest determination, at the risk of being sued first. It remains silent as to the recipient, so that a confidential report to a regulator would be indistinct from media disclosure. And an employer may still be able to draft a non-disclosure clause that attempts to prohibit protected disclosures, which the Commission thought would be nullified by Section 23, but which the Bill does not mention.

Compulsory licensing.

In section 6, the Central Government can require the holder of a trade secret, during a national emergency or other situation of grave urgency affecting the entire public interest, including epidemic and national security “etc”, to license the trade secret to third parties or the Government. Such license involves a fee in proportion to the importance of the secret and the Cost of its development, constrains the licensee to confidentiality, and terminates when the emergency situation ends. The rest of the terms are left to the rules set out under section 12. The Commission’s decision, the failure of market-based licensing of COVID-19 vaccine knowhow, is fully justified, and Nomani and Rahman supported a very narrow exception. This language contradicts that instruction: the triggers are ambiguous, CII and the Department opposed compulsory licensing of trade secrets in principle, and the Report admits that similar laws do not have such provisions.[28] Two problems arise. The vague language undercuts the argument, made by Nomani and Rahman, that patent law is good for investment, while it may

[27] Report No. 289, *supra* note 2, ¶¶ 8.14, 8.16, 8.24.
[28] Report No. 289, *supra* note 2, ¶¶ 7.7(i), 7.9, 8.17–8.19; Bill §§ 6, 12; Byadwal, *supra* note 10.

inhibit investment for a measure whose purpose is in crisis. And, as Byadwal notes, the clause contains no check against a non-cooperative owner of the trade secret, which may deter investment without delivering on the goal of the provision.

4.7 Does the Bill resolve the shortcomings of existing law?

Overall, on certainty and process: the definition, the closed list of lawful acquisition, statutory litigation secrecy and the commercial court forum address four of the five limitations set out in Part 3; the criminal-law mismatch is intentionally circumvented; and Section 27 is specifically maintained. On balance the Bill succeeds only in part: skills exclusion has no remedial limitation; the post the event whistleblower provision; the mandatory licence contributes to uncertainty; and few restraints on the abuse of claims.

5. COMPARATIVE ANALYSIS

EU Trade Secrets Directive 2016/943 and the US Defend Trade Secrets Act, 2016 (DTSA) are the natural comparators. The Directive converged national laws that had previously diverged significantly – not unlike India's own fragmentation; the DTSA created an additional federal civil cause of action on top of 50 states adopting the Uniform Trade Secrets Act.[29] Both adopt the TRIPS definition, so this Part focuses on the deficiencies identified in the latter two Parts: definition, employee mobility, reverse engineering, public-interest disclosure, and abuse of process.

5.1 Definition

Article 2(1) of the Directive and 18 U.S.C. § 1839(3) each require secrecy, commercial or independent economic value based on that secrecy, and reasonable steps to keep the information secret. They impose no additional requirement of a risk of injury to the owner. The Bill’s fourth limb is thus a departure from the Indian authorities, and, since the other three limbs provide in effect that the information must not be trivial, all it will do is add to the list of contested points. The best way forward is to preserve the clause but note that injury means loss of competitive advantage.

[29] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376; Trade Secrets Directive, *supra* note 20.

5.2 Employee mobility

Article 1(3) of the Directive state that the directive "shall not entail any ground for restricting the mobility of workers: it shall not include any restrictions concerning the use of information that does not constitute a trade secret, or of experience and skills honestly acquired by an employee in the normal course of his employment, nor any further restrictions in employment contracts in addition to those which employment law permits". The DTSA does so in terms of the remedies available. A person may not be prohibited from entering into an employment relationship, employment terms must be based on evidence of threatened misappropriation rather than just what is known, and no order may conflict with state laws on restrictions on a lawful profession, trade, or business (18 U.S.C. § 1836(b)(3)(A)(i)).

The final limit should be even more instructive for India. California's Business and Professions Code § 16600 invalidates most non-competes with respect to close to Section 27, and its courts have rejected inevitable disclosure; California is the most often-cited jurisdiction to show that a robust trade-secret regime can happily coexist with a ban on non-competes.[30] Other jurisdictions have accepted it, but the DTSA's insistence on evidence of threatened misappropriation, rather than mere knowledge, renders inevitable disclosure much less plausible there than under California's proximate-to-Section 27 invalidity. India already has the California-style ban in Section 27 and the Bill's skills exclusion; what is lacking is that express remedial limit. The former is cheap, tested and consistent with *Golikari* and *Krishan Murgai.* The latter would do just the opposite, and the Commission has itself rejected it.

5.3 Lawful reverse engineering

The DTSA excludes reverse engineering and independent derivation from 'improper means' (18 U.S.C. § 1839(6)(B)), in line with *Kewanee Oil Co. V. Bicron Corp.,* where the Supreme Court considered them as fair methods of arriving at a secret.[31] The Directive allows reverse engineering of a product that has been made available to the public or is lawfully in one's possession, but only when the acquirer is under no legally enforceable obligation to limit acquisition (Article 3(1)(b)). Section 4(1)(b) of the Bill already incorporates the Directive in this regard, with the exception of the proviso, and thus the comparison merely reaffirms the

[30] *Whyte v. Schlage Lock Co.*, 101 Cal. App. 4th 1443, 1458–64 (2002), *with PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1269–71 (7th Cir. 1995).
[31] *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974).

Bill's position and there is no lacuna. Any issue of contractual bans will be adjudicated upon by Indian courts under the Contract Act, with no clause of law being necessary to amend.

5.4 Public-interest disclosures

Article 5 of the Directive exempts acquiring, using or disclosing information in order to exercise freedom of expression and information; exposing misconduct, wrongdoing or illegal activity, if the individual did so in the public interest; workers to their representatives in the course of their duties; and protecting a legally recognized legitimate interest. Section 5 of the Bill is similar to the second limb. The DTSA adopts a more pragmatic approach. An individual is protected under federal and state trade-secret law, in 18 U.S.C. § 1833(b), if the disclosure is made in confidence to a government official or an attorney solely for the purpose of reporting or investigating a suspected criminal law violation, or if the disclosure is made in a sealed court filing, and an employer who fails to inform employees of this protection loses exemplary damages and attorneys' fees against that employee.[32] The mechanism provides certainty for a would-be whistleblower prior to disclosure, whereas the public-interest defence only provides certainty post-court determination.

5.5 Safeguards against abuse

Article 7 stipulates that remedies should be reasonable and protections should be in place to prevent abuses and the courts may penalise an applicant for abuse or bad faith; Article 9 provides for confidentiality of proceedings. The DTSA provides for civil ex parte seizure "in extraordinary circumstances" (4) and provides for fee-shifting in suits based on bad-faith claims (18 U.S.C. § 1836(b)(2), (b)(3)(D)).

5.6 What India can realistically adopt

Four of the features come with low institutional costs: a limited express remedial scope for orders restricting employment; a foreign-file reporting scheme for whistleblowers; pleading discipline against exaggerated allegations; and clarification of the open-endedness of the definition. Others don't. Civil ex parte seizure replicates powers already available to Indian courts through local commissioners and interim orders, while the Economic Espionage Act formulation addresses foreign-government conduct that the Commission has pulled aside for

[32] 18 U.S.C. § 1833(b); *see* Report No. 289, *supra* note 2, ¶ 8.15.

its own legislation. And inevitable disclosure, although supported in some Indian literature, would function as a de facto non-compete and would conflict with Section 27.

6. FINDINGS, RECOMMENDATIONS AND CONCLUSION

6.1 Findings

The flaws of the current law are their certainty, procedure and balance, not their redress. There is no settled resolution; the line between enforceable secrecy and void restraint under section 27 is drawn by the case; the criminal matters only fit - and are abusively used - on intangible information; and there is neither civil secrecy in proceedings nor an exclusive forum.

The Bill redresses these four flaws by means of four limbs definition, conduct-based misappropriation, exclusive lawful means, statutory secrecy in proceedings and a commercial court, and by rightly ruling out criminal sanctions. On net, it only partially redresses these flaws: the skills exclusion is definitional, not remedial; the whistleblower clause is a statutory defence, where the Commission requested a defence; the compulsory licensing is poorly circumscribed; and there are few limitations on the abuse of claims. It is established only as respects certainty and procedure, not balance.

India can safely rule out employment-related orders, adopt a confidential whistleblower channel and prevent abuse, learnt from the EU and the US. And it should not unnecessarily abandon the immediate draw of section 27, adopt inevitable disclosure, take a weaker definition, allow civil seizure orders and take a criminal espionage regime.

A dedicated statute is justified, and this hypothesis is validated, with one qualification: the balance clauses require the four amendments listed below.

6.2 Recommendations

A mobility safeguard and two clarifications

In section 7 include: No order under this Act shall prevent a person from entering or remaining in employment or restrict that employment except on proof of actual or threatened misappropriation, and not merely on the grounds of the nature of information known by him or of skills and experience obtained. In the explanation to section 2(f) add: Skills and

experience genuinely gained in the usual course of employment are exempt and damage includes loss of strategic advantage. Section 27 should be left unchanged. This is possible because it is a single clause taken from one that US courts have employed since 2016, reflects *Golikari* and *Krishan Murgai* and the Commission's own suggested rejection of inevitable disclosure, does not alter covenants during employment, and requires no new institution.

A confidential whistleblower channel

Amend section 5 so that a disclosure made in confidence to a public authority or lawyer, for the purpose of reporting or investigating a suspected unlawful act, is not misappropriation, and there is no requirement for a public interest element; and so that a contractual obligation purporting to prohibit such disclosures is void and cannot be enforced to that extent. The current good-faith requirement would stay. This would be possible because it reflects the Commission's proposed solution - immunity not defence; and making the reporting channel clear; because section 5 makes this the rule and the only thing it states; and because the DTSA's employer-notice scheme is avoided.

A statutory floor for compulsory licensing

Section 6 itself should be a reasoned written order setting out the emergency, fixed term (reviewable) and chance to be heard before the fee is fixed (and the open "etc." should be stricken from the list of trigger points). Procedural matters may remain in the rules under section 12. This works because section 6 already sets out a fee, confidentiality and termination; the strike amendment simply raises a procedural floor with normal administrative-law standards and does not create any new body.

Particularisation of the claimed secret

Require a claimant to particularise the alleged secret with sufficient precision in a sealed pleading, within the time created by the Bill's confidentiality duty, before the defendant has to part with its information. There is no need for a separate costs provision, as section 7(3) and the Commercial Courts Act, 2015 already give a costs discretion. This solution is possible because particularisation is a pleading requirement, not a new rule of substantive law; because the Commission's own consultees flagged the vagueness problem as a problem; and because commercial courts already manage sealed pleadings with "confidentiality clubs". Reserve the

other proposals discussed in the literature (amended section 27, inevitable disclosure, a separate criminal offence, registry of secrets). Because there is limited empirical data, a five-year statutory review would allow the criminal-law question to be reconsidered on the evidence.

6.3 Conclusion

The correct balance is that a secret be protected from dishonesty and not competition. The holder must be able to seek relief against breach of confidence, the illegitimate acquisition and knowing receipt, and be confident that the court will preserve the secret during the hearing. It must not be protected against reverse engineering, independent discovery, an employee's own skill and experience or the revelation of illegality. These four suggestions embody this vision of a judicious balance by translating principles in the Bill's vague statement into guidance that courts and whistleblowers can use.

A separate statute is necessary. Splitting the law across different sources creates costs to certainty and abuses of the criminal process, and several of the Bill's best features, namely statutory litigation secrecy, a specific forum, a closed set of lawful acquisition, a bad-faiths-threats rescue and the whistleblower provision, cannot be otherwise created by judicial law. The argument is not based on TRIPS compliance or on investments which the literature states but does not show. It is based on certainty, process and balance, and the Bill must only be enacted when those qualities are guaranteed.

REFERENCES

Indian statutory materials

Enacted laws:

- Constitution of India, Art. 19(1)(g)
- Indian Contract Act, 1872, s. 27
- Code of Civil Procedure, 1908, Order XXXIX
- Specific Relief Act, 1963
- Information Technology Act, 2000, ss. 43 and 66
- Bharatiya Nyaya Sanhita, 2023, s. 316 (criminal breach of trust), and the theft and cheating provisions
- Commercial Courts Act, 2015
- Patents Act, 1970
- Copyright Act, 1957
- Trade Marks Act, 1999
- Digital Personal Data Protection Act, 2023 † (named only as excluded from scope)

Bills, drafts and official reports

- Protection of Trade Secrets Bill, 2024 (Annexure-I to Report No. 289), especially ss. 2(d), 2(f), 3(2), 4, 5, 6, 7, 8, 9, 10, 12 and 13
- Law Commission of India, Report No. 289, Trade Secrets and Economic Espionage (5 March 2024)
- National Innovation Bill, 2008, including cl. 11(a) (never introduced in Parliament)

Foreign statutory materials

United States:

- Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376, codified at 18 U.S.C. §§ 1831–1839. The paper relies in particular on:
    - § 1833(b), the whistleblower immunity

- § 1836(b)(2) and (b)(3), covering ex parte seizure, limits on employment injunctions and fee-shifting
- § 1839(3), the definition of a trade secret
- § 1839(6)(B), reverse engineering

- California Business & Professions Code § 16600
- Economic Espionage Act
- Uniform Trade Secrets Act

European Union:

- Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets), 2016 O.J. (L 157) 1. The paper cites arts. 1(3), 2(1), 3(1)(b), 4(4), 5, 7 and 9.

Indian judicial decisions

- Niranjan Shankar Golikari v. Century Spinning & Mfg. Co., A.I.R. 1967 S.C. 1098
- Superintendence Co. of India (P) Ltd. v. Krishan Murgai, A.I.R. 1980 S.C. 1717
- Percept D'Mark (India) Pvt. Ltd. v. Zaheer Khan, A.I.R. 2006 S.C. 3426
- Birla Corp. Ltd. v. Adventz Investments & Holdings Ltd., A.I.R. 2019 S.C. 2390
- John Richard Brady v. Chemical Process Equipments Pvt. Ltd., A.I.R. 1987 Del. 372
- American Express Bank Ltd. v. Priya Puri, (2006) III L.L.J. 540 (Del.)
- Diljeet Titus v. Alfred A. Adebare, (2006) 130 D.L.T. 330 (Del.)
- Zee Telefilms Ltd. v. Sundial Communications Pvt. Ltd., (2003) 27 P.T.C. 457 (Bom.)
- Pramod s/o Laxmikant Sisamkar v. Garware Plastics & Polyester Ltd., (1986) 3 Bom. C.R. 411

Foreign judicial decisions

United Kingdom:

- Coco v. A.N. Clark (Engineers) Ltd., [1969] R.P.C. 41 (Ch.)
- Faccenda Chicken Ltd. v. Fowler, [1986] 1 All E.R. 617 (C.A.)

United States:

- Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974)
- Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443 (2002)
- PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995)

International instruments

- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Marrakesh Agreement Establishing the WTO, Annex 1C, 1869 U.N.T.S. 299, Apr. 15, 1994. The paper cites art. 39(2) and footnote 10 to art. 39, and mentions art. 39(3) † only to exclude it from scope.
- Directive (EU) 2016/943 is a regional instrument rather than a treaty, so it is listed under foreign statutory materials above.

Articles and papers

- Md. Zafar Mahfooz Nomani & Faizanur Rahman, Intellection of Trade Secret and Innovation Laws in India, 16 J. Intell. Prop. Rts. 341 (2011)
- Abhijeet Kumar & Adrija Mishra, Protecting Trade Secrets in India, 18 J. World Intell. Prop. 335 (2015)
- Dheeresh Kumar Dwivedi, Protection of Trade Secrets—Does India Need a Separate Legislation?, 3 RGNUL Fin. & Mercantile L. Rev. (Issue 2) 1 (2016)
- 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 (2023)

Online sources

- Law Commission of India, Report No. 289 (PDF): https://cdnbbsr.s3waas.gov.in/s3ca0daec69b5adc880fb464895726dbdf/uploads/2024/03/2024030619823188 41.pdf
- Yogesh Byadwal, Law Commission's 289th Report—Trade Secret and Economic Espionage, SpicyIP (May 13, 2024): https://spicyip.com/2024/05/law-commissions-289th-report-trade-secret-and-economic-espionage.html