SUPREMO AMICUS

VOLUME 27 | DECEMBER, 2021 ISSN 2456-9704

FUTURE OF TRADE SECRET IN INDIA: AN ANALYSIS OF THE EMERGING CHALLENGES IN THE DIGITAL ERA

By Bhaskar Mukherjee
Asst. Prof. of Law
Kingston Law College, Kingston Educational Institution

Arushi Sharma
Advocate, Delhi High Court

Abstract

Both the legal and business fraternity witnessed the importance of Trade Secrets and their value from time to time. Numerous International Conventions and Treaties uplifted the worth and utility of the legal protection of Trade Secrets. The US and European Union can be taken as an instance to show the importance of an existing legislation. On the other hand, India, who did not implement any strict TS laws, governs its Trade Secrets under various other legislations, enforcing both civil and criminal remedies.

Though common law plays a role in the Indian Judiciary but still it is non-binding. Gradually, technological advancements took place and the marketing and business processes shifted to an electronic base. Digital Marketing is the ultimate form of business in this hour. Research work establishes that Trade Secret is facing a lot of issues and problems while communicating on the digital platform. The current digital era has become bane for Trade Secret rather than becoming a boon.

The paper aims at addressing the issues in the digital era faced by the digital marketers and also to point out the loopholes in the current legal system while ensuring the protection of TS. It cannot be denied that a legislation governing TS is of urgent need, not only in the legal universe but also the economic growth is dependent on such implementation.

Table of Cases

List of Abbreviations

Abbreviation	Full Form
US	United States of America
TRIPS	Trade Related Aspects of Intellectual Property Rights
USPTO	United States Patent and Trademark Office
EPO	European Patent Office
TS	Trade Secret
GATT	General Agreement on Trade and Tariffs
NAFTA	North American Free Trade Agreement
USMCA	United States-Mexico-Canada Agreement
EU	European Union
UK	United Kingdom
Anr.	Another
Ors.	Others
V. / Vs.	Versus

Chapter 1

Introduction

Before initiating any business, there's a certain idea behind the functioning of the business. This idea can include questions like, 'what will help it move forward or facilitate its constant growth?' or 'what makes it unique and stand out as compared to the rest of the similar businesses in the same industry?' It is due to these reasons and more that any business owner initiates the foundation of a business and the impact of the same can be seen through a unique recipe, technology, result using the existing knowledge, process etc. which gives rise to the concept of Trade Secrets.

The reason behind protecting such Intellectual Property is multifaceted. Firstly, it protects the rights of the creator as also observed in other kinds of Intellectual Property and encourages more people by such protection. Secondly, it also provides infringement remedies and redressal mechanism in case of any breach of confidence or leaking of this confidential information without the authorization or consent of the owner and in case such consent is given as part of a necessary obligation arising out of any contract, then in case of the breach of trust that the owner puts forward while disclosing such information to the concerned party.

An improved connectivity across borders is the major identity of the 21st century. With ever changing technological advancements from basic antenna mobile phones to touch screen hi-tech ones which need a mere face ID to open, from desktop computers to tablets and so on, no one knows what the next decade of this century will introduce and the consumers are simply addicted to all kinds of tech devices too. In respect of a business, an entire digitization of the process involved including the emailing of every little detail of all activities in the business are merely a few examples of how the changes are introduced, accepted and incorporated with an ease.

However, with these changes, newer possibilities of threats and challenges have also emerged and the role of the judiciary is constantly evolving to accommodate such issues in hand. Such risks pose a greater difficulty in the case of absence of a proper legislation, in countries like India.

Research Problem Statement

When there's a law, there's always an issue that follows. This is because while on one hand such law is introduced merely to provide a solution to the existing problems, the rapidly changing society has varying needs after a point in time. In this way, the existing laws fail to offer solutions for the new problems and that's where research and surveys measuring the actual growth and implementation of such laws come useful. This research focuses on mainly two issues:

- ➔ The impact of lack of Trade Secret laws in India;
- ➔ Challenges posed by the recent lean towards digitization, especially in connection to COVID-19

While the first statement highlights the already existing issues that India faces, such impact is further enhanced with the present-day situation where many people are working from their homes globally due to a pandemic in 2020. This pandemic has not only led to many setbacks to several startups as well as small businesses but also hampered the growth of many multinationals. As per

a news article[1], around 12.2 Crore people in India lost their jobs during this period, out of which 75% belonged to the small trading concerns.

Those who retained their job portfolios had to work from home, thus involving a greater role of videoconferencing applications, for online meetings and discussing various crucial issues that concerned the day-to-day office activities. As such since there's no monitoring as to what data is collected or recorded by these applications, it wouldn't be surprising if the Cyber Security agency of the country declares them as 'unsafe' for use[2].

A country like India where there are no Trade Secret legislations in place is already vulnerable to such misuse and mishandling of secret data that is most crucial for any company and as such the threat has only increased with the new-age technologies and tech-development with respect to many websites and applications offering their services in return for a mere 'I agree' button which stipulates certain Terms and Conditions that most do not choose to read as a matter of ignorance.

This research highlights the key points as to what is meant by Trade Secret and the lack of an enactment for the same has various impacts, which shall be discussed in the chapters ahead.

Research Objectives

This research paper comprises of a comprehensive study conducted for certain reasons which are as follows:

1. To ascertain meaning of Trade Secret and its importance in India
2. To study the impact of gap created by the absence of such legislation
3. To know how other countries are operating in matters concerning Trade Secret
4. To analyse the challenges posed by the rapid advancement of technology and digitization
5. To study the Indian cases which relate to Trade Secret and the process with which they've been dealt with by the court so far
6. To be informed about the connection between Trade Secret and E-market

[1]Sumesh Nair, *Around 12.2 crore people lost their jobs: How Covid-19 will change job prospects and hiring in India*, India Today (Aug. 21, 2020, 02:17 PM), https://www.indiatoday.in/education-today/jobs-and-careers/story/around-12-2-crore-people-lost-their-jobs-how-covid-19-will-change-job-prospects-and-hiring-in-india-1713616-2020-08-21.

[2] *Zoom app vulnerable to cyber attacks, says CERT-India; issues advisory on safety measures*, Economic Times (Apr. 03, 2020, 08:52 AM), https://ciso.economictimes.indiatimes.com/news/zoom-app-vulnerable-to-cyber-attacks-says-cert-india-issues-advisory-on-safety-measures/74959554.

Methodology

In the process of writing this article, several sources were referred to, which include various journals, legal enactments, cases and conventions. The methodology adopted herein is that of a combination of Doctrinal and Analytical. On one hand, there are various laws and cases that form part of the primary source of data for this research to contribute for the doctrinal methodology while in the analytical approach, various aspects of such Indian laws have been studied and analysed in relation to the current challenges that the country faces in the form of technological advancements and upgradations.

Chapter 2

Data Collection

Data plays a vital role in providing a basis for any research problem. In this paper, data has been collected and categorised into two main heads, which are as follows:

Primary Sources:

This kind of data under the study includes various domestic laws and relevant case studies with respect to such laws. It also covers international conventions that concern our study. Such laws are mentioned in the list below:

Laws in US/UK/EU:

1. The Defend Trade Secrets Act (2016)
2. EU Directive 2016/943

International Conventions:

1. Paris Convention for the Protection of Industrial Property (Paris Convention, 1883)
2. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS 1994)
3. North American Free Trade Agreement (NAFTA 1994)
4. General Agreement on Trade and Tariffs (GATT 1948)

Domestic Laws:

1. Information Technology Act (2000)
2. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules (2011)
3. Information Technology (Information Security Practices and Procedures for Protected System) Rules (2018)
4. Information Technology (Intermediaries Guidelines) Rules (2011)
5. Indian Penal Code (1860)
6. Indian Contract Act (1872)
7. Copyright Act (1957)
8. Specific Relief Act (1963)

Secondary Sources:

These include blogs, articles, books and other write-ups by authors who have conducted a thorough research analysis in this concerning topic prior to this research paper. These mainly comprise of the following list:

Blogs and Journals:

1. IP Watchdog
2. SlideShare

3. The National Law Review
4. Lexology
5. Bar and Bench
6. The Practical Lawyer
7. Manupatra
8. Merchant Risk Council

Dictionaries:

1. Britannica

Chapter 3

Result and Discussion

As per the definition provided by USPTO,[3] a Trade Secret comprises an essential economic value which can either be potential or actual and it should not fall within the domain of the general public. Another important element to contribute to this definition, is a crucial value that such information must contain for others who have no legitimate access to such a secret and that the owner of such a secret has taken sufficient or 'reasonable' steps to protect the secrecy of such information. The main elements of the definition given above are integral to call any piece of information a 'Trade Secret' per se. This could be in any form, whether digital or physical and may include a recipe, a formula or a code that contributes to the owner's business in a significant way.

In the United States, the scope of Trade Secret is comprehensively covered by two Acts. First, the Economic Espionage Act of 1996 provides for a criminal liability under the second meaning of the term Economic Espionage, where any theft relating to a Trade Secret is punishable by either fines or imprisonment under the law. Second, the Defend Trade Secrets Act 2016 offers a further civil liability as against the offender and in this way, amends the provision of the Economic Espionage Act to include the same.

In general terms, under the US laws, protecting a Trade Secret is considered to be a complementary procedure for Patent protection. This is so because when a patent applicant discloses the full information regarding a certain invention, he/she also faces the risk of exposing their creation to the world, which is not known before such an application. Such risk is then covered under the scope of protection offered by the Trade Secret laws in that country and thus, is suitable for their nation.

On the other hand, when we look at the Indian scenario, the establishment of Official Secrets Act (1923) in the pre-independence era offers protection against espionage activities and was intended to punish those who spied on the British government, which were Indians in this case. However, this Act doesn't define the term 'secret' or 'trade secret' in any way and thus, can be considered to be redundant when it comes to the concept of Trade Secret as we know today. Another provision offered by the Information Technology Act 2000 relating to gaining access to any information without the authority of the owner of such information is punishable under the law with penalties or imprisonment depending on the specific scenario.

Cases such as *Fairfest Media Ltd v ITE Group PLC*[4], help us in ascertaining the position of Indian law with respect to the decisions taken by the court in matters of Non Disclosure Agreement (NDA). In this case, the parties had entered into an NDA before agreeing to the idea of a joint venture agreement. With the notion of entering into a Joint Venture soon, the appellant shared their confidential information with the defendants and with no such Joint Venture following this event and the expiry of such NDA within next 6 months of such sharing of information, the appellant

[3] *Trade secret policy*, USPTO (Feb 7, 2019 11:16 AM), https://www.uspto.gov/ip-policy/trade-secret-policy.

[4] (2015) 2 CHN Cal 704 (India)

stood at the chance of being taken undue advantage of by the defendant through such important information being shared already. The court ruled in favour of the appellant in this case and held that even though the parties were not bound by any agreement at the time, the defendant isn't supposed to make any use of such information for any competitive advantage therein.

As far as the Indian take on Trade Secrets is concerned, lack of legislation has caused the courts to interpret the term and related issues in the light of Indian Contract Act and deal with such cases by applying the principles of justice, equity and good conscience as also discussed under the common law system. This was highlighted in the case of *John Richard Brady and Ors. Vs. Chemical Process Equipment Pvt Ltd and Anr*[5].

In order to interpret the meaning of the term 'Trade Secret' in India, cases such as Bombay Dyeing and Manufacturing Co.Ltd. Vs.. Mehar Karan Singh[6] and Tata Motors and Anr. Vs. State of West Bengal[7]. Similarly in other cases, the Indian courts have given their own interpretation with the help of the existing laws in other fields.

So, how is it that having no legislation is causing prejudice when courts are able to decide on matters relating to Trade Secret? In order to understand this better and know the impact of such lack of legislation in India, let us first take a look at the international convention provisions and present laws in other countries concerning this issue.

The Common law System

The term 'common law' primarily consists of laws based on customs and usages.[8] This practice was initially followed by English courts centuries ago and is still an integral part of their legal regime till date. It also includes the judge-made law or precedents which help in guiding the further related cases in light of similar issues and thus shape the legal machinery in an indirect manner.

Since many laws in India have been established in the pre-independence era and some of which are still in force with amendments as per the changing times in Indian society, it is important to study the laws which are followed in other countries such as the United Kingdom. The legal system as provided by the British during colonial period is also known as the 'Common law system' and thus, has majorly contributed to Indian laws.

As per the current regime in the UK, the EU Trade Secrets Directive ((EU) 2016/943) and the Trade Secrets (Enforcement, etc) Regulations 2018 (SI 2018/597) are followed along with the common law principles of justice, equity and good conscience. Such directives and laws are also read with the provisions of Contract laws that provide for Non disclosure agreements between the parties and any breach thereof may cause serious injury to either parties. It is due to this reason that a comprehensive approach in terms of Trade Secret protection is used by the courts in the UK.

[5] (1987) AIR DEL 372 (India)

[6] (2010) 112 BomLR 375 (India)

[7] (2010) 6 SCC 243 (India)

[8] Mary Ann Glendon, *Common law*, Britannica (Oct. 30, 2020), https://www.britannica.com/topic/common-law.

All of such laws are also meant to be read in harmony and synchronization with each other and are not for replacing any definition or meaning mentioned in one by the other.

The definition provided by the EU directive adds more to the already existing definition of 'Trade Secret' under common law and is very similar to what is provided by the international Agreement on Trade Related aspects of Intellectual Property Rights (TRIPS)[9], which will be discussed later in detail. It includes that certain measures should have been taken by the owner of such a secret to protect the information contained therein and the secret should also have a commercial value. Additionally, it is also important to note that there's no bar as to what type of information can come under the purview of this Directive as applicable and adopted by the UK.

As stated under **Article 2**[10] of **EU Trade Secrets Directive ((EU) 2016/943)**

'trade secret' means information which meets all of the following requirements:

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

(b) it has commercial value because it is secret;

(c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;

While various factors have to be considered by the English courts when dealing with matters relating to Trade Secret laws such as the kind of information being discussed, employee's access to such information during the course of his/her employment and the nature of their work etc., it is also true that this comprehensive directive followed by the UK also provides for various exceptions under Article 5 which are as follows:

Member States shall ensure that an application for the measures, procedures and remedies provided for in this Directive is dismissed where the alleged acquisition, use or disclosure of the trade secret was carried out in any of the following cases:

(a) for exercising the right to freedom of expression and information as set out in the Charter, including respect for the freedom and pluralism of the media;

(b) for revealing misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest;

[9] *Trade Secrets*, WIPO, https://www.wipo.int/tradesecrets/en/.

[10] *Directive (Eu) 2016/943 Of The European Parliament And Of The Council,* EUR-Lex (Jun. 15, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943.

(c) disclosure by workers to their representatives as part of the legitimate exercise by those representatives of their functions in accordance with Union or national law, provided that such disclosure was necessary for that exercise;

(d) for the purpose of protecting a legitimate interest recognised by Union or national law.

Along with exclusively providing for remedies such as ex-parte injunction, preliminary injunction forfeiture of infringing goods etc, the said Directive also provides a Limitation period during which the aggrieved party can file a suit under Article 8. Despite the fact that something as crucial to the business as a Trade Secret would need a high level of protection, and can be said to be protected forever, it is also understood by the policy-makers that if such information loses its commercial importance in terms of economic value or may become obsolete in case it involves a specific technical know-how, the same can no longer be considered as a secret.

Yet, the Directive does not provide for a time-limit for the protection of Trade Secret and as long as it carries some commercial value and is kept a secret per se, it can call for the provisions under the said Directive. So, when we take a close look at the mentioned policy, its comprehensiveness is far more applaudable in terms of specificity and a crucial yet wholesome approach to the Trade Secret law.

International Arena

The international law does not carry the binding authority as strongly as the domestic laws do but the mere authority instilled in such international laws is deeply rooted in the free will of the States to be a member of such a community and thus gives birth to several treaties and conventions as we know today. It is after post World War II and Cold War that the need of an international uniformity, to prevent a further genocide in the name of wars, was observed and hence the United Nations was established, replacing its predecessor League of Nations.

As far as Trade Secrets are concerned, we see an enormous growth in the international treaties which are mentioned in the order of their Trade Secret discussion below:

- **Paris Convention for the Protection of Industrial Property 1883**: This treaty was signed in France (Paris) on March 20, 1883 for the purpose of providing protection to various industrial property and mentioned Trade marks, utility models, service marks, patents, geographical indications and industrial designs in its ambit of such protection. It also stated protection from unfair competition which makes it the first international treaty to include Trade Secret in the purview of its provisions.
  Among those states who were members to this convention were Brazil, Spain, Switzerland, Netherlands and Guatemala. Even though this convention mainly comprised clauses concerning National Treatment, a few common rules and Right to Priority, it was a major step towards a more globalized world where Intellectual Property was discussed and protected at large. It was administered by the World Intellectual Property Organization and is known for laying down some of the widest yet basic norms for Intellectual Property relating to industrial property mainly.

- **Trade Related Aspects of Intellectual Property Rights (TRIPS) 1995**: The establishment of World Trade Organisation provided for introducing a legal framework for the smooth functioning of trade relations between nations and avoids any conflict thereon. It was also because of the growing technological advancements and rapid urbanisation that most nations recognised the importance of this establishment as several countries have ratified the rules laid down under WTO in their domestic policies.

  As a result, member countries of the WTO have to abide by the underlying TRIPS agreement which forms a part of the policies under WTO. The idea was to promote a positive (protective) as well as negative (sanctioning in case of infringements) framework to protect the creations made out of human intellect and to reward those individuals who have put in their hard work and efforts in the same.

  According to **Article 39.2**[11], an exclusive provision for undisclosed information is protected under the purview of the TRIPS agreement. This article mentions that for an information to be eligible under the criteria for protection, it must be secret, and thus, reasonable steps must have been taken to maintain such secrecy. Even though the intention

[11] *Overview: the TRIPS Agreement*, WTO, https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

as laid down under the said article is not to treat such information as a form of property per se but it does make sure that such information be in possession of such a person with the possibility of preventing it from being misused by any third person in a way which can harm the true owner of the information. The phrase used in this article is 'manner contrary to honest commercial practices' has a broader connotation which involves breach of trust, and inducement of such breach as well.

At the same time, **Article 40**[12] of TRIPS provides for such laws as may be introduced by the member countries so as to protect the adverse effects on business and commercial activities as such non-disclosure of information may cause hindrances in proper transfer of technology. This article works as a supplementary provision to the clauses mentioned above and seeks to balance the overall trade activities.

- **North American Free Trade Agreement (NAFTA) 1994:** The North American Free Trade Agreement is an agreement between the north American countries signed by United States, Mexico and Canada in the year 1994 governing the trade relations between the member countries but superseded by the United States-Mexico-Canada Agreement (USMCA) signed in 2020. The original NAFTA was said to provide for the protection of Trade Secret in the member countries and defined Trade Secret as,

  - ➔ *'the information 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 that normally deal with the kind of information in question;*
  - ➔ *the information has actual or potential commercial value because it is secret; and*
  - ➔ *the person lawfully in control of the information has taken reasonable steps under the circumstances to keep it secret.'*[13]

  As per the agreement, it puts a mandate over the member countries to provide for protection of Trade Secrets against any unauthorized use and in case of any infringement, there should be a remedy in the form of injunctions and damages. In light of the said agreement and its implementation, Mexico has amended its Trade Secret laws to accommodate injunctions as a relief in the case of Trade Secrets.

  However, as per the USMCA, the protection provided for Trade Secrets is even stronger as it involves not only civil and criminal remedies but also for penalties exclusively for government officials in case of any unauthorized disclosure of such confidential

[12] *Id.*

[13] *North American Free Trade Agreement*, SICE, http://www.sice.oas.org/trade/nafta/chap-172.asp.

information along with specific judicial procedures to prevent leaking of such information during court proceedings[14].

- **General Agreement on Trade and Tariffs (GATT) 1948:** With the main objective of removing trade barriers such as tariffs to ensure a smooth flow of trade across borders, the General agreement on Trade and Tariffs was brought to existence in 1948. However, due to several complications and non-compliance issues the same was also rendered non-operational making way for the World Trade Organization in 1994 which was more suited to the needs of a rapidly changing world.

  Under the said GATT agreement, provision for protection of 'undisclosed information' clearly indicates the Trade Secret regime and prohibits an unauthorised use which facilitates malpractices in trading activities. Additionally, it also established a third-party liability if the same were either negligently or knowingly made use of such information which was said to be obtained in an unauthorized manner.

  Despite its redundancy, this provision in GATT helps in understanding the original timeline as to when the need for such protection was originally felt and put to firm laws across nations.

Role of USPTO and EPO

In the US, since the procedure for filing a Trade Secret is a complimentary procedure that accompanies the patent application, the United States Patent and Trademark Office is the main registering body in respect for the same. As per the guidelines set forth by the USPTO[15] on their official site, while filing for a patent, the applicant has to specifically mention such information that amounts to being a Trade Secret. It is not the duty of any of the officials to assume any piece of information mentioned in the application to be a Trade Secret per se. It is also clearly set out by the Office that in case of any plea under the Freedom of Information Act, such Trade Secret if found to be a secret after due consideration shall be withheld and the remaining contents of the patent application shall be made public for the sake of fulfilling the obligation as mentioned under the Freedom of Information Act.

A distinct mention of such disclaimers by the USPTO on their main website in accordance with the Patent laws[16] in the country sets an example of how official notifications should be laid out leaving no scope for any confusion in the future. It also paves way for putting a mandatory

[14] *UNITED STATES–MEXICO–CANADA TRADE FACT SHEET Modernizing NAFTA into a 21st Century Trade Agreement*, Office of the United States Trade Representative, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/fact-sheets/modernizing.

[15] *2760 Trade Secret, Confidential, and Protective Order Material [R-8.2012]*, USPTO (Jun. 25, 2020, 05:07 PM), https://www.uspto.gov/web/offices/pac/mpep/s2760.html.

[16] *Appendix L - Patent Laws*, USPTO (Jun. 25, 2020, 06:20 PM), https://www.uspto.gov/web/offices/pac/mpep/mpep-9015-appx-l.html#d0e303884.

obligation on the patent applicant to mark the scope of a Trade Secret well in advance in order to avoid getting such information out in the public in case any plea to disclose the same is made in the future as per the Freedom of Information Act of US.

Whether to prefer protection under Patent laws in the US or exclusively mention about the Trade Secret parts in the application is a choice solely dependent on the facts and circumstances of such Intellectual property. As often suggested by lawyers in the US, it is a matter of competitive advantage. In the sense that, if patenting an invention has more advantage for the owners, than withholding the information entirely under the Trade Secret regime, such that this disclosure is beneficial for the company/owner of the Intellectual property, then patent is the answer that they're looking for. For example, in the case of softwares, due to the Alice Corp. V. CLS Bank judgement, it is difficult to seek a patent for the same as per the decision given by the US Supreme Court.[17]

EPO

European Patent Office derives its powers from the establishment of European Patent Organization which came into effect through the signing of European Patent Convention (1973). The main aim behind such an establishment was to provide for a stronger cooperation amongst the countries in Europe with respect to granting patents. This convention paved the way for obtaining a patent in the majority of the European nations via a single patent application following a standard procedure provided under the Convention. This procedure avoided the hassle of filing in every such nation separately, saving both time and energy of the applicants. EPO, or European Patent Office is the one ensuring the smooth functioning of such procedure and thus exclusively focuses on patent applications.[18]

It is also to be understood that even in case the European Patent Organization grants a patent to any applicant, the said applicant still has to seek validation from the nations individually. The convention merely provides for a set procedure that seeks to strengthen the relations across Europe with respect to patents. Another important thing to note about this system is that a patent can be acquired outside of the European countries depending on the established connections between European Patent Organization and the other states.

As per European Patent Office, the term 'know how' is closely linked and hence can be understood in terms of Trade Secret protection in the European regime. According the guidelines mentioned, know-how relates to a piece of information which is known only to the owner of the information and is undocumented. It is also stated therein that without such information anyone else, other than the owner who is in possession of such information, may find it difficult or impossible to exploit the original idea behind it.

[17] Derek Handova, *The Business of IP: Choosing Between Patents and Trade Secrets*, IP Watchdog(May 25, 2016), https://www.ipwatchdog.com/2016/05/25/choosing-patents-and-trade-secrets/id=69368/.
[18] *European Patent Office (EPO)*, USPTO (Mar 27, 2020 03:14 PM), https://www.uspto.gov/learning-and-resources/pursuing-international-ip-protection/european-patent-office.

This said information can be commercially valuable and therefore can also be exclusivelyprotected under any agreement involving license(s). Even though it cannot be protected under theEPO rules, it is also important to note that if any part of such know how is to be patented, any exclusion of mentioning such know how in the application primarily also has the risk of invalidating such patent claim in the future, as a part has been left out in the application. Therefore,it is always advisable to consult a patent attorney regarding what exactly can/cannot be treated asa know-how.[19]

Impact of International precedents on Indian Judiciary

"The primary search must be for an objective and independent interpretation capable of accommodating the needs of a diversity of national legal systems."[20]

In light of the above statement, it is important to note that while a lack of legislation is the root of many problems faced by trade concerns in respect of Trade Secret protection in India, the contribution by indian judiciary stands at being of utmost importance in the same. The lack of such legislation is also the reason why India follows the Common law system while deciding cases related to Trade Secrets. The role played by precedents or judge-made law has evolved since the independence making it broader as also established by various landmark Constitutional cases such as Keshvananda Bharati V. Union of India[21] where the judiciary has interpreted the Constitutional text in a more inclusive sense.

In terms of Intellectual Property laws, it has always been the duty of Indian judiciary to interpret the cases concerning IPR in synchronicity with the international regimes set by TRIPS and WTO, to which India is a party. Henceforth, it goes without saying that when such new laws are introduced such as in the case of Patent Amendment 2005, they're also to be given more importance leaving the old laws redundant. Another notable difference is the setting up of new institutions in conformity with such changes in the legislations so as to accommodate a smooth functioning of the same.

For instance, in the case of *Diamond v. Chakraborthy*, the concept of 'novelty' was in question before the US Supreme Court and while different countries have their own interpretation of the same, it was held in this case that the bacteria created by Dr. Chakraborthy was a non-naturally existing one and is therefore a patentable subject matter having unique attributes, name and purpose.

In India, earlier right to property was a fundamental right enshrined in Article 19(1)(f) of the Constitution which was later repealed and added under Article 300-A which states that no person shall be deprived of property except by the authority of law. Hence, it is still considered as a constitutional right, though it is no longer a fundamental right. Accordingly, this Constitutional provision when read in light of intellectual property laws ensures a protection of the interest(s) of

[19] *Forms of IPR*, EPO (Mar. 18, 2016), https://www.epo.org/learning/materials/inventors-handbook/protection/ipr.html.

[20] Baltic Insurance Group v. Jordan Grand Prix Ltd. (1999) 1 All ER 289

[21] (1973) AIR SC 1461 (India)

the creator or inventor as against any infringement or duplicity by the general public without due authorisation and procedure provided under the law.

The main conflict in terms of Trade Secret arises when such procedures are not present in India as there is no law for the same. Similarly, in the usual scenario, the judiciary is required to interpret such laws in the ordinary course of its functions. However, in the case of Trade Secrets, the lack of precedents and the urgency in seeking relief on the parties' end, creates a pressure on the courts to decide upon issues with urgency. Another contributory factor is the amount involved in such cases. As protecting a Trade Secret is crucial for any business concern, the loss amount is as huge as the whole business going down as such confidential information forms the basis of the trading concern. Delay in such matters can also pose problems in establishing breach and presenting proof in the courts with respect to the same issues in hand. Due to these and other related reasons, the Courts have no option but to decide the cases with whatever laws exist in the country at present.

There have been instances such as in the case of *John Richard Brady And Ors. v. Chemical Process Equipments P. Ltd. and Anr.*[22], where despite an absence of contract the honourable court has awarded an injunctive relief as part of a wider interpretation of the contract laws.

In yet another important landmark judgement of *Diljeet Titus v. Alfred Adevare & Ors.*[23] it was held that the court has a certain responsibility of stopping a breach of confidence irrespective of whether any other right exists or not. This means that not only does the right to protect a Trade Secret originate from its owner's claim over such secret but more importantly it is stemmed in the mere nature of such confidential information which essentially puts anyone in possession of it under an obligation to keep it a secret throughout. This also affirms the fact that Trade Secrets are amongst the most important assets that come under the purview of Intellectual Property Rights as an entire business and the livelihood of those who work in such a trading concern depends on the sole secrecy of it.

Even though in some cases like that of *American Express Bank Ltd. v. Ms. Priya Puri*[24] the Court has laid down the definition of Trade Secret as 'a peculiar mode of business, which may comprise of a formulae, or a know how which is purely technical in nature and at the same time which is not in the public domain or commonly known to others', it is also important to consider instances where the Court had to strike down the possibility of the same knowledge being in the public domain. Such examples can be found in cases like *Anil Gupta and Anr. v. Mr. Kunal Dasgupta and Ors.*[25] where despite the disputed information being in the public domain, the honourable Court held that since by application of the plaintiff's brain, a different and unique result was obtained, such information amounts to be protected and an injunction was granted in this regard to prevent other parties from claiming or making unauthorized use of it.

Another important aspect when it comes to protecting one's Trade Secret comes into picture when the owner has to establish that such information was 'believed to be a Trade Secret' by nature.

[22] (1987) AIR Delhi 372 (India)
[23] (2006) 32 PTC Del 609 (India)
[24] (2006) III LLJ 540 Del (India)
[25] (2002) 97 DLT 257 (India)

This becomes difficult especially when there's a lack of evidence to support the same in the court of law. The same was iterated in the case of *Ambiance India Pvt. Ltd. V. Shri Naveen Jain*[26]. Even though this doesn't happen in the laws outside India due to a well-founded law in place to protect such information, Indian judiciary has to rely on the existing laws to protect the interest of the owners. The common law as applicable in India doesn't provide for such protection of information and thus, mostly the contractual obligations are questioned primarily in the Court.

A yet another commendable effort by the High Court of Bombay was made during the suit proceedings of *Bombay Dyeing and Manufacturing Co. Ltd. V. Mehar Karan Singh*[27]. In this case a basic criteria which is to be considered while deciding whether a piece of information falls under the Trade Secret regime or not was laid down. This criteria is as follows:

- The amount of money and/or effort spent in obtaining the said information;
- Duration of time others will have to spend to acquire such information;
- The value that such piece of information holds for the owner as against those who may take undue advantage of the same;
- How much and in what manner is the said information available to those working within the trading concern;
- The number of precautions taken by the owner of such information to prevent others from accessing such information and;
- The extent to which those working outside the business are aware of the information

Despite these proper guidelines, other courts of the same or superior authority level are not bound to follow the same criteria as this is not a part of any legislation and hence, this may or may not be used for any further cases in this regard.

Another drawback for not having a legislation in place for Trade Secrets, is the establishment of the burden of proof. As per the Indian Evidence Act 1870, it lies on the person asserting a claim and hence the one who will lose if no evidence is provided by either parties. In other words, in the case of Trade Secrets, the one claiming the ownership and redressal for the infringement will also have to provide evidence that such breach has taken place in the first place. The main obstacle is that there are many cases where such information is not to be disclosed in the suit openly, it becomes all the more difficult to prove the breach. This also happens where the information was protected via other modes which are stolen or the existence of the same cannot be proven otherwise such as a piece of paper that may go missing from a locker.

In the case of *Beyond Dreams Pvt. Ltd. & Ors. V. Zee Entertainment and Anr.*[28], it was laid down that to prove misappropriation of a confidential information or know how, the owner of such information has to prove the following:

[26] (2005) 122 DLT 421 (India)
[27] (2010) 112 BomLR 375 (India)
[28] (2016) 5 Bom CR 266 (India)

- There has been a threat to use such information or an unauthorised use of such information has already taken place which is causing harm to the aggrieved party;
- The owner took reasonable steps to ensure the secrecy of such information and that such information was only transferred when the owner was under a contractual obligation;
- By no means the said information was in the public domain or easily accessible to anyone and was therefore a secret per se.

In cases where a prima facie case has been established by the plaintiff and the plaintiff would suffer immensely if an injunction is not granted at the earliest, it is observed that the Courts have usually granted an injunctive relief in favour of the aggrieved party having proven their cause sufficiently at the initial or final stage. The discretion is however, exercised by the courts and varies from case to case. This was also affirmed in the case of *Gujarat Bottling Co. Ltd. V. Coca Cola Co.*[29]

A similar trend has also been observed in the cases outside of India where the US Courts also believe that a Trade Secret loses its essence as soon it goes into the public domain or is disclosed to anyone outside the trading concern. The case of *State ex rel. Lucas County Board of Commissioner v/s. Ohio Environmental Protection Agency*[30] confirms this about Trade Secret laws in the US.

Amongst the most crucial rules laid down by the courts in regard to Trade Secrets is by relying on the Springboard doctrine. According to this doctrine, any person who has acquired any piece of confidential information shall not use such confidence put forward by the owner of such information as a springboard to conduct any activities which are destructive for the rights of the owner of such information and can possibly cause harm to the trading concern of the owner. This springboard stays intact even when such information gets published or goes into the public domain and can be accessed by any person. This valuable landmark doctrine have been reiterated in various cases such as Precision Engineers v. Delhi Jal Board[31], Ratna Sagar Pvt. Ltd. v. Trisea Publications[32] and the famous Michael Heath Nathan Johnson v. Subhash Chandra And Ors.[33].

[29] (1995) 5 SCC 545 (India)
[30] 88 Ohio St.3d 166, 174 (2000)
[31] (2003) 103 DLT 129 (India)
[32] (1996) 64 DLT 539 (India)
[33] (1967) AIR SC 878 (India)

Chapter 4

The Emerging Digital Era And Challenges

Even though the 20th century has witnessed a remarkable change and a gradual shift in the paradigm of trade and commerce with countries like India opening their gates to the Western world during the 1990s with Globalization, Privatisation and Liberalisation policies, the 21st century differs in many ways to the previous era. According to a report by International Telecommunication Union[34]Digital advancements have beaten every previous record of growth in history with population numbers of the developing nations reaching 50 per cent in a mere two decades. There are various reasons that have caused this spike in life expectancy ratio and contributed to a healthier living conditions as witnessed in the earlier time periods. As per UN[35], such supportive factors include access to trade and public services, better connectivity through an improvised infrastructure and a more efficient health sector with the inclusion of AI or Artificial Intelligence technologies that are helping save more lives.

However, with the rapidly changing as well as growing technology sector, the traditional methods of conducting business have also changed. The introduction of advanced and structured technology has paved the way for reduced cost of transactions across the borders thereby, enhancing trade activities and expansion of several multinational corporations or MNCs. On one hand, the scope for small businesses has increased through market platforms such as Amazon, eBay and Flipkart, enabling them to reach a large number of people and other marketing benefits, the risk that come with such advancements are equally greater too.

The changed methods of businesses across borders have kept the good old shipment container process intact while everything from viewing the products though videos on social media pages, tracking the orders through RFID codes online and payment via numerous vendor websites have emerged in the last decade. This is more visible in developing countries like India.

The growing concern for businesses, especially the small scale traders and startups is the complete digitization of data with large amounts of information stored in the form of CDs, memory sticks, USBs and other digital devices. This handy technology on one hand makes it easy to store large data files and also helps in categorising files on the basis of their need and access to the employees working inside a company, on the other hand it also makes it equally smooth for any competitor to gain access to any crucial information that have been stored via the same company network that any decent hacker can get through. Indeed, it is possible to track digital trails to catch such spies but that's not the case that happens all the time. Sometimes, there are no trails while on other occasions, many businesses cannot simply afford to track them due to limited investment and capital.

[34] *ICT Facts and Figures 2017*, ITU, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf.

[35] *The Impact Of Digital Technologies*, United Nations, https://www.un.org/en/un75/impact-digital-technologies.

In countries like US, laws such as the Computer Fraud and Abuse Act and Economic Espionage Act and Computer Fraud and Abuse Act have provided well-grounded remedies to Trade Secret owners who have been wronged and also offer initial warning signs in case of any misappropriation of such confidential information which is deemed crucial for a business.

Some of the main challenges as faced by various businesses worldwide are as follows:

1. Lack of awareness about online strategies: In many developing countries like India, there has been lack of awareness as to how such confidential information of any business can be easily accessed by anyone from a different country or region online and how the same can be protected and what all necessary means are required to protect such information.
2. Lack of awareness about the laws: India is amongst those nations which do not have a Trade Secret legislation and the awareness regarding the same is also lacking. There are various businesses who are not aware of the value of a specific information which should be confidential and not known to even the employees of the business in order to protect the uniqueness or smooth functioning of the same.
3. Videoconferencing lacunas: Despite an IT Act in place, there's still no guarantee that such breach of confidential information imparted through bond of trust to the employees cannot be accessed by third parties who offer a platform for the video conferences betweenthe employees of a company or business. According to a news report[36], applications like ZOOM which is amongst the most common apps that were used in the recent pandemic in 2020, contain a security bug responsible for leaking people's email addresses and pictures and in some cases have also allowed strangers to be added to a meeting. This not only endangers the confidential matters of a company but also invades the privacy of an individual.
4. Online payment portal glitches: While payments through third party vendors has facilitated the growth of businesses across borders who can now avoid the hassle of maintaining huge payment records and gateways, the same can also amount to fraud and misappropriation in various cases. According to a recent report in 2019[37]online payment fraud has cost businesses around the globe approximately 1.8 % of their total revenue. This is a growing issue in terms of Trade Secrets for business as such revenue loss can hamper the growth of their business thereby putting the confidential information in grave danger through such frauds.
5. Metadata issues: There are various fields associated with a single storage file or means of communicating or transferring data online. One such example to understand this is Microsoft Outlook[38]. Usually, any reader or composer of an email focuses on mainly a few

[36] *Users' email ID, photos may have been leaked on Zoom*, The Times Of India (Apr. 1, 2020, 10:50 AM), https://timesofindia.indiatimes.com/gadgets-news/users-email-id-photos-may-have-been-leaked-on-zoom/articleshow/74924698.cms.

[37] *2019 MRC Global Fraud Survey Results*, Merchant Risk Council, https://merchantriskcouncil.org/resource-center/surveys/2019/2019-mrc-global-fraud-survey-results.

[38] Guriqbal Singh Jaiya, *Protecting Trade Secrets: Challenges in the Digital Environment*, WIPO (May 21, 2008), https://www.wipo.int/edocs/mdocs/sme/en/wipo_smes_cgy_10/wipo_smes_cgy_10_ref_theme06_01.pdf.

fields such as 'To', 'From', 'Subject', and the main body of content, however, such mails comprise of 100 data fields which can also pose a serious threat to any business by exchanging such information falling within the purview of confidentiality.

6. Increased Cost: In order to protect the businesses and monitor any ongoing exchange of information between the employees and an outsider or even amongst the employees, the management can increase the surveillance through monitoring and constant upgradation of the devices used in offices such as desktops, laptops etc. Any hiring of a specialised staff in this regard or an e-security personnel will also add to the costs incurred by the businesses.
7. Knowledge diffusion: There's only a limit to which employees' interaction with other fellow colleagues can be monitored and hence diffusion of such knowledge may also comprise of imparting details about any confidential information which may cause serious prejudice to business per se. A famous example of Coca Cola's case in 2006 is a firm affirmation of this issue. In this case, three employees of the Coca Cola company were initially charged with selling the secret recipe of Coca Cola drink to the rival company of Pepsi[39].
8. Multiple storage issues: There are many people who a unaware that by simply clicking on the 'delete' button, does not erase the whole existence of the file per se. Instances showthat many files can be easily retrieved even after they were said to be deleted and thus, in this way, any secret information which is stored in more places than one and later deletedin order to prevent its misappropriation can also make the situation worse. For instance, the trendy application of WhatsApp has an automatic backup feature which stores the dataof existing chats, media files and call logs in the server every day unless it is manually changed in the settings. There have also been various claims and news reports regarding this app leaking data to big multinationals like Google[40].

[39] AP, *Ex-Coca-Cola Worker Sentenced to 8 Years in Trade Secrets Case*, CNBC (May 23, 2007, 01:15 PM), https://www.cnbc.com/id/18824080.

[40] Ankita Chakravarti, *WhatsApp may have leaked your number on Google, claims cybersecurity researcher*, India Today (Jun. 9, 2020, 01:30 PM), https://www.indiatoday.in/technology/features/story/whatsapp-may-have-leaked-your-number-on-google-claims-cybersecurity-researcher-1687139-2020-06-09.

Chapter 5

Trade Secret and E-market

Trade Secret and E-marketing

A trade secret is practically something which is secret and which gives meaning to its owners lists. Technical and scientific material is protected as trade secrets, such as formulae, manufacture procedures and requirements, designs, programming codes, etc. The trade secret can include both trade as well as financial secrets. The identities of custodians, price records, marketing and business plans, the internal cost system, supply agreements, as well as other related, non-public information may be covered by consumers who are purchasing expectations and specifications, the ingredient recipe for a specific product.

E-marketing deals with such aspects as covered by Trade Secret protection like software source code that exposes the software's algorithms and uniqueness or any secret production method or process which gives us some advantage (lower cost, more attractive product, greater efficiency, marketing competitiveness).

As with cyber crimes, it is of paramount importance and interest to safeguard our business secrets and other proprietary knowledge. This includes all the knowledge that we use for running our company that we deem sufficiently valuable and secret that enables us to compete. Brand specifications, consumer lists, pricing predictions and even other forms of information may be a trade secret in the field of E-Marketing.

We need to develop procedures to protect our trade secrets after we complete an audit. They are as follows:

It must be made sure that everyone who sees a specific businessperson’s confidential data knows that it is a secret. Inform associates, clients, vendors and staff that the content is classified, exposed to trade information. It is to be ensured that without the written consent of the owner of such confidential information, the employees agree not to use such information against the primary company. An important part comes into picture when the same is to be written; and once these documents are signed, they will be legally binding. The records should be marked as "Confidential."[41]

Physical defence enforcement methods must also be included in a business concern and these are as follows:

- Putting up "No Intrusion" signs, building fences, locking exits and hiring security guards to keep such information safely in a locker. Secrets should be locked up with effective passcodes known only to the owner.

[41] Shakun Soin, E- Marketing (Jul. 10, 2018), SlideShare, https://www.slideshare.net/ShakunSoinTaneja/e-marketing-105120000.

- Using identity badges for employees and visitors to monitor access to the business. Guidelines should be set that require employees to sign confidential papers.

- Login configuration should always be maintained. They are intended for use in accessing printers, copiers, fax machines and other machines for the copying or transmission of secrets.

- Measures must be taken to prevent the exiting employees from imparting the same knowledge even after when they leave. Before returning to their workplaces, sensitive materials should be retrieved from the discharged workers' offices and it is also important to get them to sign before they go.

Issues and Drawbacks : E- Marketing

Keeping in mind the current Pandemic it is quite established that to maintain covid protocols, social distancing must be followed at any cost. If we witness the Contract market, we can see that the traditional way of executing contracts has been shifted to e-contracts. In the field of Trade Secret, the Digital Marketers always indulged in sharing information digitally, more so in the current period. While communicating with the receiver of information a digital platform is always required, which acts as a medium to transfer the information.

A major issue that surfaces in this field is hacking. Information that costs around millions are being hunted by cyber criminals on a daily basis. So the loophole is that even though the sender and the receiver are maintaining all the necessary requirements to execute the transfer of know-how, like NDA (Non-Disclosure Agreements) and other legal formalities and even though both the parties abide by the said contract, yet somehow the information gets leaked.

We cannot deny the technological shift that has taken place and has affected the lives of all, both in a positive and a negative way. With the help of E-marketing, the information is being transferred in the blink of an eye. In the same manner, they are getting hacked or leaked. It becomes very difficult to hunt the cyber criminals down. The four most important pillars of Trade Secret are : originality, commercially valuable information, non-existence in the public domain, reasonable efforts to maintain its confidentiality. Due to the negative impact of e-marketing the fourth pillar gets hampered.

The presence of the Information Technology Act ensures the protection of information against a breach by a body corporate, or any person under a contract. Therefore if there is a breach of contract in the field of trade secret, then IT Act will ensure penalties, but the loophole that has been discussed earlier cannot be solved through this said Act. Only a concrete legislation can help the IP of Trade Secret survive from this issue.

Solutions to the issues faced by Marketers while executing Trade Secret digitally

Digital marketing should understand how important business properties are, such as trade secrets, proprietary documents, copyright and patents can and should be protected. In general, trade secrets include material, processes or commercial devices which are handled confidentially and which are unknown or not publicly disclosed. Commercial confidentiality conflicts also arise in client dealings and business plans.

In accordance with, but not limited to, the provisions of the Trade Secrets Act, comprehensive secrecy, non-disclosure and computer/data access arrangements should be enforced. Such arrangements should provide specific terms and limitations on data usage and the immediate return on cessation of jobs of sensitive information.

Commercial secrets should be factually correct, with password security and protected. Only those people who have a genuine reason for requirements in their work should have access to the said information. The downloading of proprietary applications and material on handheld devices without proper written authorisation should be specifically restricted to employees. Employees approved with such access to the confidential information granted should be mentioned in records immediately after the specified work has been done. Records hould be kept for every access to such information.

If the protection of trade secrets and the measures for privacy are not implemented properly, through the use of confidentiality clauses and other laws, the right to classify the property as a trade secret may be lost. Such security and confidentiality arrangements should be necessary for all sectors, from lower staff to vendors, consultants, top management groups, and other third parties with access to business secrets. Such secrecy agreements should be necessary to maintain confidentiality.

A trade-secret conformity officer should be appointed to implement confidentiality enforcement programmes. The appointed officer shall ensure that its legal responsibilities to protect corporate secrets are regularly notified to employees. Necessary written communications should often be conducted to remind staff about their lawful continuity and include the return of all records on ownership.[42]

[42] *How Digital Marketers Can Protect Their Corporate Trade Secrets*, The National Law Review (Nov. 6, 2018), https://www.natlawreview.com/article/how-digital-marketers-can-protect-their-corporate-trade-secrets.

Chapter 6

Alternate to Trade Secret Law in India

Primarily, the cases have to be decided based on the principles of Justice, Equity and good conscience as in the case of any dispute where no relevant law or precedent exists.

In the case of any leak of information when it comes to Trade Secrets, it is also an issue of breach of trust and where a contract such as a non-disclosure agreement is agreed between the parties, it becomes a matter of Contract Act. To avoid any further misinformation, Indian courts have established three main categories for interpreting such disputes where such confidential information is misappropriated[43]. These are as follows:

a) In the case of a license agreed between the parties, where one party is under the obligation to maintain the confidentiality of such information;
b) In the case of a an employment, where the employee was trusted with such private and confidential information and he failed to maintain its secrecy;
c) In the case of a deliberate act by a non-authorized person to acquire the said information from the one who is in charge of keeping it confidential.

In all three cases, the intention of the accused party plays an important role along with the said act of misappropriation as if it is established to be mala fide.

Information Technology Act, 2000

Although India has no clear business secrecy rule, Indian courts maintain trade secrets under different legislation, including contract law, copyright law, equity principles and – at times – common law infringement measures (which in effect amounts to a breach of contractual obligation). Section 72 of the Indian Contract Act 1872, while restricted to electronic documents, offers such safeguards as well.

The solutions for the trade secrets owners through various existing Indian legislations are:

An order to prohibit the revealing of a trade secret by a licensee, employee, seller or another party; to include reimbursement of any classified and sensitive information and to compensate for all damages caused by the disclosure of trade secrets.

Contract Law

In India, an individual may be bound by a contract, which forbids the disclosure of confidential information.

However, the court continued to appeal for a more just jurisdiction and an injunction in the absence of a contract in *John Richard Brady v Chemical Process Equipments Pvt Ltd*[44]. The complainant

[43] Saltman Engineering Co Ltd vs. Campbell Engineering Co Ltd., (1948) 65 RPC 203.

[44] (1987) AIR Delhi 372 (India).

had invented a processing device for fodder and wanted to provide the defendant with thermal panels for indigenous production of the same. The complainant shared with the defendant technical materials, basic information about how, sketches and requirements for the fodder processing machine. The parties concluded an agreement to provide thermal specialist panels; however, the plaintiffs subsequently found that the accused could not supply the required thermal panels and did not order the purchase. The complainant sent a complaint for misappropriation of the know-how, drawings, sketches and requirements that the respondent had been informed of, after learning of the defendant's own manufacturing unit on fodder.

Law on Copyright

In certain cases, customer knowledge has been recognised by judges, as copyrightable content, in the form of databases.

In order to assess market profitability and consumer behaviour or to just retain an inventory of products, companies constantly gather data, organise it in a systematic or methodical manner for the electronic access. Databases are therefore a valuable tool for companies to operate smoothly and to prepare for their future growth. Copyright law protects these databases. Under section 2(o), compilations like computer databases are described as literary works under Copyright Act 1957.

In *Govindan v Gopalakrishna*[45], concerning a compilation, the originality was considered invalid, but is still covered by statute. Therefore, no group can even in such works rob or seize the outcome of other knowledge, talents or jobs.

The current legal status requires all efforts, industries, or expenses to produce works that are copyrightable, but only certain works can be protected which may be unique in nature; and require a certain literary effort.[46]

Indian Penal Code

Under certain clauses of the Indian Penal Code, 1860, a person that violates the trade secret can be punished. In the event of a malicious misappropriation of information, exchanged for gainful motive, for instance, a person in violation could be charged under section 403 of the code. Similarly, an individual can also, for the purposes of transmitting the information confidentially to an unknown third person and/or other than to whom it was entrusted under the contract, be charged under Section 405 or Section 408 of the Criminal Procedure Code.

It is important to mention here that motive is a necessary precondition for proceeding under the Code. However, although the civil nature relief is available under the Contract Act and various sections of the IT Act, in that case the motive is not a precondition.

[45] (1955) AIR Mad 391 (India).

[46] Ranjan Narula & Rachna Bakhru, *Protecting trade secrets in India*, Lexology (May 1, 2018), https://www.lexology.com/library/detail.aspx?g=c83e8a6c-a02e-44ba-8723-94087d2e5e20.

Specific Relief Act, 1963

The supplier can contact the jurisdictional civil court to request a prohibitory injunction against that individual in accordance with section 38 of the Specific Relief Act of 1963 in the cases, where the supplier of the information is in violation of the confidentiality arrangement by the receipt of the information.

Civil Procedure Code, 1908

A party can also apply to issue a temporary interdictory injunction in accordance with CPC Orders 39, Rule 1 & 2, before the interdict appeal is eventually heard and a decree has been announced by the Court. However, where the judgment-debtor disobeys the above prohibition decree, disclosing the secured sensitive data in whole or in part, a person can be subject to proceedings under Order 21, Rule 32 of the CPC, in which a person is subject to civil detention or property attachment or both. In the same context, Rule 2-A of the CPC can be brought against a party for the breach of the temporary injunction under Order 39. Furthermore, if a person violates the provisional or final prohibitive decree of the court, it may prosecute that person in accordance with the Controversy of the Courts Act of 1971.[47]

[47] Pareekshit Bishnoi, *Breach of confidentiality maintenance covenants amid 'work from home' during COVID-19 lockdown: Concerns and remedies*, Bar and Bench, (Apr. 21, 2020, 06:00 PM), https://www.barandbench.com/columns/breach-of-confidentiality-maintenance-covenants-amid-covid-19-concerns-and-remedies.

Chapter 7

Need for a Trade Secret Legislation

From all the above legislations it is clear that to protect one single IP there is an urgency of more than four to five legislations and various disperse remedies. A lack of consolidated Trade Secret legislation brings forward various issues. One of the most challenging issues that tags along is the ambiguity. Which law to implement and which not. Although the Indian Judiciary with the help of common law protects the existence of Trade Secret in India, it creates a lot of problems like delayed justice and misinterpretation.

The organisations, in the current scenario, are attempting the use of patent, copyright, label etc. to protect intellectual property. But the statute does not replace trade confidentiality alone as certain clauses can only be tackled through commercial secrecy. Trade secret is really relevant for a developing nation like India because it has a strategic advantage. Common law protects trade secrets in India, and where we have no clear law that governs a particular subject, we still find it difficult to achieve fair justice. There are different procedures inside organisations to deal with privacy concerns, but there are also huge instances of informa ion theft, which can be a disgrace to workers or something. The fact that foreign corporations operate globally, which means that they must comply with the respective laws, makes a trade secret legislation important for India. In the absence of these laws certain corporations fail to operate in a given region, so a separate Trade Secret act in India is urgently needed.[48]

The preservation of trade secrets is very important because it facilitates creativity and supports business ethics, and because it promotes equal competition in the industry, it is also vital to a company's development. If the framework for protections is sufficient so more transparent trading in transactions will result and international investment and trade will definitely be increased. As the patenting of an invention cannot be patented due to the efficient regime or process, the burden of patent lawsuits can be less covered under trade secrets laws. Moreover, no breach of the basic right to privacy would occur as a result of the successful regime.

There is no substantive law or enforcement regime for trade secrets in India, although Article 27 of the regime offers legal remedies to some extent. It limits the disclosure of details he obtained during his employment. Once more, though, the opinions of the courts on this subject are not universal. There is no criminal responsibility clause in India unlike the United States.

A transparent and definitive strategy about the security of business secrets is also essential for the protection of commercial secrets. In order to tackle the issue of unfair competition, a Sui Generis system provided for by Article 39 of the TRIPS and by Article 10 bis of the Paris Convention is needed. In order to eliminate ambiguity with respect to trade secrets, India is obliged to adopt comprehensible rules and regulations as part of TRIPS.

[48] Brijendra Singh, Shalini Agarwall, and Karishma Rai, *Need for separate Trade Secret Act with required Law*, The Practical Lawyer, http://www.supremecourtcases.com/index2.php?option=com_content&itemid=1&do_pdf=1&id=24329.

In addition, Indian laws on civil and criminal liability can also be implemented in India, according to the 1996, Uniform Trade Secrets Act in the USA. In the United States, the law allows for civil and criminal liabilities under one single consolidated legislation.

Efficient and strict action should be taken to ensure the birth of a robust regulation that addresses liabilities for infringers of all civil and criminal matters, whilst bearing in mind the National Innovation Bill of 2008.[49].

[49] Ravindra Chaba & Shyam Sundar Chaba, *Inadequacy of the Trade Secret's Protection laws in India and Legal Regime Existing in U.S.*, Manupatra, http://www.manupatra.com/roundup/369/Articles/Inadequacy.pdf.

Chapter 8

Conclusion and Suggestions

There are various conventions as mentioned in the above chapters which govern the regime of Trade Secrets internationally and thus establish the importance of its protection as well. As also evident from the examples discussed in the article, various countries have succeeded in protecting the business concerns with respect to Trade Secret and have provided a proper mechanism to seek redressal in case of any infringement. Even though India is a party to TRIPS agreement and has abided by other mandates provided in the agreement, it still hasn't been able to offer a Trade Secret protection and lags behind not only in terms of providing protection to the interests of Trade Secret owners but also in spreading awareness with respect to this branch of Intellectual Property.

Little has been done so far in terms of a draft bill which caters to the needs of Trade Secret protection and yet a ray of hope can be seen in the judicial pronouncements discussed above where judges have taken references from the existing laws of Copyright Act, Contract Act, Specific Relief Act, Indian Penal Code and so on to prevent any further misappropriation and awarding recovery of damages caused to the owner of such information. However, there's no denying that the work of the judiciary will become easier with legislation in place.

So far, such void created by non-existence of a legislation for Trade Secret in India was difficult yet still manageable but with the rapid leap towards a globalised world and technology transfer, a greater risk is certainly not too distant in future. As also evident from the examples of Zoom and WhatsApp applications, a breach of confidentiality awaits at a snap of a finger and a mere 'I Agree' button at the renewal of policy guidelines by such apps is hardly ever seen or rather properly read by the users.

Business practices are increasingly relying on e-marketing, and a full digitization of the work makes it even easier for the hackers and those competitors who invest in gaining undue advantage from others. The risk is even greater when there is no digital trail left by such hacking practices at an expert level, whether occurring within the country or from outside, leaving the owner of Trade Secrets even more vulnerable than ever. In the absence of a proper proof against the hacker or competitor, no prima facie case can be established which further leads to losses for the business owners while simultaneously discouraging others to follow the same trend in fear of no protection with regard to their Trade Secrets.

It is therefore an urgent need of the hour where only a legislation can provide for a framework wherein stringent penalties and wider definitions can cover all facets of the issues that are discussed in the paper.

Despite various claims that the trading concerns have suffered in the past and continue to be at a loss with no legislation in place for protecting their Trade Secrets, the threats are even greater with the digitizing world's rapid growth. On one hand, where protecting an individual's privacy in these times is also a concern for the cyber laws and an increased mandate in the criminal provisions is required for the same, it is also necessary to provide for various clauses, definitions, authorities

and the like to keep a check on this crucial Intellectual Property that is committed to boost the economy in the long run.

Nevertheless, these shortcomings can be overcome by a few suggestions as mentioned in the next chapter.

In order to combat the challenges posed by the emerging trends in the digital world, a Trade Secret protection has become an urgent need of the hour. Here are a few recommendations for the same:

1. **A consolidated legislation:** Seeking help and references of 6-7 legislations is not only a tedious task but also paves the way for various drawbacks. For example, there is no specific authority to register, maintain a record or provide for a structural framework for registering Trade Secrets. A legislation will not only facilitate a proper mechanism and protect the interest of a crucial Intellectual Property like Trade Secret but also provide for concrete support against any infringement from across the borders too. What happened with the Neem and Haldi cases in the case of Traditional knowledge is a good example to establish the fact that in the absence of a legislation, no amount of proof is sufficient and litigation for the same becomes a long battle. This consolidated l gislation must include:
    a. **Definitions:** 'Trade Secret' as well as other related important terms such as 'breach', 'unauthorized user' etc must be included and interpreted in a wide sense so as to avoid any narrow escape by those who wish to infringe such a right.
    b. **Penal provisions:** Such penalties as incorporated in the said legislation should be strict and should impose heavy fines to those who are found guilty in order to discourage any further misappropriation by individuals or companies who look forward to such malpractices.
    c. **Term of protection:** Since Trade Secrets form an integral part of the business and are considered to be the foundation of the establishments of several well-known brands such as McDonald's and KFC, it is important to provide for a lifetime protection to Trade Secrets as evident in the laws of other countries.
    d. **Mechanism for registration:** This should provide for a proper authority facilitating for the registration process of such Trade Secrets and at the same time, not require full disclosure of such information as it is crucial for the business to function.

2. **Awareness programs:** Conducting seminars, workshops, posting advertisements, and related banners across the country are some of the ways in which the government can educate and spread awareness about Trade Secret in various marketing companies and thus enable the growth of Trade Secrets at large. Letting the citizens and business persons know about the value of keeping their recipe or know-how a secret is as important as having legislation in the first place.

3. **The Personal Data Protection Bill:** The already existing Personal Data Protection Bill[50] which was introduced in the parliament in the year 2019 should be speedily analysed and enacted with amendments as the lawmakers deem fit in order to facilitate for the breach of confidence in cases of data transfers online. It is yet another powerful tool to safeguard the interests of not only the owner of Trade Secrets but also the citizens of the country as a whole and provide protection against the hackers and illegit Terms and Conditions posed by the apps in general.

4. **Specific internet platforms:** An appropriate choice of internet platforms must be made to ensure a secured transfer of know-how and confidential information in the case of Trade Secrets can enable a better communication between parties who are under obligation to disclose such information either via a license agreement or an employment agreement.

5. **Economic growth reasons:** Big multinationals like KFC and Coca Cola still have the means to afford a stronger and firmer protection not only because their origin countries have laws in this regard but also because they can simply afford to. However, there are various Indian companies which have their unique recipes, technologies and processes who cannot afford to provide a strong protection to their Trade Secrets in the similar fashion. Arrangements should be made in the form of a special protection to help these businesses access the litigation process at a lower cost which they can afford. These small and medium scale companies have an equally good contribution to boost the Intellectual Property sector and thus the whole of Indian Economic Market as a result.

[50] The Personal Data Protection Bill, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

Bibliography

Legislations:

1. The Personal Data Protection Bill, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

2. Directive (Eu) 2016/943 Of The European Parliament And Of The Council, EUR-Lex (Jun. 15, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943.

3. Indian Copyright Act, 1957

4. Civil Procedure Code, 1908

5. Specific Relief Act, 1963

6. Indian Penal Code, 1860

7. Indian Contract Act, 1872

8. Information Technology Act, 2000

9. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules (2011)

10. Information Technology (Information Security Practices and Procedures for Protected System) Rules (2018)

11. Information Technology (Intermediaries Guidelines) Rules (2011)

News Articles:

12. Sumesh Nair, Around 12.2 crore people lost their jobs: How Covid-19 will change job prospects and hiring in India, India Today (Aug. 21, 2020, 02:17 PM), https://www.indiatoday.in/education-today/jobs-and-careers/story/around-12-2-crore-people-lost-their-jobs-how-covid-19-will-change-job-prospects-and-hiring-in-india-1713616-2020-08-21.

13. Zoom app vulnerable to cyber attacks, says CERT-India; issues advisory on safety measures, Economic Times (Apr. 03, 2020, 08:52 AM), https://ciso.economictimes.indiatimes.com/news/zoom-app-vulnerable-to-cyber-attacks-says-cert-india-issues-advisory-on-safety-measures/74959554.

14. Users' email ID, photos may have been leaked on Zoom, The Times Of India (Apr. 1, 2020, 10:50 AM), https://timesofindia.indiatimes.com/gadgets-news/users-email-id-photos-may-have-been-leaked-on-zoom/articleshow/74924698.cms.

15. AP, Ex-Coca-Cola Worker Sentenced to 8 Years in Trade Secrets Case, CNBC (May 23, 2007, 01:15 PM), https://www.cnbc.com/id/18824080.

16. Ankita Chakravarti, WhatsApp may have leaked your number on Google, claims cybersecurity researcher, India Today (Jun. 9, 2020, 01:30 PM), https://www.indiatoday.in/technology/features/story/whatsapp-may-have-leaked-your-number-on-google-claims-cybersecurity-researcher-1687139-2020-06-09.

Official Websites:

17. Trade secret policy, USPTO (Feb 7, 2019 11:16 AM), https://www.uspto.gov/ip-policy/trade-secret-policy.

18. Trade Secrets, WIPO, https: /www.wipo.int/tradesecrets/en/.

19. Overview: the TRIPS Agreement, WTO, https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

20. North American Free Trade Agreement, SICE, http://www.sice.oas.org/trade/nafta/chap-172.asp.

21. UNITED STATES–MEXICO–CANADA TRADE FACT SHEET Modernizing NAFTA into a 21st Century Trade Agreement, Office of the United States Trade Representative, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/fact-sheets/modernizing.

22. 2760 Trade Secret, Confidential, and Protective Order Material [R-8.2012], USPTO (Jun. 25, 2020, 05:07 PM), https://www.uspto.gov/web/offices/pac/mpep/s2760.html.

23. Appendix L - Patent Laws, USPTO (Jun. 25, 2020, 06:20 PM), https://www.uspto.gov/web/offices/pac/mpep/mpep-9015-appx-l.html#d0e303884.

24. European Patent Office (EPO), USPTO (Mar 27, 2020 03:14 PM), https://www.uspto.gov/learning-and-resources/pursuing-international-ip-protection/european-patent-office.

25. Forms of IPR, EPO (Mar. 18, 2016), https://www.epo.org/learning/materials/inventors-handbook/protection/ipr.html.

26. ICT Facts and Figures 2017, ITU, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf.

27. The Impact Of Digital Technologies, United Nations, https://www.un.org/en/un75/impact-digital-technologies.

28. Guriqbal Singh Jaiya, Protecting Trade Secrets: Challenges in the Digital Environment, WIPO (May 21, 2008), https://www.wipo.int/edocs/mdocs/sme/en/wipo_smes_cgy_10/wipo_smes_cgy_10_ref_theme06_01.pdf.

Dictionaries:

29. Mary Ann Glendon, Common law, Britannica (Oct. 30, 2020), https://www.britannica.com/topic/common-law.

Journals and Blogs:

30. Derek Handova, The Business of IP: Choosing Between Patents and Trade Secrets, IP Watchdog(May 25, 2016), https://www.ipwatchdog.com/2016/05/25/choosing-patents-and-trade-secrets/id=69368/.

31. Shakun Soin, E- Marketing (Jul. 10, 2018), SlideShare, https://www.slideshare.net/ShakunSoinTaneja/e-marketing-105120000.

32. How Digital Marketers Can Protect Their Corporate Trade Secrets, The National Law Review (Nov. 6, 2018), https://www.natlawreview.com/article/how-digital-marketers-can-protect-their-corporate-trade-secrets.

33. Ranjan Narula & Rachna Bakhru, Protecting trade secrets in India, Lexology (May 1, 2018), https://www.lexology.com/library/detail.aspx?g=c83e8a6c-a02e-44ba-8723-94087d2e5e20.

34. Pareekshit Bishnoi, Breach of confidentiality maintenance covenants amid 'work from home' during COVID-19 lockdown: Concerns and remedies, Bar and Bench, (Apr. 21, 2020, 06:00 PM), https://www.barandbench.com/columns/breach-of-confidentiality-maintenance-covenants-amid-covid-19-concerns-and-remedies.

35. Brijendra Singh, Shalini Agarwall, and Karishma Rai, Need for separate Trade Secret Act with required Law, The Practical Lawyer, http://www.supremecourtcases.com/index2.php?option=com_content&itemid=1&do_pdf=1&id=24329.

36. Ravindra Chaba & Shyam Sundar Chaba, Inadequacy of the Trade Secret's Protection laws in India and Legal Regime Existing in U.S., Manupatra, http://www.manupatra.com/roundup/369/Articles/Inadequacy.pdf.

37. 2019 MRC Global Fraud Survey Results, Merchant Risk Council, https://merchantriskcouncil.org/resource-center/surveys/2019/2019-mrc-global-fraud- survey-results.

*****