Trade Secret Protection in India: The Policy Debate

Working Paper
September 2015

By Chandni Raina, Professor, Centre for WTO Studies,
Indian Institute of Foreign Trade
New Delhi
Email: chandni.raina@nic.in

Centre for WTO Studies (CWS)
Indian Institute of Foreign Trade
Trade Secret Protection in India: The Policy Debate

By Chandni Raina, Professor, Centre for WTO Studies, Indian Institute of Foreign Trade

Abstract:

The concerns relating to the Indian trade secret protection regime as expressed in the US Special 301 report stands on three planks, the first being that the extant regime is less effective in addressing theft of trade secrets in situations where there is no contractual relationship, the second concerns the difficulty in obtaining damages and the third relates to lack of sufficient procedural safeguards to protect against disclosure of trade secrets and other confidential information in civil or criminal litigation. The report goes on to state that disclosure of trade secret in litigations acts as a major deterrent to using the court system to enforce rights. This paper attempts to examine each of these concerns in the background of available jurisprudence on trade secret protection in India. It then goes on to examine whether trade secret protection can be an option in protecting technological improvements and implications thereof.

Keywords:
Introduction

Protection of trade secrets in India has generally not been a subject matter of much discussion in the past. The present attempt at examining the issues is based on the recent interest on the subject as reflected in the United States Special 301 reports of 2014 and 2015\(^1\) where inadequacy of the Indian trade secret regime was referred to and the submission made by the IPR think tank set up by the Indian Government in its first draft\(^2\) which expressed the need for enacting a law to address gaps in Trade Secret protection. The concerns expressed in the Special 301 report stand on three planks, the first being that the extant regime is less effective in addressing theft of trade secrets in situations where there is no contractual relationship, the second concerns the difficulty in obtaining damages and the third relates to lack of sufficient procedural safeguards to protect against disclosure of trade secrets and other confidential information in civil or criminal litigation. The report goes on to state that disclosure of trade secret in litigations is a major deterrent for the owners from using the court system to enforce rights. This paper attempts to examine each of these concerns in the context of trade secret protection in India.

Trade Secret in common parlance is ‘information of commercial value kept secret’. It could comprise consumer profiles, list of customers and suppliers or may consist of information on distribution networks, advertising strategies or may include information on manufacturing processes\(^3\) and technical know-how. Unlike copyrights, patents, designs and layout circuit designs, trade secret is not really a ‘property right’ as there are no exclusive rights\(^4\) assigned to the trade secret owner. The trade secret regime allows independent discovery/reverse engineering and its use by a third party. On the positive side, trade secret comes into existence on its creation and no costs are involved in seeking a right on it. However, the benefits can be enjoyed only so long as it remains a secret or is not in the normal course developed or generated by another person or entity through proper means, which is the negative aspect. The owner of the trade secret therefore needs to make efforts/invest resources to protect his confidential information. Such protection mechanism could involve contract or confidentiality agreements with employees, suppliers and other business associates to whom the trade secret would need to be disclosed or may get divulged in the normal course of business and/or put in place a system to ensure protection of the trade secret. Since there are no rights being created, operative mechanism for protecting trade secrets would be to allow the owners a legal recourse against unauthorized disclosure of their secret or ‘disclosure in a manner contrary to honest commercial practices’\(^5\) i.e. against unfair

\(^{2}\) www.dipp.nic.in/English/Schemes/intellectual_property_rights.aspx
\(^{3}\) Adopted from the WIPO website http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm
\(^{5}\) ‘in a manner contrary to honest commercial practices’ is a phrase used in the TRIPS Agreement.
competition both on account of violations of the confidentiality clauses in contracts or on the basis of principles of equity/fairness.

Trade secret protection is the oldest form\(^6\) of intellectual property protection. It has been practiced by traditional communities who devised customary laws and mechanisms to ensure that knowledge remained within a community or with certain identified individuals in the community. In the medieval ages, the guild system promoted the use of trade secrets by confining technical knowhow to the members of the guild only. More recently, the Agreement on Trade Related Intellectual Property Rights (TRIPS), which was the first multilateral agreement that discussed protection of trade secret, albeit largely drawn from the United States Uniform Trade Secret Act (UTSA)\(^7\), brought in clarity to the definition by setting down the boundaries in the form of three conditions\(^8\) that any information claiming to seek trade secret protection must comply with. The first requirement being that the information must be secret i.e. not generally accessible or known to persons that normally deal with the kind of information. The second proviso is that it must derive commercial value from it being secret and the third stipulation is that the owner should have taken reasonable efforts to protect the secret. The footnote to Article 39.2 of TRIPS goes on to further elucidate that legal remedies should be available to address breach of contract, breach of confidence and inducement to breach, and acquisition of undisclosed information by third parties who knew or were grossly negligent in failing to know that acquisition was not based on honest commercial practices. While the TRIPS Agreement brought in lucidity to what could be characterized as a trade secret and the type of remedies that should be available to an owner, there was recognition that, in the absence of a formal right, member States could only allow protection against unfair competition. At the same time the fact that TRIPS allowed member States the flexibility to address this issue either through a dedicated law or through the common law system was an acceptance of the vast divergences in the mechanisms adopted by countries to protect trade secrets.

This recognition of diversity in protection of trade secret is also underscored in the 2014 report of the OECD\(^9\) on Approaches to protection of undisclosed information (Trade Secrets) in 11 OECD countries and the BRICS countries. According to the report, there are some broad similarities in regimes when it comes to the definition and scope of trade secrets. However, it goes on to observe that the dissimilarities in the technology transfer requirements and the effectiveness of legal systems in enforcing trade secrets are more extensive and deep. Elaborating on the scope of protection, the report states that most countries under examination would protect technical information, confidential business information and know

---


\(^7\) The UTSA defines trade secret to mean information, including a formula, pattern, compilation, program device, method, technique, or process, that: i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

\(^8\) Article 39.2 of TRIPS

how as trade secrets, with a caveat for independent creation and/or reverse engineering of the knowledge by another party as legitimate means to arrive at knowledge/information which was hither to a trade secret, running as a common thread. Within remedies available, the report found that provisions for third party liability especially when the party knew that the information provided was a trade secret, was another area of commonality. Among the most significant dissimilarities was the availability of criminal remedies. While most common law countries do not have criminal remedies, these were found to be in existence in Brazil, China, Colombia, Japan, South Korea, United States of America, Peru, Russia and Sweden, although their availability was questionable in some countries like China and Russia. Further, while civil remedies of injunctions and damages were provided as means to protect trade secrets in majority of countries under study, there were variations across countries in the practical availability of such remedies.

The subsequent sections of the paper are divided into three parts. Section 2 examines the rationale for protecting intellectual property and considers whether trade secret protection enables socially optimum outcomes for technology development. Section 3 of the paper assesses in detail the available jurisprudence in the context of India and outlines the various facets of the protection provided in the country including remedies against third parties and criminal remedies. An area of concern to many has been the inevitable disclosure of trade secrets during litigation being a disincentive for the affected party to raise disputes. This aspect will be discussed in section 3 for its relevance to a robust protection regime. The last section looks at trade secret protection as one of the options for protecting technological improvements and will examine the implication of an amendment to the legal regime that tilts the balance in favour of trade secret protection.

2. Does Trade Secret Protection lead to suboptimal level of technological improvements?

Intellectual Property can be defined as the creation of human intellect. Creativity\textsuperscript{10} as represented through technological improvements is non-rivalrous\textsuperscript{11} in use-as its use by one does not limit its use by another. It is also non-excludable-as no one can be excluded from using the technology in the absence of a formal right. This situation of seamless diffusion of technology results in positive externalities, as the society is undoubtedly benefitted by the additions to the body of knowledge without being directly involved in its developments. However, with the benefits of improvement getting dissipated throughout the society for everyone and anyone to use, the gains to the individual innovator from discrete improvements in technology would be much lower than what would be possible if he could have had exclusivity over the innovation. If left to the market forces, the divergence in the benefits derived by the private innovator and the society will result in a scenario where technological improvements would be underprovided and the equilibrium would be socially suboptimal.

\textsuperscript{10} Creativity could be in the form of artistic expression or could be a technological improvement or innovation, or a design of an object or a mark that uniquely identifies a product to its producer. However, for the sake of the paper, I assume creativity to imply technology improvements only.
Government intervention becomes necessary to create an artificial system of rights to resolve the market failure. In exchange, this facilitates disclosure of the innovation which in turn adds to the body of knowledge and promotes further research and development. The rationale of the rights based system, thus, was to allow the society to achieve an optimum level of technology development and dissemination which is also an understanding reflected in Article 7 of TRIPS.

The question then is whether trade secret which is a form of intellectual property addresses market failure and enables an optimum level of technological improvement. Here, it is important to note that market failure in case of technological improvements is because of two reasons. The first being the inability to exclude others from using improvements and the second is the positive externality resulting from addition to the body of knowledge and its dissemination.

To understand and respond to the above question more completely, we must look at the scope of trade secrets- i.e. what can be included as trade secrets. In the absence of a definition of the scope in the TRIPS Agreement, a good place to begin would be the scope as defined under the Uniform Trade Secret Act of the USA which became the basis for the construct of Article 39.2 of TRIPS and is by far a comprehensive exposition of the subject matter. Under the UTSA, trade secret could be information, including a formula, pattern, compilation, program device, method, technique or process. In other words, it could be any business information that derives commercial value from it being kept secret with the owner making reasonable efforts to maintain this secrecy. Broadly this would cover information generated in the normal course of business such as customer profile and lists; information on suppliers and distribution networks and advertising and distribution strategies; and technical information on a manufacturing process or method, a program device or a pattern.

The first category therefore comprises confidential business information generated from normal course of business such as customer lists, distribution networks, and advertising strategies. When these are kept secret, they create barriers to entry of new entities as this valuable information would need to be generated again thereby entailing additional costs and time on the part of the competitors, while playing no role in enhancing the body of technical knowledge or know how.

Technical/technological information is the other category of trade secrets. I look at the impact of keeping improvements in technology a trade secret through a standard exposition of the Marginal Benefit and Marginal Cost analysis in the context of the quantum of R&D and research costs. The quantum of R&D, assumed to be equivalent to technological innovation, is indicated on the x-axis and the y-axis represents the research costs.
The benefit derived by a private individual from technical information is depicted by the downward sloping marginal benefit curve indicating that lower the research costs, greater will be the willingness to carry out research. The cost incurred is indicated by the upward sloping marginal cost curve, indicating that extent of research is directly proportional to its costs i.e. more research requires more outlays or resources. Since, innovation, if disclosed, adds to the existing knowledge and spurs further technological development, it can be safely assumed that the Marginal Social Benefits (MSB) curve in the diagram is to the right of the Marginal Private Benefit (MPB) curve implying that for each unit of research carried out the benefit to the society will be higher than the private benefit. According to standard microeconomic theory, the equilibrium point for the society is reached where MC=MSB which is also the optimum quantum of research and the expenditure incurred i.e. q* and e* from the point of view of the society.

In the first scenario, let us now assume that the innovator does not need to put in resources to ensure that technology or know-how remains a secret. Since no additional resources are to be set aside for protecting the invention, the cost incurred by the innovator in carrying out the research is reflected by the Marginal Cost (MC) Curve. The marginal benefit curve of the innovator is indicated by the MPB. The equilibrium point would be the point of intersection of the two curves indicating that the innovator will spend ‘e’ amount to be at the ‘q’ level of research.

In the second scenario, the innovator now has to take reasonable efforts to keep the technology/research secret. The marginal cost curve for him would be the Marginal Private Cost (MPC) curve, indicating that for each level of research, the cost incurred is higher as compared to the previous case because of the efforts/resources put in to keep the knowledge secret. The equilibrium is reached at q₁ with e₁ being the amount spent. Since q₁<q and e₁>e,
it may be concluded that the quantity of research carried out when reasonable steps have to be taken to protect the trade secret, will be less than when he is not required to protect his technological innovation from it getting known to a larger group of people. However, both \((e_1,q_1)\) and \((e,q)\) are suboptimal levels of research indicating that use of trade secret protection for the purpose of protecting technological improvements is suboptimal as compared to the socially optimal position \(q^*\) and \(e^*\).

The analysis reveals that trade secret protection leads to suboptimal equilibrium resulting in research output that is less than what may be desirable for the society at outlays that are much more than what may be acceptable. This is so because technological improvements if kept as trade secrets do not add to the body of knowledge and cannot be a basis for further development by third parties. Moreover, diversion of resource from research and development to protecting and maintaining trade secrets, on the one hand, and investments by third parties to duplicate efforts in a situation of asymmetric information, on the other, also result in sub optimality for the society as a whole. It would be appropriate to state that the social benefits of private research are much greater than which accrue to individual inventors while marginal private costs of technological improvements are much higher than the marginal social costs-a classic outcome of positive externalities of technological improvements. Coming back to the market failure issue, we can see that trade secret helps to exclude others from using the technology but the loss of positive externalities due to this exclusion leads to a sub optimal solution.

Is trade secret protection then totally unnecessary? No. Trade Secret is a potent tool for businesses in maintaining their competitive advantage. It has developed as the private individuals remedy to address the problem created by the inability to exclude a third person, in the absence of a formal right, from access to the technical information generated. This mechanism creates the incentive among the inventors which may be lost if technology could diffuse seamlessly as soon as it is developed. All that is being said is that at any point in time businesses have options to protect their technological improvements in various ways and while trade secret protection is one of the ways, it is not the most optimal route from the society’s point of view.

When will technical know-how be kept a trade secret? There are three broad categories of situations when technical know-how is likely to be kept secret. The first is when technological developments are kept secret by choice because the returns from keeping it a secret would be far greater than patenting it. There could be two possible scenarios for this. The first situation could arise when the utility of the invention is likely to outlast the 20 year patent protection and reverse engineering is difficult without disclosure- recipe of coca cola, Hershey’s chocolates appear to be good examples\(^{12}\). Even when the utility of an invention may have less than a twenty year horizon, trade secret protection may help if the product itself does not disclose the process adopted- say in case of metallurgical inventions. On the

other end of the spectrum would be inventions that have a very short life span making it
unbeneficial for inventors to seek a patent right for such inventions.

The second category of technical know-how to be kept trade secret would be those
which are unlikely to meet the patentability criteria. The third category consists of know-how
that complements a patented invention but is not central to the patent itself. This is often the
case in biotechnological innovations and in wind, solar and other climate change relevant
technologies. The combination of patented invention and tacit know-how would in turn
enhance the value of the invention making it difficult to work the patent even after the expiry
of the patent period.

Thus, trade secret protection can actually be relevant for a large spectrum of
technologies. The type of protection sought would largely depend on the owners own
assessment of the strengths and weaknesses of these options which in turn would be governed
by the policy and legal framework and his evaluation of the needs of the sector.

3. Trade Secret Protection in India

There is no particular law that protects trade secrets in India. Evolved through
judgments, trade secret protection in India has been upheld on the basis of principles of
equity and on common law action for breach of confidence.13 Elaborating upon this, the
Calcutta High Court in the Fairfest Media Ltd vs Lte Group Plc and Ors, (2015)14, stated that
“the essence of this branch of law whatever the origin it may be, is that a person who has
obtained information in confidence is not allowed to use it as springboard for activities
detrimental to the person who made the confidential communication.”

The Indian case laws have tried to address various aspects of trade secret protection-
whether it is defining trade secret/confidential information or the grounds under which trade
secrets can be protected or the scope of remedies. While the Indian courts have drawn
extensively from English case laws, they are now increasingly relying upon the growing body
of domestic jurisprudence on trade secret protection.

In the next couple of paragraphs an attempt has been made to examine the Indian case
laws on trade secrets to bring out the discussion on the definition and the import of the term
‘confidential’, the contours of protection provided and the remedies available including in
situations where there may not be an underlying contract and when action is required against
third parties. This section will also look at the jurisprudence on inevitable disclosure of trade
secrets when disputes come before courts. I have organized this part into three subsections.
The first deals with the definition of confidential information as adopted by the courts; the
second examines the substantive issues of scope of remedies and the third subsection
discusses the inevitable disclosure angle.

13 High Court of Calcutta while summarizing the legal status of trade secret protection in India in the Fairfest Media Ltd Vs Lte Group Plc and Ors (Calcutta High Court, 8th January 2015) http://indiankanoon.org/doc/65868467/
14 Ibid
i) **What is regarded as Confidential Information/Trade Secret?**

The decision of the Court of Appeal in the Saltman Engineering Co. Vs Campbell Engineering Co Ltd.\(^\text{15}\) (hereinafter ‘Saltman case’) is an important judgment extensively relied upon by Indian courts to establish whether information shared between the owner and the recipient is indeed confidential. The court in this case, had held that confidential information “must not be something which is public property or public knowledge. On the other hand, it is perfectly possible to have a confidential document, be it a formula, a plan, a sketch or something of that kind, which is the result of work done by the maker on materials which may be available for the use of anybody; but what makes it confidential is the fact that the maker of the document has used his brain and thus produced a result which can only be produced by somebody who goes through the same process.” In the same vein the Delhi High Court in the Ambience India Pvt. Ltd Vs Shri Naveen Jain in 2005 held that “trade secret is protected and confidential information which the employee has acquired in the course of his employment and which should not reach others in the interest of the employer. However routine day to day affairs of the employer which are in the knowledge of many and are commonly known to others cannot be called trade secret.” Similarly the Calcutta High Court in the Fairfest case (2015), the Delhi High Court in Diljeet Titus Vs Alfred A Adebare and Ors (2006), Hi-Tech Systems and Services Ltd Vs Suprabhat Ray and Ors (2015) and Burlington Home Shopping Pvt. Ltd Vs Rajnish Chibber (1995) clearly establish that information which is duly protected by its owner and which can be potentially damaging to the owner if it is disclosed would get covered as trade secret or confidential information. The court decisions reveal that trade secrets can be formulae, technical know-how, a peculiar mode or method of business adopted by the employer which is unknown to others\(^\text{16}\). It could also include joint venture agreements, loan agreements, and lists of clients or disclosure agreements relating to clients\(^\text{17}\). Financial arrangement, customer lists, business information such as cost and pricing, projected capital investments and inventory marketing strategies could also be classified as trade secret.\(^\text{18}\) In the Burlington shopping case while the arguments relied on copyright infringement of the client database, applicability of trade secret protection to compiled database was also stressed.\(^\text{19}\)

From the foregoing it is apparent that in India a broad set of information falling in the category of business or industrial information and technical know-how or process would get protected as trade secret so long as the information is not accessible to persons readily, has commercial value from it being kept a secret and the owner has taken steps to protect it.

ii) **What can Trade Secret/Confidential Information be protected against?**

Trade secret or confidential information is information that is closely held by the owner. Since this information is also pertinent for the running of his business, it may have to

\(^\text{15}\) [1948] 65RPC 203
\(^\text{16}\) Ambience India Pvt Ltd Vs Shri Naveen Jain (Delhi High Court;2005) Eq. citation: 122 (2005) DLT 421, 2005 (81) DRJ 538
\(^\text{17}\) Diljeet Titus Vs Alfred A Adebare &Ors (Delhi High Court; 2006) Eq. citation: 130 (2006) DLT 330, 2006 (32) PTC 609 Del
\(^\text{18}\) Hi-Tech Systems & Services Ltd Vs Suprabhat ray and Ors (High Court of Calcutta; 2015) MANU/WB/0464/2015
be shared with certain employees or business associates like suppliers, joint venture partners in the interest of work. In such situations the owner may take recourse to contracts or confidentiality clauses in agreements to ensure protection of the trade secret. The contracts or confidentiality clause typically require the employee to keep confidential information secure and not divulge it during the course of employment and thereafter. When employees resign in breach of agreement, they may also be required to honour the non-competition clause requiring them to abstain from being engaged in similar activities for a certain period of time.

Examination of the case laws on the subject indicates that while the confidentiality and non-competition covenants have been upheld by the Indian courts, an important consideration has been the reasonableness of these restrictive covenants in contracts. Decisions have been given after evaluating whether the restrictive covenants would run contrary to the spirit of Section 27 of the Indian Contract Act, 1872, which holds any agreement that is in restraint of trade or exercise of a lawful profession to be void. The issue relating to reasonableness of the restrictive covenants in agreements was examined by the Supreme Court of India in the Niranjan Shankar Golikari Vs Century Spinning and Mfg Co. Ltd case. The Apex court held that negative covenants operative in the period of the contract of employment cannot generally be considered to be in restraint of trade. It also stated that negative covenant that the employee not engage himself in a trade or business or get self employed and perform similar or substantially similar duties is not a restraint of trade unless the contract is unconscionable or excessively harsh or unreasonable or one sided. In the extant case it found that the restriction as placed in the contract as reasonable and did not amount to restraint of trade. Discussing the need to carefully frame negative covenants especially when these concern employees, the same court in the Superintendence Company of India (P) Ltd Vs Sh Krishan Murgai held that there is inherent inequity in the bargaining power of the employee and the employer when it comes to employment contracts so much so that the employee may give no thought to the substance of the contract at the time of appointment. According to the Court, the restraint should ‘not be greater than necessary to protect the employer nor unduly harsh or oppressive to the employee’. The court therefore, disfavoured a broad restrictive covenant requiring the employees not to engage in a business similar or competitive with that of the employer after the termination of this contract of employment on the grounds that it would unduly affect the employee’s means of procuring a livelihood.

At the same time the courts have taken a grim view of employees using trade secrets or confidential information they were entrusted with as spring boards in the course of their business or career. In the Hi-tech systems and Services Ltd Vs Suprabhat Roy & ors case,

---

20 Section27. Agreement in restraint of trade, void.—Every agreement by which any one is restrained from exercising a lawful profession, trade or business of any kind, is to that extent void. Exception 1. — Saving of agreement not to carry on business of which goodwill is sold.—One who sells the goodwill of a business may agree with the buyer to refrain from carrying on a similar business, within specified local limits, so long as the buyer, or any person deriving title to the goodwill from him, carries on a like business therein, provided that such limits appear to the Court reasonable, regard being had to the nature of the business.
21 MANU/SC/0364/1967
22 1980 SCR (3)1278
23 MANU/WB/0464/2015
the court found that the respondents were soliciting business from customers of the plaintiff on the basis of confidential information acquired by them while working for the plaintiff. The court, therefore, issued an injunction against the respondents from orchestrating any breach of an existing contract of the plaintiff with third parties on the grounds that the breach of an existing contract entitles the plaintiff to equitable relief. Similarly in the Niranjan Goliarkari case, the Supreme Court agreed with the findings of the High Court and the trial court that disclosure of specialized information to a rival company would harm the interest of the respondent and upheld the injunction on the appellant on the ground that it “is restricted as to time, the nature of employment and as to area and cannot therefore be said to be wide or unreasonable or unnecessary for the protection of the interests of the respondent company.”

In the Embee Software Pvt Ltd Vs Samir Kumar Shaw & Ors, the High Court of Calcutta, citing previous decisions in the Desiccant Rotor International Pvt Ltd Vs Bappaditya Sarkar and ors, VFS Global Services Pvt Limited V Mr Suprit Roy of the Delhi and Bombay High Court respectively, held that non-solicitation clause did not amount to restraint of trade, business or profession therefore would not be hit by Section 27 of the Indian Contract Act, 1872. It went on to state that an ex employee even in the absence of a specific non solicitation clause in the contracts cannot practice it to damage the business of the ex employer.

In case of contracts between companies, such as between vendor and purchaser and in partnership agreements, the courts have taken a less constrained and more favourable view of restrictive covenants. In M/s Gujarat Bottling Co. Ltd (GBC) and others Vs Coca Cola and Others, the Apex court had held that the agreement signed between the parties in 1993 was a franchise agreement allowing GBC to manufacture, bottle, sell and distribute the beverage while also restricting the right of GBC from dealing with competing goods. The view of the court was that the negative covenant facilitated the distribution of the good of the franchiser and that it cannot be considered as restraint of trade. It also said that the subsequent action of transfer of shares of GBC to Pepsico Ltd without information being given to Coca Cola was in breach of the agreement signed in 1993 and that the said company had acted in an unfair and inequitable manner in its dealings with Coca Cola. The court, consequently, did not see “any infirmity in the injunction imposed by the High Court restraining GBC from using the plants in Ahmedabad and Rajkot from manufacturing, bottling, selling or dealing with or concerning in any manner whatsoever with the beverages of any person till January 25, 1996.” In the Fairfest Media case, the petitioner had entered into a non disclosure agreement (NDA) with the respondent ahead of the proposed joint venture agreement between the two. The NDA was valid for six months from the date of signing which was 15th March 2013. Following the agreement and on the request of the respondent, confidential financial and marketing information was transmitted by the petitioner. The joint venture proposal was however withdrawn by the respondent in April 2014 but in the meanwhile all confidential information was taken by the defendant and the non disclosure agreement signed between the petitioner and respondent was also no longer valid. Relying on the exposition of the law by Lord Griffiths in the Attorney General Vs Guardian Newspaper Ltd (No. 2) (1990), IAC 109,

---

24 AIR 2012 Cal 141
25 http://indiankanoon.org/doc/175180860/
26 MANU/MH/1043/2007
that the right to remedy was not dependent on contract but in fact existed as an equitable remedy, the court examined the case on the basis of principles of equity and the spring board doctrine and inter alia restrained the defendant from sharing any information concerning marketing strategy, customer base received from the plaintiff for their proposed travel show.

More complications in protection of trade secret or confidential information arise when there is no underlying contractual agreement or when theft of the information is by a third party. As far as the former is concerned, the case that has been cited in many judgments is that of John Richard Brady Vs Chemical Process Equipments (1987)\textsuperscript{27}. The defendants had got the drawings of the fodder production unit from the plaintiff for a limited purpose of providing a certain part required in the plant. However, they were found to have misappropriated the information and had used it as ‘spring board’ to enter the business. While examining the case the Delhi High Court relied on the statement of Lord Greene in the Saltman case that as long as the information was confidential it did not really matter whether there was a formal contract protecting it from disclosure and misappropriation. The court restrained the defendants from using the information in their possession and imposed costs on grounds of general rules of equity and breach of confidence. While deliberating on the facts, the court drew attention to the statements made by Lord Greene in the Saltman case on the remedies that should be available when confidential information is at stake. Explaining this in the context of three scenarios, Lord Greene had submitted that if there is a contract and a party receives confidential information, then even if the contract is silent on it, there would be an obligation on the receiving party to keep the information confidential. In another situation when a defendant has used confidential information obtained directly or indirectly from a plaintiff without the consent, express or implied, he would be guilty of infringement of the plaintiff’s rights. In yet another situation, so long as the information was confidential, there would be obligations on the party receiving it whether or not there was an underlying contract.

As further examples will indicate, confidentiality and principles of equity are sacrosanct conventions in trade secret protection in India and operate independent of an underlying contract. In Escorts Construction Equipment Ltd Vs Action Construction Equipment P. Ltd(1998)\textsuperscript{28}, an ex employee after putting in nearly ten years of service in key positions, left the company and in a span of the next three years set up a company which manufactured very similar Pick and Carry Hydraulic Self Mobile Cranes as produced by the plaintiff. There was no underlying contract which had been dishonoured. The Delhi High Court however imposed an injunction on the grounds of breach of confidence as the defendant who was an ex employee of the plaintiff had tried to misappropriate the designs of his ex employer. It held that the balance of convenience was in favour of the plaintiff as unless the defendants were restrained by the ad interim injunction, irreparable loss or injury which could not be estimated in terms of money would be caused to the plaintiff.

\textsuperscript{27} 81 (1999) DLT 122
\textsuperscript{28} http://indiankanoon.org/doc/1315312/
More recently, the Karnataka High Court in the V.V Sivaram and Ors vs Foseco India Limited (2005)\textsuperscript{29} agreed with the injunction imposed by the trial court against the defendants (appellants in this case) on grounds of breach of confidence because the defendants who had left the company after putting in nearly 12 years were in possession of confidential knowhow which they made use of to produce a product similar to that of the plaintiff and tried to pass it off as such. The court accepted the fact that an implied duty to protect the plaintiff’s right was enforceable and went on to say that disclosure of confidential information after cessation of employment by an employee can be restrained.

Theft of trade secrets on the instigation, or by third parties, is an important area where jurisprudence is growing in India. In the Base International Holdings Vs Pallava Hotels Corporation Limited, the defendants had signed an agreement with the plaintiff to set up Holiday Inn Crowne Plaza at Madras. Overtime, the defendants received confidential information concerning among other things the Holiday Inn System, the hotel plans and other recommendations, advice and information on hotel computer system, room reservation technology etc. The defendants were in turn required to complete the construction by 31\textsuperscript{st} December 1995 upon which the license to use the Holiday Inn system was to be given. The plaintiff had the right to terminate the agreement in case the construction was not completed in time. Since the defendants failed to complete the hotel by 31\textsuperscript{st} December 1995, the plaintiff could not grant the license to them to use the Holiday Inn System for operating the hotel. However, no further action of termination of Agreement was taken by the plaintiff. In February 1996, the second defendant, on the other hand, wrote a letter on behalf of the first defendant seeking termination of the agreement on the grounds that construction could not be completed on time by them. The very same day the defendants also entered into an agreement with Hilton International. The High Court of Madras\textsuperscript{30}, observed that the defendants “clandestinely attempted to bypass and give a go bye to the agreement entered into with the plaintiff without putting the plaintiff on notice.” The court, citing the Supreme Court decision in the Gujarat Bottling Co Ltd Vs Coca Cola, went on to say that “it cannot be disputed that Hilton International is fully aware of the arrangement between the plaintiff and the defendant...” and held that “it would not be possible to quantify the damage that would be caused to the plaintiff by reason of the conduct of the defendants in terminating the agreement and hitching up with Hilton International”. The court granted injunctions against the defendants restraining them from using or converting to use the proprietary information of the Holiday Inn System. Interim prohibitory injunctions were also imposed on the defendants from transferring, alienating or creating any interest in favour of any third party directly or indirectly in the proposed hotel and further the defendants and others including representatives, stockists etc were also restrained from commissioning and operating the hotel.

While the role of a third party was alluded to in the above case leading to injunctions being imposed stopping the operations of the new hotel, it was dealt with in a more forceful

\textsuperscript{29} MANU/KA/0520/2005 Eq citation 2006(1)KCCR429
\textsuperscript{30} MANU/TN/1929/1998 Eq citation 1999(19)PTC252(Mad)
manner by the High Court of Karnataka in the Homag India Private Ltd Vs Ulfath Ali Khan\textsuperscript{31}. In this case the court stated that documents prima facie establish that the first defendant was prompted by the second defendant M/s IMA Klessmann GmbH to commit breach of confidentiality by transferring confidential data from his official Homag account to his personal email account. It went on to state that “in the circumstances, it is not necessary for plaintiff to establish that the second defendant has been using plaintiff’s confidential business information to promote business of the second defendant” and held that breach of confidentiality and misuse of confidentiality are actionable rights. The defendants were restrained through a temporary injunction from carrying on business, dealing with the plaintiff’s customers and from utilizing information in the form of technical data, manufacturing process, marketing plans, offers, pricing, customer list, software, specifications, engineering methods etc.

As recounted above, the jurisprudence indicates that theft of confidential information whether through physical custody of it or through electronic means has been firmly discouraged by the Indian legal system. Even so, the growing use of information technology in communication and in storage of proprietary information had led to the need to provide civil and criminal remedies against information theft through the electronic route and against its misuse. This led to the promulgation of the Information Technology Act, 2000 and its further amendment in 2008. The legislation provides legal recognition to e commerce including the use of alternatives to paper based means of communication and storage. The law has further tightened the enforcement measures and facilitates imposition of stiff statutory damages, penalties and imprisonment for, among other situations, theft of confidential information such as unauthorized use of data/information obtained from computer systems, tampering of source code or its theft and unauthorised download of database or information in removal storage medium. Section 43 of the legislation makes it liable for the offender to pay damages by way of compensation not exceeding Rs 1 crore to the person affected. In addition section 66 of the said legislation provides for imprisonment for a period of up to three years or a fine of upto Rs 5 lakhs or both. The legislation recognizes third party liability if the party knowingly accepts or had reasons to believe that the information given to it was stolen. Besides this, provisions of the Indian Penal Code and the Evidence Act, 1872 have also been amended to enable action against cyber crimes. There have been a number of cases where provisions of the IT Act have been invoked- Mphasis BPO Fraud case in 2005 on unauthorized use of computer resource, Syed Asifuddin and Ors Vs the State of Andhra Pradesh which related to tampering of computer source and Kumar Vs Whiteley on unauthorized access and alterations to the computer database\textsuperscript{32} - are a few. In a recent judgment in the Arhan Technologies Vs Endo Kogyo Co. Ltd\textsuperscript{33}, the State Information Technology Department levied a damage of a total of Rs 60 lakhs on the

\textsuperscript{31} MANU/KA/1569/2012
\textsuperscript{32} http://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/
\textsuperscript{33} Complaint no. 2 of 2013 dated 28\textsuperscript{th} January 2013; order by Secretary, Information Technology, Mantralaya, Govt. of Maharashtra on 18\textsuperscript{th} June 2013
defendants for the misappropriation of confidential business information. The case was, however, later withdrawn after out of court settlement between the parties.\textsuperscript{34}

In addition to criminal liability under the IT Act, Sections 405-409 of the Indian Penal Code (IPC) which relates to criminal breach of trust and section 418 concerning cheating can also be invoked but only to get an appropriate remedy against a grave offence. This has been very evidently laid down in the Bombay High Court Judgment in the Pramod, Son of Laxmikant Sisamkar vs Garware Plastics and Polyester case\textsuperscript{35}. The petitioners were engineering graduates who were working with the defendants for a period of three years and had later left the company to join some other organization. The contention of the defendants was that they had not handed over the documents in their custody and that the special technical knowledge that the petitioners had gained while in the service of the defendants would be used by them in the new organization. On the basis of the written complaints the Chief Judicial Magistrate had registered cases against the petitioners for offences of criminal breach of trust and cheating punishable under section 408 and 420 of the IPC which was then challenged in the High Court of Bombay. The court found that the defendants had not mentioned any particular documents to have been in the custody of the petitioners at the time they left service. The court also found that the new company joined by the petitioners had yet to commence production; therefore, held that it was premature (as the company had yet to begin production) to allege that the technical know-how gained by the petitioners was used by them. While, setting aside the orders of the trial Magistrate, the court observed that “it is well settled that criminal prosecution is a serious matter and would amount to harassment of the accused and also to the abuse of the process of the court if without sufficient grounds it is allowed to proceed”. It went on to state that the remedies should not be used to harass or seek person vendetta or be used with an ulterior motive to pressurize the accused.

In this section, we have so far discussed a wide array of cases where trade secret protection is the central issue. The Indian jurisprudence indicates that protection for trade secret is provided not only when there is an underlying contract but also in the absence of any contract on grounds of equity and breach of confidence. Courts have extensively relied upon the statement of Lord Greene in the Saltman case - that as long as the information was confidential it did not really matter whether there was a formal contract protecting it from disclosure and misappropriation. In case of contracts, legal validity of confidentiality and non-competition covenants have been upheld by the Indian courts if the contracts are found to be limited in time, nature of employment and area. However, where contracts involve companies, the courts have viewed the negative covenants favourably to facilitate distribution of goods of the franchiser rather than being in restraint of trade. Even in the absence of an underlying contract, theft of trade secret and its use as spring boards by employees has been viewed seriously by the courts. Accepting that implied duty to protect the plaintiff’s right is enforceable, the courts have held that disclosure of confidential information after cessation of employment by an employee can be restrained. In the area of theft of trade secret by third

\textsuperscript{34} Vide order dated 24\textsuperscript{th} March 2014

\textsuperscript{35} 1986(3) BomCR 411
parties, the Indian courts have had to deal with cases where theft has been either actively orchestrated by third parties or where third parties have been passive beneficiaries.

While criminal remedies for breach of trust are available, the underlying principle is that it should not be used as a tool for harassment. At the same time, the Information Technology Act 2000 and its subsequent amendments takes cognizance of the growing menace of cyber crimes providing therefore for stiff statutory damages, penalties and imprisonment to those found guilty of theft of confidential information and computer source code.

Let me now get into the related question of the type of civil remedies that an owner of trade secret can seek. In the Fairfest case, the court summarized the possible remedies that could be sought by a trade secret owner, to include –obtaining an injunction to prevent disclosure of the trade secret, return of all confidential information and compensation for any loss suffered due to disclosure of trade secret. While all these remedies are available, courts have extensively relied on injunctions to address trade secret theft in India on the grounds that it is the only feasible remedy for an action that is liable to cause ‘irreparable loss that cannot be estimated in monetary terms’ to the owner of the trade secret. The superiority of injunction as an effective remedy over damages is widely recognized in legal literature. Murphy (2007) in his paper on ‘Rethinking Injunctions in Tort Law’ argues that when it is difficult to value the loss objectively and it is primarily left to the claimants to do so, damages will be imperfect remedies and injunctions would always be better in such situations. This would apply squarely to trade secrets which by their very nature are undisclosed and hold different monetary value to the claimants, making it difficult to establish the exact monetary value. Be that as it may, although injunctions may be the superior remedy having an immediate impact of complete seizure of operations of the errant company or in the mobility of an employee, damages or relief is also available to the owner under the Indian law if sought. In the Bombay Dyeing and Manufacturing Company (2008), the High Court of Bombay issued an injunction against disclosure of confidential information relating to the Goa property of the plaintiff and also allowed them to seek relief through a separate suit. In fact in many cases involving theft of trade secrets where injunctions are imposed, the affected party is invariably allowed to seek relief separately. Moreover, with the Information Technology Act, 2000 specifically allowing for statutory damages, remedies to cyber crimes usually involve imposition of damages and other penalties.

iii) Can trade secrets be protected against inevitable disclosure in the court system?

Trade secret by its very nature is confidential information or technical knowhow of value to the owner and duly protected by him. An important concern, therefore, has been that litigation involving trade secrets is liable to make the information public thereby defeating

---

36 http://indiankanoon.org/doc/1315312/
38 2010 vol 112(8) Bom LR 3739
the very purpose of granting protection under law. This issue has been examined in detail in the 9 bench judgment of the Supreme Court of India in the Naresh Shridhar Mirajkar and Ors Vs State of Maharashtra and Anrs\(^{39}\). The case concerned a defamation suit filed against the Blitz magazine in the High Court of Bombay. One of the witnesses had requested that his evidence should not be given any publicity. When this was agreed to by the High court, one of the journalists moved the Supreme Court under Article 32 of the Constitution for alleged violation of Article 19 of the Constitution on the grounds that the fundamental rights of the petitioners were violated.

The Apex Court addressed two fundamental questions. The first was whether the High Court had the power to allow the proceedings to be held ‘in camera’ and whether such an order would violate the fundamental rights under Article 19 of the Constitution. Addressing the first issue, the 9 member bench stated that although “the code of civil procedure contains no express provision authorizing a court to hold its proceedings in camera, the court has inherent jurisdiction to pass an order excluding the public when the nature of the case necessitates such a course to be adopted.” It observed that Section 151 of the Code of Civil Procedure 1908, by giving the courts inherent power to make such orders as may be necessary for the ends of justice or to prevent abuse of the process, enabled courts to decide whether or not to have trials in camera. This decision, nevertheless, had to be entirely based on whether this would aide the ‘the administration of justice itself’.

On the issue of whether it would violate the fundamental rights as enshrined in Article 19 of the Constitution, the Apex Court while reflecting on the observations of Viscount Haldane, LC, stated that “public trial of causes is a means, though important and valuable, to ensure fair administration of justice itself, on the one hand, and public trial on the other, inevitably, public trial may have to be regulated or controlled in the administration of justice.” Elaborating upon the broad exceptions to holding public trials, the Apex Court said that, “trial in closed session is generally, ordered to prevent publicity which is likely to deter parties or their witnesses from giving evidence, on account of the nature of the evidence such as ...... matters publication of which may harm the interests of the State or the public at large, for instance, disclosure of official secrets, or matters which lead to publication of secret processes, publication of which would destroy the very basis of the claim for relief etc.”

Ensuring non disclosure of trade secrets in court proceedings is an essential concern of the courts in India as is apparent from the opinion of the Apex court. Courts have out rightly refused disclosure of information on the grounds that the information would then become public and not remain confidential.\(^{40}\) The OECD report also echoes this, in the case of India, recognizing that secrecy of confidential information can be sought by the plaintiffs during litigation.\(^{41}\)

\(^{39}\) Naresh Shridhar Mirajkar And Ors Vs.Respondent:State Of Maharashtra And Anr. Date Of Judgment:03/03/1966 Citation 1966 SCR (3) 744

\(^{40}\) Fairfest Media Ltd vs Itc Group Plc & Ors on 8\(^{th}\) January 2015

4. **Trade Secret Protection - As one option for technological improvements?**

The type of protection sought by an inventor for the technological improvements depends on the quality of the invention - i.e. whether it could stand the test of patentability under the law of the country where he seeks to protect it and the strength of the possible alternative i.e. trade secret protection vis-à-vis patent protection. One can argue, as indeed it was done through the dissenting note of Justice Douglas in the decision of the Supreme Court of United States in Kewanee Oil Company Vs Bircon Corporation\(^{42}\) et al, that there is an inherent policy conflict in allowing an invention to be kept a secret. It was argued that if the federal patent law provides fixed term protection in exchange of complete disclosure of an invention, how can States allow perpetual protection without any requirement to disclose the invention? An even greater conflict arises; if trade secrets aim to protect only those inventions that are inherently not patentable because under the patent law, such inventions would normally be part of the public domain. The Supreme Court of United States in this seminal case evaluated whether the Ohio trade secret law ‘stood as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress’ as reflected by the federal patent law and held that trade secret and patent law have their distinct roles and until a decision is taken to the contrary by the Congress, States should be free to grant protection to trade secrets.

Subsequently, of course the Uniform Trade Secret Act came into being which has been gradually adopted by most States with the exception of the State of New York where common law continues to be the basis of protection of trade secret. Although the rationale for a dedicated legislation on trade secret was to bring in greater uniformity in how cases were decided across States, yet the prefatory note to the United States Uniform Trade Secret Act with 1985\(^{43}\) amendments drafted by the National Conference of Commissioners on Uniform State Laws as approved by the American Bar Association is instructive and intriguing as it focuses on the problem faced when a patent granted for a period of 17 years\(^{44}\) is revoked or invalidated by courts. This is evident from the following statement included in the prefatory note to the legislation:

> “A valid patent provides a legal monopoly for seventeen years in exchange for public disclosure of an invention. If, however, the courts ultimately decide that the Patent Office improperly issued a patent, an invention will have been disclosed to competitors with no corresponding benefit. In view of the substantial number of patents that are invalidated by the courts, many businesses now elect to protect commercially valuable information through reliance upon the state law of trade secret protection. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974), which establishes that neither the Patent Clause of the United States Constitution nor the

\(^{42}\) 416 US 470(1974)

\(^{43}\) Uniform Trade Secret Act with 1985 amendments drafted by the National Conference of Commissioners on Uniform State Laws, Annual Conference meeting in its 94th year in Minneapolis, Minnesota, August 2-9, 1985 with prefatory note and comments approved by the American Bar Association Baltimore, Maryland, February 11, 1986

\(^{44}\) This was before the TRIPS obligations of 20 years were brought in.
It is interesting to note that the raison d’être to have a uniform code on trade secret is not to enhance the remedy against unfair trade practices but instead to strengthen and bring in uniformity in trade secret protection across the states in the US to provide innovators the option to protect their innovations against the background of increased invalidations by courts.

Trade Secret protection as defined under TRIPS Article 39.2 aims at securing the confidential business and technical information from being stolen through either a breach of confidence or contract or through intervention of third parties. It does not try to address trade secret protection as an answer to court action of invalidation of patents and in this sense the prefatory note to the Uniform Trade Secret Act clearly brings out the divergence in the rationale behind UTSA vis-à-vis the reason in the TRIPS Agreement.

This brings us to the critical question of choices made by innovators and the impact it is likely to have on the flow of technical information in the society and therefore on the ecosystem for further technological development. As far as an individual inventor is concerned, trade secret protection has certain clear advantages over seeking patent protection—when a patent is granted, it is done so on the basis of the strength of the invention; and even if the grant is for twenty years from the date of filing, it is always amenable to challenge and invalidation- the prefatory note to the UTSA is a reflection of that issue. On the other hand trade secret is just any information or technical information that has been kept secret or undisclosed by the owner. Therefore, there is never any assessment of the strength of the secret for it to be amenable for protection.

Further, with patentability standards varying across countries, patent rights have become increasingly uncertain. This is especially when there is a movement in many countries to further raise the bar as far as the patentability criteria are concerned. In such a situation if the trade secret law is strengthened across the world, it will provide a viable option to inventors to keep their inventions secret. More importantly, a stronger trade secret law will ensure enhanced protection to tacit knowledge or know-how that may complement a patent, enabling the owner to protect his patented technology better-in fact even beyond the patent period.

From the society’s point of view, however, it would create an irreconcilable chasm between private benefits and societal welfare, thereby strike at the very core of the rationale for intellectual property protection. From India’s point of view, the Indian Patent Act, 1970 crafts a fine balance by rewarding important inventions while rejecting smaller and materially insignificant changes that do not meet the criteria as set by Section 3(d); it ensures that traditional knowledge or software per se is not patentable; sets an exceptional poise between the rights and responsibilities of the innovators by putting in place a robust disclosure
requirement and comprehensive provisions dealing with compulsory license. If stronger trade secret protection as sought by some countries (and this is not an unforeseen happening given the move to have a regulation that harmonizes trade secrets protection in EU, further attempts at modernizing the Uniform Trade Secret Act and with the USA seeking better protection in countries such as India and China) becomes the norm worldwide, innovators would be incentivized to adopt the route of trade secret protection. What would then happen to our well thought out provisions of the Indian Patent Act, 1970? Are they set to become superfluous in the long run? If so, then at what cost to the economy?

5. Conclusion

Although India does not have a dedicated law that addresses trade secret protection, yet the analysis of case laws brings out the rich and growing jurisprudence on this subject covering the vital themes of definition of trade secrets, substantive protection remedies and the associated issue of inevitable disclosure in courts. The legal regime has been dynamic to keep pace with the technological changes evident from the promulgation of the Information Technology Act, 2000 and its subsequent amendments that covers theft of confidential information through the electronic route and mandates stiff penalties, damages and imprisonment. The criminal remedies are also provided in serious offenses through Section 405-409 and 418 of the criminal procedure code.

While the trade secret regime as thought out under TRIPS was for protection against unfair competition, it is now increasingly being seen as an alternative to patent protection. Literature indicates that substantial part of inventions in the US do not translate into patents but are kept as secrets. The paper by Anton and Yao (2004) brings out that fact that most firms strategize on how much to disclose and parts that need to be kept a secret. They go on to explain that in situations of asymmetric information with patent not being an absolute right and the fact that disclosure can lead to imitation, companies will have incentives to keep inventions or certain crucial parts of that invention secret.

The stronger the trade secret law becomes, the incentives to keep technological improvements secret will also increase. Of course this action of the inventor might work in favour of the inventor and maximize his returns but on the contrary it can actually work against the society as without complete disclosure, the body of knowledge available to the society as a whole will not augment, thereby not only adversely affecting further technological advancements, but also disbalancing the objects and reasons behind different intellectual property rights.