SAFEGUARDING SECRET IN SHARED SPACES: LEGAL STRATEGIES FOR TRADE SECRET PROTECTION IN OPEN INNOVATION

Nirmala. R. Harish[1], Assistant Professor, CMR University School of Legal Studies

Ritika Singh[2], B.A. LL.B. (Hons), CMR University School of Legal Studies

ABSTRACT

Innovation in the current generation no longer develops in isolation but rather through the collaboration of industries, universities, and research institutions- a concept that is commonly referred to as open innovation. By far, the main advantage of this approach is the cost saving and faster development that is made possible by the sharing of ideas, resources, and technology among the organizations taking part in the. On the other hand, it puts forward a big issue of how to ensure the security of the absolutely confidential aspect of the most sensitive intellectual property - trade secrets - in the case. Trade secrets, those comprises of confidential business information such as algorithms, clients list, formulas, and industrial processes, hold value only as long as they are not reveal. Unlike patents, they are not registered and it rely solely on the owner's diligence in maintaining secrecy.

The complex relationship between trade secret usage and innovation openness is examined in this study. It examines how collaborative platforms, such as cloud systems, collaborative research labs, and data-sharing technologies, foster innovation while simultaneously raising the possibility of data leakage or exploitation. In order to identify these problems, the paper discusses a variety of contract-based protection measures such Non-Disclosure Agreements (NDAs), secrecy clauses, and joint development agreements that most precisely specify ownership, authorship, and the use of rights. Additionally, it highlights organizational and technology solutions including encryption, blockchain verification, access control, and internal compliance training, highlighting the fact that security is a cultural as well as a technical problem.

[1] Assistant Professor, CMR University School of Legal Studies.

[2] Student of B.A.LL.B. (Hons), CMR University School of Legal Studies.

Trade secret issues frequently result from poorly defined collaboration borders, according to the interpretation of key decisions. Additionally, they stress that having clear contractual rules and efficient communication are two of the best methods to prevent problems from becoming legal difficulties.

In the end, the authors came to the conclusion that a system of regulations that balance protecting private information with promoting knowledge sharing will sustain open innovation.

INTRODUCTION

Innovation rarely occurs in emptiness in the modern world. Universities, research centers and businesses are progressively engaging to develop new technology and products. We often refer to this habit as open innovation[3]. Organizations share knowledge, concepts, and resources with one another rather of conducting all of their own research. Carbon copy examples of such occurrences could be a case of a large pharmaceutical company teaming up with a small biotech company or a software startup collaborating with a university. The two main results of these synergies are cost savings and an acceleration of the innovation process. However, it also brings up some very significant challenges, such how to protect confidential information.

Among different kinds of intellectual property, those which are the most vulnerable in open innovation are trade secrets[4]. A trade secret is essentially any knowledge that is different from the rest and that provides a company with a competitive advantage over others[5]. Such examples could be a chemical formula, a software platform, a manufacturing process, or even a client list. The only thing that makes a trade secret valuable, in contrast to patents or copyrights, is that it is confidential. The benefit disappears once it is leaked. The likelihood of one partner disclosing such secrets is always quite high because knowledge is shared often in joint research. Currently, one of the most important legal and practical concerns in collaborative initiatives is the protection of trade secrets.

[3] Henry Chesbrough, *Open Innovation: The New Imperative for Creating and Profiting from Technology* (Harvard Bus. Sch. Press 2003).

[4] David Orozco, *Legal Strategies for Protecting Trade Secrets in Collaborative Research*, 17 J. Intell. Prop. L. 1 (2010).

[5] Uniform Trade Secrets Act § 1(4) (1985).

Trade secrets and other confidential information, for example, financial worth due to their secrecy, and are that they are carefully guarded by their owner.

These examples are intended to demonstrate mathematics, designs, industrial processes, software codes, and marketing tactics. Unlike patents, trade secrets do not come with government registration. Therefore, the owner's attempts to keep them hidden—whether through digital security, NDAs (Non-Disclosure Agreements), or restricted access—are the only way to ensure their safety. A trade secret is no longer defined as such if the information is made public in any way. However, if the secret is kept, the protection can remain for a very long period.[6]

Trade secrets are not subject to any time limitations. Only confidentiality is a prerequisite for them to exist.

For example, a soda recipe that is patented will be made public and thus, no longer protected after 20 years. Similar to the formula of Coca-Cola, it can be kept going without sharing forever if it is considered a trade secret.

OPEN INNOVATION AND SHARED SPACE.

Open innovation is a method in which businesses are supported outside the concepts, skill, and technology in addition to their own inner research. The model allows information to flow from both ways: businesses can hire outside their experts while also letting individuals develop their own products or ideas. For instance, a technology company collaborates with a university on the idea of a new software research, or a pharmaceutical drug company may allow a smaller research company to examine. There are various kinds of open innovation; some are based on official joint ventures, while others are based on modified union like industry-academic partnerships or collaborative working platforms. The wish to exchange knowledge across organizational boundaries in order to encourage is what unites all these strategies. The interest of collaboration helps to explain the rise up in open innovation. In the first place, it makes a larger pond of ideas and resources available than any one company could create on its own. For example, mostly startups frequently give new ideas, and established companies provide capital and access to markets. Besides, partnerships transport the expenses and risks of research

[6] *Coca-Cola Co. v. Koke Co. of Am.*, 254 U.S. 143 (1920).

along with them. Very often it is too costly for one company to come up with a new drug or a technology, but by coupling their financial resources, several partners can dilute the money burden. Collaborations have a strong potential to shorten the time to the market of the research results as well. The reasoning leading to this is that if experts of many different fields work together, they can figure out solutions to the problems in a much faster and more efficient way. Therefore, open innovation not only makes the progress of science and technology faster for the whole society, but it also brings more benefits to the participants of the process immediately.

While open innovation has a number of advantages, there are some risks associated with personal data privacy. Joint laboratories, cloud-based platforms, and collaborative digital tools are examples of shared spaces that are very beneficial for data interchange, but they are problematic from the perspective of information being duplicated, misused, or leaked. For instance, in a conference paper, a research partner can inadvertently disclose important information, or a worker on a collaborative project might submit to a third party.

There are situations where collaborator may deliberately take and use trade secrets to gain an advantage thus, the problems of disputes and court cases emerge. With international projects, the challenge of guaranteeing the same level of protection becomes much more complex due to disparities in legal systems and enforcement. Therefore, even if open spaces facilitate cooperation, they also necessitate the deployment of robust security measures, such as confidentiality agreements, restricted access, and careful oversight of information sharing.

CONTRACTUAL MECHANISMS FOR TRADE SECRET PROTECTION.

When sole person or group of persons collaborate together, few a times they disclose important information that they would likely to prefer not to be made out to the public. A new innovation, research findings, commercial ideas, or trade secrets can be the subject of this. Numerous measures have been taken to put such information under the protection of trade secret. The most commonly used instrument is a Non-Disclosure Agreement (NDA). It is essentially a written agreement between two parties which says, "I will not disclose or use the information you shared with me for my benefit." It defines the limits very clearly and offers legal backing in case of violation. Confidentiality terms quite often are added to larger contracts together with NDAs, especially in business or research collaborations. The provisions in question clearly indicate that in the absence of mutual agreement, any data, discoveries, concepts shared

during the project are to be regarded as confidential or secret. As an example, these kinds of agreements stipulate that the outcomes of a partnership between two universities or a company and a research institute cannot be revealed to the other party without authorization.

Joint creation or license agreements are used as means of cooperation between the parties to not only create something new but also share knowledge. Such contracts specify in very fine details the user, the purpose and the conditions of using the information supplied. When one party permits another to use their intellectual property—such as a patent, technology, or creative work—licensing agreements play a major role. By clearly outlining the rights and responsibilities, they not only make everything comfortable but also prevent uncertainty.

Also, among different IP (intellectual property) sectors that challenge the IP field, those related to the ownership and authorship of the intellectual property are the most frequent ones. Questions such as: Who owns the patent? arise when an invention, research paper, or creative work has several creators. Which of them is the primary author? Who receives the rewards and recognition? Disagreements could be the result of unresolved issues. Ownership, revenue-sharing, and authorship agreements can help avoid a lot of problems.[7]

TECHNOLOGICAL AND ORGANIZATIONAL MEASURES.

Nowadays, the safeguarding of data and intellectual property rights demands a combination of organizational and technological initiatives. Among these are the digitally secure and privacy measures that are implemented with tools such as multi-factor authentication, encryption, identity, and access management, as well as data loss prevention systems. Sensitive data are secured both while being sent and when stored. The legislations such as the Digital Personal Data Protection Act, 2023 in India, mandate that companies take the necessary security measures to avoid incidents of personal data breaches[8] while also providing that lawbreakers will be punished with fines in case of non-compliance.

Besides that technology, the access to control and need-to-know basis sharing are equally valuable. Permissions are to be checked on a regular basis in order to prevent their misuse or leakage, and employees as well as third parties should be granted access to the information that

[7] Christopher M. Holman, *Protecting Trade Secrets in Collaborative Research: Challenges for Global Innovation*, 45 Vand. J. Transnat'l L. 917 (2012).
[8] Digital Personal Data Protection Act, No. 22 of 2023, § 9, India Code.

is only necessary for their work. The principle of least privilege, which is likewise endorsed by international standards such as ISO/IEC 27001, is yet another acknowledgment that highly secure access control systems play a key role. Advancing technologies such as artificial intelligence and blockchain are becoming more and more valuable intellectual property protection tools. Blockchain can offer tamper-proof timestamps and proofs of creation for digital files, and these can later be presented as the strongest evidence in case of a dispute, whereas AI tools can -locate online platforms to find copyright infringement, or unauthorized use of trademarks.

Still, these should not be considered as replacements for formal IP registration but rather as support means that make enforcement and the gathering of evidence easier. On the level of the organization, internal compliance policies and training create the culture and the discipline that are necessary for permanent protection.

Policy documents are expected to describe in detail aspects such as data classification, acceptable use, vendor obligations, breach response, and holding periods. At the same time, training programs should continuously enhance employees' knowledge regarding safe practices, scam recognition, and their legal rights and obligations.

Regulations such as Section 43A of the Information Technology Act, 2000 (which provides for the payment of compensation in case of a security breach of sensitive personal data) and Section 72 (which provides for a penalty for the unlawful disclosure of information) signal that companies have a legal obligation to protect their information in a secure manner[9]. Likewise the DPDP Act of 2023 besides organizational and technical measures, has breach notification obligations. When these are combined, these technological tools, stringent access controls, ingenious blockchain and artificial intelligence applications, strong internal compliance frameworks not only provide sufficient protection intellectually property and business secrets but also help companies to be in accordance with the law while receiving the trust of the stakeholders.

LESSONS FROM TRADE SECRET DISPUTES IN INNOVATION PARTNERSHIP.

Trade secret disputes have become a common theme in the aftermath of the collaboration in

[9] Information Technology Act, No. 21 of 2000, §§ 43A, 72, India Code.

the pharmaceutical industry, where companies share highly confidential research data and processes even before acquiring patents. As a result, AbbVie v. BeiGene (2024) is a story of how a research association can turn into a legal battle in a matter of minutes if scientists decide to change their loyalties[10]. AbbVie filed a lawsuit against the ex-partner to whom it alleged the exploitation of confidential information concerning cancer treatment research. Another instance of how agreements sometimes can act as a reserve of commercial value is the Emcure–HDT conflict over COVID-19 vaccine technology[11], which has become a licensing relationship as a result of the settlement. The early cases in the field of oral drug delivery technologies, such as Eli Lilly & Co. v. Emisphere Techs., Inc., also, feature that disagreements nearly always come up in the absence of proper agreements[12]. These situations remind us that pharmaceutical drug industry NDAs and explicit ownership terms are as indispensable as the science itself.

Waymo v. Uber (2017–18) was the main turning point that unveiled the very high value of algorithmic trade secrets[13]. The lawsuit was about the algorithms for self-driving cars. Uber agreed to pay a settlement and to discontinue the use of Waymo's proprietary assets. In the Kevlar fiber case of DuPont v. Kolon, the misappropriation caused by a former employee led to significant damages and even criminal pleas[14], and the case served as a warning example of the harmful side of leaks of knowledge. Also, courts have delineated "use" of the secret. To illustrate, in Silvaco Data Systems v. Intel, a court in California decided that, under CUTSA, merely utilizing object code without access to source code was not considered as the reallocation of the latter[15]. Such are the disagreements to which these referred are; they stress that access control, source calling, and watching staff departures are crucial to safeguarding the spirit of innovation in AI and software partnerships.

When these disputes are geographically remote from each other; they still convey almost the same lessons. Firstly, delineating the features of a trade secret and demonstrating that the information was kept confidential are the main thrusts of winning the claims. Secondly, the protective shelters rely primarily on such measures as NDAs, joint-development articles, and exit provisions. India is also an example of such a situation where the legal system is based on

[10] *AbbVie Inc. v. BeiGene Ltd.*, No. 1:24-cv-00876 (D. Del. 2024).
[11] *Emcure Pharm. Ltd. v. HDT Bio Corp.*, 2022 SCC OnLine Bom 1734.
[12] *Eli Lilly & Co. v. Emisphere Techs., Inc.*, 408 F. Supp. 2d 668 (S.D. Ind. 2006).
[13] *Waymo LLC v. Uber Techs., Inc.*, No. 3:17-cv-00939, 2018 WL 646701 (N.D. Cal. 2018).
[14] *E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc.*, 637 F.3d 435 (4th Cir. 2011).
[15] *Silvaco Data Sys. v. Intel Corp.*, 184 Cal. App. 4th 210 (2010).

contract law and breach of confidence laws rather than giving birth to the separate trade secrets statute. Thirdly, the manner in which evidence is handled can have a significant impact on a court case's result; as the DuPont-Kolon scuffle reveals, even cases that are well supported can be weakened by file deletions or unprofessional record-keeping. Last, but not least, settlements cups not only to cover losses but also, as the Emcure-HDT case shows, to relaunch collaborations and keep the value going. Contracts, company procedures, and laws being in sync will make open innovation more effective to be in harmony to protect the confidential information that partners share, be it in pharma, artificial intelligence, or agriculture.

India does not have a well-defined trade secrets statute and as a result, contracts, equity, and breach of confidence are the instruments used to resolve disputes. The courts have been vocal in their view that information shared in a relationship based on trust should be treated with care and not be thrown to the wolves. One of such instances was the decision of Bombay High Court in Rochem Separation Systems (India) Pvt. Ltd. v. Nirtech Pvt. Ltd. (2006) where it was held that the ex-employee who joined a competitor and was charged with the theft of patented designs should be restrained[16]. The judges opined that while it is the right of an employee to use the knowledge and skills that s/he has acquired, s/he is not allowed to appropriate the employer's exclusive technological secrets. Similarly, the Delhi High Court in John Richard Brady & Ors. v. Chemical Process Equipments Pvt. Ltd. (1987) held that the defendants were stopped from gaining monetary benefits based on the use of the established designs and blueprints of equipment, thereby indicating that exploitation of confidential information for monetary use is illegal[17]. These examples show how Indian courts have consistently been on the side of trade secret enforcement through the use of equity even without statute.

The case of American Express Bank Ltd. v. Priya Puri (2006) is another significant Indian example, where the Delhi High Court took on an employee accused of stealing private client lists. The court explained that client databases and detailed business plans that are developed by an employer should be the confidential information[18] of the employer even though the employee's "general skill and knowledge" might be transferred. Correspondingly, the Bombay High Court in Sundial Communications Pvt. Ltd. v. Zee Telefilms Ltd (2003) held that ideas and proposals for programs given in confidence and kept secret may be regarded as exclusive

[16] *Rochem Separation Sys. (India) Pvt. Ltd. v. Nirtech Pvt. Ltd.*, 2006 SCC OnLine Bom 838.
[17] *John Richard Brady & Ors. v. Chemical Process Equipments Pvt. Ltd.*, 1987 SCC OnLine Del 157.
[18] *American Express Bank Ltd. v. Priya Puri*, 2006 SCC OnLine Del 19.

information[19]. All these decisions brought it out that in India the trade secret claims' enforceability heavily depends on the proper drafting of NDAs, employment agreements, and recording of confidentiality situations.

Best practices and policy recommendation

The most challenging aspect of any collaborative endeavour is usually striking the correct balance between transparency and protection; this is particularly true in fields like technology, artificial intelligence, and pharmaceuticals. Thus, a great method to foster innovation is for researchers and companies to work together by exchanging information, resources, and ideas. However, complete transparency carries the risk of giving the wrong party access to the most crucial trade secrets. The solution to this dilemma is to identify the private information even before the project begins, reveal it gradually, and only reveal what is required. As a result, there is no risk of losing the essential business knowledge.

Another essential move in the teamwork process is the establishment of solid contracts and methods. The majority of problems should be managed by cooperation research agreements, licenses, and non-disclosure agreements (NDAs) which make it clear the ownership of the results, the use of the confidential material, and the way the collaboration will be after the partners have worked together. Besides that, contracts specify the rights to access, the steps for resolving disputes, and the data handling instructions. The established procedures from the agreements help to eliminate misunderstandings and provide solid proof if there is a dispute. But the development of trust between partners is equally, if not more, crucial than the completion of formal paperwork. Honesty, equitable benefit sharing, and open communication are all components of trust. Researchers and companies should endeavour to establish a setting where maintaining anonymity is not only required by law but also a regular practice. High moral standards, internal control systems, and regular training are all signs that such a culture exists. Collaboration is facilitated by confidentiality policies, and the foundation of collaboration is trust, which can endure forever.

In the end, there is growing desire for the international harmonization of legal trade secrets. Currently, different nations provide varying degrees of protection; for instance, India primarily depends on contracts and court rulings, whereas the United States has comprehensive laws such

[19] *Sundial Communications Pvt. Ltd. v. Zee Telefilms Ltd.*, 2003 SCC OnLine Bom 1102.

the Defend Trade Secrets Act. International projects are less stable due to the differences in protection levels. A unified system, whether governed by regional agreements or international organizations like WIPO, would make cross-border interactions between businesses and researcher considerably easier.

Such harmonization should not only guarantee that partners have comparable protection for their trade secrets regardless of the nation in which they conduct business, but it should also not obstruct future innovation.

CONCLUSION.

One of the most challenging open innovation issues in the world is the protection of trade secrets. For example, technological, AI, and pharmaceutical collaborations will only be successful if we can find the right balance between sharing and safeguarding.

In cases like American Express Bank Ltd. v. Priya Puri and Rochem Separation Systems v. Nirtech Pvt. Ltd., Indian courts have ruled that in the absence of specific legislation for trade secrets protection, they treat the matter as one of contract law and also base their decisions on principles of equity[20]. However, domestic conflicts like Waymo v. Uber and DuPont v. Kolon basically show that if ownership and confidentiality are unclear, things can turn violent very rapidly, and then lawsuits will be brought. These examples generally indicate the need for protective regulations, at the very least, very tight agreements, and caution while handling data.

Moreover, the protection of trade secrets will depend on the next changes in the law that will take not only into account the international but also the interconnected nature of innovations. For example, the US with its Defend Trade Secrets Act has already set the stage for a more open and clear protection of the issues in question while India and other developing countries are still dependent on court judgments and non-disclosure agreements. The introduction of an all-encompassing trade secret law in India would be beneficial with regard to the aspects of trust, confidence, and local and international cooperation. Moreover, a harmonized global framework created by such entities as the World Intellectual Property Organization (WIPO) could provide standardization and safety for cross-border research and collaboration. Finally,

[20] World Intellectual Property Organization (WIPO), *Trade Secrets and Innovation* (2020).

transparent innovation can be maintained if it relies on a well-defined legal framework, ethical cooperation, and trust, which protect the most valuable knowledge.[21]

[21] WIPO, *Model Provisions on Protection Against Unfair Competition* (1996).