



Affording Trade Secret Protection Against Reverse Engineering: Global Approaches and Lessons for India

Author: Jayanti Ranjan¹

Abstract

Trade secrets constitute a very essential intellectual property asset for software companies in recent times. They contribute to the business's economies of scale, which gets adversely impacted by instances of breach. Breach of trade secrets are caused by breach of confidentiality, unauthorised public disclosure, and access to these assets. Reverse engineering is essentially moving back from the product to the very origin of the idea, tracing the procedural nuances resulting in such innovation. This procedural knowledge is then used by these developers to redesign or remodel new products based on the same technical knowledge. India does not have a legal framework either for trade secrets or reverse engineering processes, and thus, it becomes more challenging for the original owners of this information to raise claims against breach of their trade secrets. The economic significance of a trade secret is lost once it loses its confidentiality and is made publicly available, thus disincentivising producers from exploring and designing new modes of knowledge. This paper addresses the concerns relating to inadequate protection of trade secrets, along with the grave intensity of the issue in relation to the use of reverse engineering processes and how other nations have responded to it.

Keywords: Trade Secrets, IP Asset, Reverse Engineering, Non-Disclosure Agreement, Misappropriation

Introduction

Trade Secrets are generally protected through the signing of Non-Disclosure Agreements ('NDA') between the parties and do not require a formal registration process like patents.

¹ 3rd Year Law Student at Chanakya National Law University, Patna.

These private contracts are the only instruments for employers and businesses to contain the misuse of sensitive information by former employees through restrictive covenants such as NDAs. Although India does not have a codified statute conferring protection on trade secrets, common law jurisprudence has developed in this area based on the principles of equity, contract, and breach of confidence.² The Supreme Court ('SC') has also upheld the enforceability of post-employment obligations, clarifying the scope of this restriction to be limited to the extent of protection and not to restrict professional freedom unduly.³

Reverse engineering is a process of disassembling a product to comprehend its operation or design. This process may be violative of intellectual property laws in many jurisdictions, especially if it violates patents or is used for unauthorised extraction of trade secrets. The process remains lawful so long as it obtains permission or access from the owner of such an IP asset, and when done for specific reasons like interoperability or education. But there isn't any clear marker for when this process can result in an innovation or invention, especially if it originates from enhancements or modifications in the pre-existing proprietary knowledge.⁴

Defining Trade Secrets

A trade secret relates to technical know-how and knowledge, confidential to its holder. This form of IP is of a highly commercial nature, giving the holder a competitive edge in the outside world over this knowledge.

“An intellectual property may be recognised as a trade secret if it contains the elements of confidentiality, significant economic value and the making of reasonable efforts to maintain secrecy of such information. The information must be kept confidential and should not be publicly accessible and such confidential information holds significant economic value to its holder, which, if compromised in any way, causes economic loss to the holder. The owner of this property makes reasonable efforts and takes adequate measures to protect the confidentiality of this knowledge from unauthorised disclosure to the public.”⁵

² Mohini V, Guarding the Invisible: Trade Secrets Law in India, *Managing Intellectual Property* (Oct. 16, 2025), <https://www.managingip.com/article/2fgqllnfh03y9dwpvpm9s/sponsored-content/guarding-the-invisible-trade-secrets-law-in-india>

³ Niranjan Shankar Golikari vs The Century Spinning And Mfg. Co. Ltd (1967) AIR 1098.

⁴ Shubham Kumar Jha, *Legality of Reverse Engineering: Impact on Trade Secrets and Intellectual Property* (SSRN Working Paper No. 5112045, 2024).

⁵ Sharad Vadehra, Shikha Mittal & Rachana Bishnoi, *Trade Secret Protection in India: A Comprehensive Overview*, Kan & Krishme (May 12, 2025), available at <https://kankrishme.com/trade-secret-protection-in-india-a-comprehensive-overview/>

To decide as to whether such confidential information amounts to a trade secret, the relevant factors to be considered are: the status of the employee and the nature of his work, nature of the information itself, imposition of a duty to maintain the secrecy of information by the employer and a clear distinction between confidential and non-confidential information⁶

International Standards Relating to Trade Secrets

Article 39 of the Agreement on Trade Related Aspects of Intellectual Property Rights ('TRIPS Agreement')⁷ provides protection for trade secrets against unfair competition. Article 44 of the agreement sets forth the minimum requirement for enforcement as "*that "judicial authorities shall have the authority to order the infringer to pay the right holder damages adequate to compensate the injury the right holder has suffered"*", provided that the infringer knew or "*had reasonable grounds to know*" that she was engaging in an infringing activity."⁸

*"It also enables Members to adopt in their internal legal system a wide variety of effective remedies perfectly in sync with the principles of international law, including, among others, provisional measures inaudita altera parte."*⁹ Bilateral Trade Agreements and other IP-related Agreements are also relevant in interpreting TRIPS obligations because of the 'Most Favoured Nation' rule set forth by Art. 4 TRIPS¹⁰. The most favoured national rule provides for an equitable standard of protection, privileges and immunities if granted to one nation to be accorded to all other nations in a similar and alike manner by the signatory member with only an exception to any bilateral or multilateral agreement.

Evolving Jurisprudence in India

In the *Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber*¹¹, the Delhi HC had observed that 'Trade secret law protects a wide array of business data, Customer Lists and other compilations of business data which may be copyrightable as fact works. The courts have time and again upheld the use of confidentiality clauses in employment contracts as a necessary provision to secure the employer's intellectual assets.

⁶ Pollock & Mulla, "Indian Contract and Specific Relief Acts" (13th ed. Vol. 1, Lexis Nexis Butterworths Wadhwa, 2006), pg. 839.

⁷ Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.

⁸ Ibid.

⁹ Davide Arcidiacono, The Trade Secrets Directive in the International Legal Framework, 1 Eur. Papers 1073, 1080–81 (2016).

¹⁰ Agreement on Trade-Related Aspects of Intellectual Property Rights art. 4, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.

¹¹ 1995 IV AD (Delhi) 732.

In *V.N. Deshpande v. Arvind Mills*¹², the court was examining clause 9 of the agreement, which restricted the employee from sharing any secret and confidential information of such nature as was mentioned in the list after his termination from employment. Therefore, the court was right in granting an injunction against the divulging of such trade secrets by the employee as a means to protect the reputation and brand value of the employer in the market.

It has also been clarified through judicial rulings that the details of the customers are not trade secrets nor are they property.¹³ The reason for uploading restraints against an employee is to prevent the proprietary rights of the employer if it is reasonably necessary for securing trade relations or trade secrets. However, this right is available for use to curb competition or against the use of personal skills acquired by the employee during his employment tenure.¹⁴ Also, the stance of the court is very clear as to the period of such limitation on the employee, which is to prevent the sharing or divulging of inside trade information by the employee only up to the contract period.¹⁵

Available Remedies

Section 27 of the Contract Act¹⁶ comes into rescue for the employers to protect their confidential trade information from being shared by the employee. This provision restricts the employee from disclosing any information which he has acquired during the tenure of his employment with the employer.

The courts have granted the relief of injunction (both interim and final) in a suit for infringement of a trade secret. The Delhi High Court in the *Mr. Arjun Dagal & Anr. v. Mr. Shubham Gandhi & Anr*¹⁷ case granted the plaintiff an ex parte ad interim injunction restraining the defendants from manufacturing, marketing, distributing, selling, using, advertising, marketing, offering for sale or in any manner dealing in any garment or product under the plaintiff's label. Damages in the form of actual, punitive or exemplary have also been awarded in cases of serious misuse of such information causing undue loss to the owner. Moreover, the courts are also empowered to pass specific orders directing the defendant to return or destroy the misappropriated information.

¹² MANU/MH/0080/1945.

¹³ MANU/DE/2106/2006.

¹⁴ *Herbert Morris Ltd. v. Saxelby*, (1916-17) ALL ER Rep. 305.

¹⁵ *Zaheer Khan v. Percept D'mark (India)* MANU/MH/1576/2003.

¹⁶ Indian Contract Act, No. 9 of 1872, § 27 (India).

¹⁷ *Mr. Arjun Dagal & Anr. v. Mr. Shubham Gandhi & Anr.* CS(COMM) 918/2025.

Current Dilemma

Trade secret protection in India is weak due to the absence of a dedicated law to confer statutory protection, whereas jurisdictions like the US¹⁸ or EU¹⁹ has have specific legal statutes for the protection of trade secrets. The absence of a statutory framework in India gives space for enforcement issues to arise. Enforcement is challenged because the scope of protection and the available remedies for infringement are missing, and trade secret protection is mainly enforced through contractual relationships between parties. The jurisprudence is also not concrete on the issue, and time and again, courts have given varied and distinct opinions on the nature and ambit of protection guaranteed to the holder. There is no unanimity of opinions among precedents as well.

The legislative or jurisprudential progress in the area is much lower than the number of breaches committed, or the value of economic loss caused because of such breaches to business entities. The problem has accelerated at a high pace in recent years, due to the growth of cross-border and transnational trade. In the absence of an established domestic framework, it disregards the interests of domestic parties in case of a breach committed by international parties. The domestic holders are at a much more vulnerable state, wherein all the technical knowledge gets drained by way of such breaches by international firms in Joint Venture arrangements. There is no uniform international enforcement standard, whereas some jurisdictions like the US and EU have a well-developed legal framework to confer protection to their domestic companies, which makes it a more urgent need for Indian companies at this juncture.

The EU Comparative

The Trade Secrets Directive²⁰ provides for common rules of protecting trade secrets across member nations. The framework enforces consistent statutory governance of trade secrets to prevent their misappropriation. The Trade Secrets Directive aims at approximating Member States Laws and Legislation concerning the protection of “undisclosed know-how and business information against their unlawful acquisition, use and disclosure.”²¹

¹⁸ Uniform Trade Secrets Act (Nat’l Conf. of Comm’rs on Uniform State Laws 1985).

¹⁹ 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 art. 3, 2016 O.J. (L 157) 1.

²⁰ 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.

²¹ Davide Arcidiacono, The Trade Secrets Directive in the International Legal Framework, 1 *Eur. Papers* 1073 (2016).

The protection extends to trade secret by defining it as “*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*”, that “*has commercial value because it is kept secret*” and that “*has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.*”²² For claiming reliefs against such infringement and obtaining damages, the element of fault or intention must be established according to Article 14.²³

A very peculiar provision under Article 3 mentions, permissible means of acquisition of trade secrets, “*independent creation or discovery*”; “*observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret.*”²⁴ This ensures the permissibility for obtaining access to such trade secrets through another person using authorised means. This clearly explains how well thought out the framework is, which not only defines trade secrets, recognises them as IP, and provides relief of damages, but also lays down the clear distinction between lawful use of trade secrets and their misappropriation.

The US Comparative

The U.S. has two major legal frameworks to govern the misuse of trade secrets: the Uniform Trade Secret Act (‘UTSA’)²⁵ and the Economic Espionage Act of 1996 (‘EEA’)²⁶. Both these acts establish two key elements for defining a trade secret; firstly, the person has subjected such information to reasonable efforts to maintain its secrecy, and secondly, the information derives independent economic value. The remedies available under UTSA are protective orders passed by the courts, holding in-camera proceedings, sealed cover records, and granting an injunction against the defendant restricting him from disclosing the alleged trade secret without the court’s prior approval.²⁷

²² 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 art. 2, 2016 O.J. (L 157) 1.

²³ 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 art. 14, 2016 O.J. (L 157) 1.

²⁴ *Supra* note 19.

²⁵ *Supra* note 18.

²⁶ Economic Espionage Act of 1996, 18 U.S.C. 1831–1839.

²⁷ Uniform. Trade Secrets Act § 5 (Uniform Law Comm’n 1985).

The US courts have recognised the operation of the doctrine of inevitable disclosure in cases of trade secrets, mostly in cases of employer-employee relationships. The courts believe that the misappropriation of the trade secrets is inevitable if the employee who has the knowledge of such trade secrets of the employer or his company accepts an equivalent position with a competitor.²⁸

Impact of Reverse Engineering Technologies on Trade Secrets

As previously discussed, trade secrets provide businesses and companies with an economic edge over their competitors, and this IP asset is a result of the hard labour and technological knowledge of the creators, which ought to have protection to foster self-reliance in technology among various sectors of the economy. Reverse engineering processes are used these days by companies to break down a software program and understand its underlying algorithm. This knowledge about the constituents of a program helps these developers in innovatively developing new programs; these developers must first obtain consent from the original creators before accessing it.

Reverse engineering is a pro-innovation measure that helps in the enhancement and growth of innovation by promoting the use of existing technical know-how to create new and updated solutions to the problems of changing times. The same technical knowledge used a decade back, with some improvements, could restructure the existing program and result in a technological revolution.

The benefits of this process are attractive towards fostering re-innovation. However, it also poses serious concerns for the owners or original creators of this sensitive information which provides them with a competitive edge in the market. Their interests are compromised if their knowledge is misused unlawfully without their prior permission and then broken down and used for the remodelling of a new product. The most adverse impacts would be unethical counterfeiting and cloning. This undermines the work of the original producers and compromises their IPR.

Since Indian law does not cover reverse engineering methods under its statutory framework, it becomes even more difficult for original creators to seek protection against a breach of their trade secrets committed by way of reverse engineering. Some recent cases related to such

²⁸ David W. Quinto, Stuart H. Singer, "Trade Secrets – Law and Practice" (OUP, 2009) Pg. 91.

breaches include counterfeit Apple AirPods²⁹ and the piracy of Taylor Swift's³⁰ DRM-protected songs.³¹

Finding Solutions

With the elaborate discussion as to how significant trade secrets are as an Intellectual Property to commercial enterprises remains starkly clear. Now the real question which arises is whether reverse engineering poses serious concerns regarding misappropriation of trade secrets, and if so, what is the way to afford adequate protection for these intellectual assets against this process?

To reduce the risk of losing trade secrets, which hold economic importance to their owners and holders, they must confer protection using licensing agreements, confidentiality agreements, and increasing brand awareness for customers to eliminate the chances of product piracy. The easiest and most feasible method would be by way of licensing agreements, wherein the holders consent to the use of these trade secrets in a limited manner through conferring a license for use. They may limit the licensee to deploy reverse engineering processes. This also grants the holder economic benefits from the sharing of these secrets through the collection of licensing revenues. This reduces the opportunity costs for the holder.³²

Confidentiality Agreements are mostly used in employment arrangements between employers and employees to maintain the secrecy of the information, but can also be extended to other developers for further innovation by limiting the reverse examination of the mechanical or technical processes.

The most effective way to protect the technical know-how about the development of a product is to balance the adverse effects of reverse engineering, which are generally the flooding of markets with pirated products or cloning, by creating consumer awareness. This ensures that the consumers know the product and the brand very well so as to differentiate between real and fake products developed through the breakdown of the original processes of

²⁹ Aaratrika Bhaumik, Sale of Alleged Fake Apple AirPods to Lawyer: Allahabad High Court Orders No Coercive Action Against Flipkart Officials, *LiveLaw* (Nov. 4, 2022), <https://www.livelaw.in/news-updates/sale-alleged-fake-apple-airpods-lawyer-allahabad-high-court-no-coercive-action-flipkart-officials-213286>.

³⁰ Alan Chiu, James Choi & Alison Choy, A Swift Return – A Lesson in Music IP from Taylor Swift's Reclaiming of Master Recordings, *Lexology* (June 4, 2025), <https://www.lexology.com/library/detail.aspx?g=203bf1b9-bebf-4f9b-b5cd-6244f469aff1>.

³¹ Shubham, *supra* note 4.

³² Carmen Tamara Ungureanu & Ștefan Răzvan Tataru, *The Legality of Reverse Engineering or How to Legally Decipher Trade Secrets*, 177 SHS Web Conf. 02001 (2023).

manufacturing, such as Coca-Cola, a very famous beverage drink has a lot many deceptive look alike products available in the market, however the marketing and advertising lessen the chances of consumer purchasing the counterfeited ones.

Lastly, the trade secret holder can implement protection measures against reverse engineering starting from the design and manufacturing stage of the product. Thus, the trade secret holder may use sealing systems or construction materials that break down in the disassembly process and make reverse engineering difficult, if not impossible. The manufacturer or developer can use different techniques in this context, such as encapsulation of hardware components to make non-destructive disassembly almost impossible; mislabelling or marking components to mislead a potential reverse engineer; adding some 'locks' on the product components or within the software program.³³

Conclusion

It is pertinent to note from all this discussion that trade secrets are as valuable an intellectual property as the others, such as copyright, trademarks, and patents. Most of the IPs have today secured protection, which develops the ambition for creative and innovative developments. However, trade secrets contribute much more to the economies of scale of a commercial entity but still lack adequate protection from the lawmakers. The nature of protection afforded is mainly through contractual relations among parties and creates huge potential for infringement disputes arising out of contractual breaches. Also, the variation in judicial interpretation leads to uncertainty and a lack of uniformity. By drawing out a comparative analysis of the US and EU laws, it brings to our attention that there exists a codified legal framework guaranteeing relief against economic damages suffered from misappropriation of such secrets; the EU's framework in this regard has a more nuanced structure.

The complexities in the protection of trade secrets have increased manyfold with the growing use of reverse engineering technologies in the absence of any statutory guidelines to regulate their limited use in decoding or deciphering the trade secret of a mechanical process. This instigates a fear in mind of trade secret holders regarding unauthorised exploitations without any remedies or limitations per se, to address this challenge. Since reverse engineering methods are mostly deployed for breaking down the manufacturing or development process of a product, which necessarily exploits the trade secrets of the creator or owner, the extent to which such use of the derived knowledge of trade secrets should be allowed to protect genuine

³³ P. Samuelson, S. Scotchmer, *The Yale Law Journal*, 111(7), 1662 (2002).

interests of the general public and in specific the asset holder remains ambiguous and up for legislative dialogue towards the enactment of a law addressing all these key issues.