Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

The confidentiality clause in tech-related Contracts and consequences of breach

Rieya Dadhich[a]

[a]Amity University, Gurugram, India

Received 23 September 2022; *Accepted* 03 October 2022; *Published* 12 October 2022

A company's three primary security goals for securing its information are confidentiality, integrity, and availability. Employees of technology firms, consultants, independent contractors, partners, licensees, and even joint ventures must sign confidentiality agreements. Such agreements have a broader range of applications, even outside of high-tech firms, because they are used to protect and safeguard confidential business information such as financial data and marketing plans, as well as other unpublished price-sensitive information in the case of publicly traded companies. If one of them is compromised, it could cost a company a lot of money. A company's foundation is built on the data and information it creates and secures to grow. This article discusses the need for confidentiality in technology-related agreements, the drafting and negotiating strategies to be used, also the repercussions of violation under Indian law.

Keywords: *confidentiality, resolution, negotiation, consequences.*

INTRODUCTION

A technology agreement, also known as a technology service agreement, is a legal contract typically used between a corporation and a technology service provider to explain each party's rights and duties when they engage in a commercial partnership. Fees, the extent of the

technology company's services, and what each party will do if the contract is cancelled are all items that technology agreements cover. A technology agreement is frequently utilised when a firm employs another company to conduct services such as engineering or uses proprietary software and technology to deliver a specific service. In the business agreement and dispute resolution procedures, these agreements assist in identifying who is liable for what.

This information may include but is not limited to trade secrets, hardware and software technologies, source codes, client information, and workforce information. These are the intellectual properties of a company that have been developed or earned through capital and hard work, and they must be protected at all costs. The definition of "confidential information" is the most important in confidentiality agreements. It is impossible to define confidential information in every situation because it varies from case to case and must be defined based on the nature of the business involved. The parties must reach an agreement on the conditions to be followed. The main goal of defining confidential information is to set the boundaries for disclosure without revealing any information or secrets.

IMPORTANCE OF CONFIDENTIALITY

These agreements can transmit various types of information, such as technical expertise, ideas, research information, chemical formulae, and other information of a similar nature. These types of disclosed information are precious to the disclosing party because they can significantly impact the Company's business. The Disclosing Party will ensure that such valuable information does not enter the public domain. Companies are under no obligation to disclose confidential information to the public unless it is in the public interest, as defined by the Information Act of 2005. [1]

Privacy as a concept means defining confidentiality and how it should be valued. The extent to which privacy is protected as a right (and should be legally protected). The law does not define privacy; instead, it determines which instances of confidentiality shall be legally protected. It is

[1] Right to Information Act, 2005, s 8(1)(d)

worth noting that the common law lacks a broad right to privacy, and the Indian Parliament has been hesitant to adopt one. The terms confidentiality and privacy are relatively interchangeable. Confidentiality entails a stated or inferred basis of an independent equitable norm of confidence. Individuals, groups, or institutions have the right to decide when, how, and to what degree information about them is shared with others. The right to privacy is more of an implication and is the "right to be left alone."

In legal terms, confidentiality emerges when a duty of confidence exists between a "data collector" and a "data subject." This might be due to several conditions or various categories of information, such as work, medical, or financial information. An obligation of confidence grants the data subject the right not to have his information used for other purposes or divulged without his agreement unless there are other compelling public-interest grounds. A confidential agreement aids access to trade secrets, source codes, hardware, and software technology that is restricted to protect the client's intellectual property. Protection from third-party liability on intellectual property issues in the event of disclosures. Liability in the event of a contract breach. Restriction of Access improves clients' technological position. Fair IP allocation between your client and the third party, access to information required for operation is granted.

Epic Systems Corp. v Tata Consultancy Service

Epic Co. hired Tata Consultancy Services to test Epic's software in the United States in 2014. Tata was also working on similar competing software to Epics. Tata employees downloaded thousands of Epic documents before wiping computers clean to obfuscate the transfers. Epic Systems Corporation was awarded $940 million in a jury trial. However, the case is currently being appealed in the United States. This is a clear case of trade secret theft and a breach of the confidentiality and integrity of the information provided by Epic Systems Corp. by TCS. If the fundamental breach had gone undetected, Epic Systems could have lost a significant amount of money. To avoid such situations, it is always recommended that the contracting parties enter into a confidential agreement that defines what information will be shared between the parties, how it will be processed, and who will have access to it to avoid future disputes.

DISPUTES CONCERNING CONFIDENTIALITY AND THEIR RESOLUTION

The following are the disputes regarding confidentiality:

1. **Technology reverse engineering:** Most technology transactions are business-to-business transactions in which one party offers technology in the form of hardware or software to the other party. Because the party has spent significant time and money creating that technology, it is their intellectual property. The party producing such technology is the exclusive owner of such technology and is licencing it to the other party. As a result, the licensee is required not to reverse engineer the technology or decompile the program, as this would result in a financial loss to the owner.

2. **Transfer of business model**: When organisations negotiate, finalise, implement, or operationalise a contract, the confidentiality components of their business models are shared. Companies in this field refuse to enter into confidential agreements, which may lead to future conflict.

3. **Privacy Breach**: The case of TCS is one such issue in which the firm accesses another company's data without its consent to obtain financial advantages and gain a competitive advantage through the leaked data. The other party suffers a financial loss due to the data theft.

4. **Infrastructure Conflicts**: Some firms engage in an agreement and commit to take adequate measures and create technology and infrastructure to the level required to reduce the risk of an information breach but fail to do so. Due to a lack of appropriate measures, such occurrences result in a conflict between the parties.

5. **Contravention of privacy laws or GDPR**: The bulk of Indian tech firms operate as 'processors of data,' giving outsourcing services to tech firms outside of India that are 'controllers of data.' The parties must agree on how data will be exchanged and how it will enter the organisation. As a result, these Indian enterprises must comply with the Controller's country's privacy laws and regulations, and failure to do so might result in significant consequences.

RESOLUTION OF CONFLICT

Each organisation, under an agreement, is obligated to enhance its technology to ensure that no information is leaked from either side. However, suppose there is a breach, and a party has incurred loss due to the violation of confidentiality of the technology or information disclosed. In that case, the following options exist to resolve the dispute:

1. **Training and Compliance**: Preparing ahead of time is preferable to waiting for the storm. Most businesses constantly train their personnel, monitor them, upgrade their security systems, and take precautionary measures to prevent information loss.

2. **Mobile Phone Policy**: Employees' use of mobile phones in the workplace might allow them to rapidly share secret corporate information with friends, relatives, or rivals without the firm's awareness. Employees must not be allowed to take images, communicate sensitive information, or post such sensitive content to their devices. A mobile phone policy should be implemented to prevent breaches of confidentiality, and workers should be made aware of the repercussions of such violations.

3. **Compensation**: The Party that has incurred a loss may seek compensation and damages from the competent authorities for the loss caused by the violation.

4. **Injunction**: If there is still any information leakage due to the negligent or reckless behaviour of the person at fault, an injunction can be granted against them to stop them from causing such a breach and causing additional harm to the other party.

5. **Indemnity**: This is the favoured method of resolving disputes by most businesses because if the breach causes harm, the other party is obligated to indemnify (make good on the loss) the party that has incurred damage as a result of the breach.

6. **Damages**: The plaintiff may seek the necessary damages for breach of the confidentiality agreement, and the court will appropriately award such claims.

7. **Account of Profit**: This is a remedy in which any gains gained by the defendant are taken away from him, and he is unable to enjoy any benefits originating from the agreement's violation of the confidentiality provision.

8. **Permissible Disclosure**: As a non-disclosure, a certain amount of the technology involved must be provided as it is required to disclose such technical information to an employee or a subcontractor who will take part in manufacturing the product or a component of the product.

9. **Designate a "data guard"**: Each party might agree to appoint a "data guard," a person tasked with vetting private information given by the other party. Information supplied to the "data guard" may still be kept confidential. Still, ownership rights would not be transferred unless the "data guard" concluded that revealing sensitive information to the research and development team was worthwhile.

CONSEQUENCES OF BREACH

The Information Technology Act, 2000[2]

The Indian Parliament passed the Information Technology Act 2000. It obtained the President's assent on June 9, 2000, and went into force on October 17, 2000. This Act is based on Resolution A/RES/51/162 issued by the United Nations General Assembly on January 30, 1997, concerning the Model Law on Electronic Commerce previously adopted by UNCITRAL[3]

Considering the need for uniformity of the law applicable to alternatives to paper-based communication and information storage methods, the aforementioned United Nations General Assembly resolution recommends that all States give Model Law on Electronic Commerce favourable consideration when enacting or revising their laws. The Government of India had the foresight to begin the entire process of creating India's first-ever information technology legislation in 1997.[4] It is critical to understand that the legislative intent behind the Information Technology Act of 2000 was not to ignore the national or municipal (local) perspectives of

[2] Information Technology Act 2000
[3] United Nations Commission on International Trade Law 1966
[4] UNCITRAL Model Laws for E-commerce 1997

information technology but rather to ensure that it has an international perspective, as advocated by the UNCITRAL Model Law on Electronic Commerce.

The fundamental concepts of the Information Technology Act of 2000 are listed below:

It is worth noting that the Indian Parliament created a new legal framework for data security and privacy by passing the Information Technology Act in 2000.

The data protection and privacy principles are as follows:

(i) defining 'data, 'computer database, 'information, 'electronic form, 'originator, 'addressee, etc.

(ii) imposing civil liability if anyone gains access to or secures access to a computer, computer system, or computer network;

(iii) imposing criminal liability if anyone gains access to or secures access to a computer, computer system, or computer network; and

(iv) designating any computer, computer system, or network as a protected system.

(v) implementing penalties for breaches of confidentiality and privacy; and

(vi) establishing a regulatory authority structure, including adjudicating officials, the Cyber Regulations Appellate Tribunal, and so on. [5]

Section 72. Penalty for breach of confidentiality and privacy[6]

Except as otherwise provided in this Act or any other law currently in force, any person who, in the exercise of any of the powers conferred by this Act, rules or regulations made thereunder, obtains access to any electronic record, book, register, correspondence, information, document, or other material without the consent of the person concerned and discloses such electronic

[5] Vijay Pal Dalmia, 'Data Protection Laws In India - Everything You Must Know' (*Mondaq*, 13 September 2017) <https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know> accessed 23 September 2022

[6] Information Technology Act 2000, s 72

form, book, register, correspondence, information, document, or other material to any other person. The part mentioned above has only a restricted use. It is limited to the acts and omissions of those individuals who have been given authority under this Act, Rules, or Regulation.

Section 72 of the Act applies to any person who, in the exercise of any of the rights given by the Act or its related rules and regulations, obtains access to any of the following:

i) Electronic record,
ii) book,
iii) Register,
iv) Correspondence,
v) Information,
vi) Document, or
vii) Other material. [7]

If a person reveals such electronic record, book, register, communication, information, document, or other material to another person. In that case, he shall be punished with imprisonment for a term extending to two years, or a fine reaching one lakh rupees, or both. If such a person discloses an electronic record, book, register, communication, information, document, or other material to another person. In that case, he faces imprisonment for up to two years, a fine of up to one lakh rupees, or both.

The Act confers powers to:

(Ss. 17[8]-18[9]) The Controller of Certifying Authorities

(Ss. 17 and 27[10]) The Deputy and Assistant Controllers of Certifying Authorities

(S. 31[11]) Licensed Certifying Authorities and (Rule 312) Auditors

---

[7] *Ibid*
[8] Information Technology Act 2000, s 17
[9] Information Technology Act 2000, s 18
[10] Information Technology Act 2000, s 27
[11] Information Technology Act 2000, s 31

(S 46[12]) The Adjudicating Officer

(Ss. 48-49[13]) The Presiding Officer of the Cyber Appellate Tribunal

(S. 56[14] and rule 263) The Registrar of the Cyber Appellate tribunal

(S. 79) Network Service provider

(S. 80) Police Officer (Deputy Superintendent of Police)

Section 72 is that anybody who has gained access to such information should not take undue advantage of it by exposing it to a third party without the approval of the disclosing party. A trust duty exists between the "data collectors" and the "data subject." Sections 43 (a) - (h) of the Act encompass various cyber contraventions linked to unlawful access to a computer, computer system, computer network, or resources.[15]

Section 43 of the Act covers instances such as:

(a) computer trespass, violation of privacy, etc.
(b) unauthorised digital copying, downloading, and extraction of data, computer database, or information; theft of data held or stored in any media,
(c) unauthorised transmission of data or programme residing within a computer, computer system, or computer network (cookies, spyware, GUID, or digital profiling are not legally permissible),
(d) data loss, data corruption, etc.,
(e) computer data/database disruption, spamming, etc.,
(f) denial of service attacks, data theft, fraud, forgery, etc.,
(g) unauthorised access to computer data/computer databases and
(h) instances of data theft (passwords, login IDs), etc. [16]

[12] Information Technology Act 2000, s 46
[13] Information Technology Act 2000, s 49
[14] Information Technology Act 2000, s 56
[15] Information Technology Act 2000, s 80
[16] Information Technology Act 2000, s 43

The Information Technology Act of 2000 establishes legal responsibility for data theft, computer database theft, and privacy violations, among other things. The Act also includes a whole Chapter (Chapter XI) on cybercrime, with sections 65-74 covering a wide range of cybercrime offences, such as unauthorised alteration, deletion, addition, modification, change, destruction, duplication, or transfer of data, and computer database.

Section 65 of the Act,[17] for example, protects not only computer source code but also data and computer databases; similarly, section 66 [Hacking with Computer System] covers cyber offences related to (a) illegal access, (b) illegal interception, (c) data interference, (d) system interference, (e) misuse of devices, and so on. The Information Technology Act of 2000 establishes criminal penalties for data, computer databases, and privacy violations, among other things.

PROPOSED CHANGES TO THE INFORMATION TECHNOLOGY ACT OF 2000 IN TERMS OF DATA PROTECTION AND PRIVACY

In its recommendations, the Expert Panel established by the Department of Information Technology, Ministry of Information Technology, Government of India suggested the following improvements to the Act to increase data protection and privacy:

Section 43 of the IT Act, 2000

(v) Reasonable security practices and procedures mean, in the absence of a contract between the parties or any special law for this purpose, such security practices, and policies as appropriate to the nature of the information to protect that information from unauthorised access, damage, use, modification, disclosure or impairment, as may be prescribed by the Central Government in consultation with the self-regulatory bodies of the industry, if any. Section 43, Explanation (vi) Sensitive personal data or information means such personal information prescribed as sensitive by the Central Government in consultation with the industry's self-regulatory bodies.

[17] Information Technology Act 2000, s 65

It is important to note that the proposed amendments would not only pave the way for self-regulation in terms of defining what constitutes reasonable security practices and procedures and sensitive personal data or information but would also grant sensitive personal data statutory protection. Furthermore, the proposed revisions have broadened the scope of section 66 by aligning it with the provisions of the Indian Penal Code, 1860,[18] and by defining the amount of criminal liability in data theft, computer database theft, privacy breach, and so on. Furthermore, the newly proposed sub-section (2) of Section 72 holds intermediaries (network service providers) accountable for data and privacy infractions. Now, such intermediaries must pay damages as compensation to the impacted subscribers.

Drafting of Confidentiality Clause

When creating a confidential agreement, make sure it includes the following essential clauses:

Define the technology under consideration: It is preferable to be highly inclusive rather than underly inclusively when discussing technology. Try to anticipate short-term demands like technological improvements as feasible to (hopefully) prevent the need to give a new or updated NDA before the ink on the original is dry.

Define "confidential information": Define what information will be considered confidential, how to determine that, and what the exceptions to information are.

One of the most frequent provisions used to protect sensitive information is as follows: *"The Executive shall hold in a fiduciary capacity for the benefit of the Company all secret or confidential information, knowledge or data relating to the Company or any of its affiliated companies, and their respective businesses, which shall have been obtained by the Executive during the Executive's employment by the Company or any of its affiliated companies and which shall not be or become public knowledge (other than by acts by the Executive or representatives of the Executive in violation of this agreement). After termination of the Executive's employment with the Company, the Executive shall not, without the prior written consent of the Company or as may otherwise be required by law or legal process,*

[18] Indian Penal Code 1860

communicate or divulge any such information, knowledge, or data to anyone other than the Company and those designated by it."

You may have noticed that this secret clause does not specify the objects. Instead of a hazy definition, businesses should be crystal clear about the goals of adopting a non-disclosure agreement and stick to the agreement's defined purpose. A detailed description not only helps the Receiving Party comprehend what information is secret (as opposed to ordinary information), but it also reduces the danger of the agreement being invalidated by a court owing to ambiguity. It's also a good idea to mention exceptions to the confidential obligation. Furthermore, agreements, all information that is not publicly available or susceptible to being discovered by a third party or independent market research is confidential. In some circumstances, information relevant to company models, customer lists, and so on is deemed sensitive.

Define the term for exchanging data: It is critical to define how long the parties will share sensitive information. This is typically maintained for one year. - How? The length of the agreement will determine this.

Define the duration of confidentiality requirements after the contract's expiration or termination: This is distinct from the information exchange period, which usually lasts for the length of the contract. This is when the parties agree not to divulge the secret information supplied after the time of exchange has elapsed. This time is often set at 3-5 years so that even if the term of the deal expires, the party cannot release this information till this duration, and the other party can upgrade its technology by that time.

Do not disclose source code - this does not contribute to drafting: Only distribute software in object/machine code format. Do not distribute the source code. The human-readable instructions a programmer puts in word processing form when designing software are called source code, and it is the primary source of IP.

Who has access to the information: Define who has access to sensitive information; keep the numbers low; the more people who have access to the data, the less confidential it is.

Authority to settle the disagreement: It is preferable to use alternative dispute resolution to resolve conflicts between parties since courts are regarded as public property, and information that is meant to be confidential will no longer be such once the dispute reaches the court.

These sections are not exhaustive and are provided for reference only; the parties can agree on which clauses to include in the agreement by consensus.

NEGOTIATION OF THE CONFIDENTIALITY CLAUSE IN TECH-RELATED CONTRACTS

- **Understand the organisation's aims:** Due diligence is required to determine the party's background, the areas they deal with, previous relationships with the parties, and the goals they want to achieve by agreeing with your party.
- **Avoid sharing too much:** Because the NDA is generally the first agreement between parties, and the relationship is still growing, avoid sharing "crown jewels" under the NDA.
- **Be Wary of the Title:** Although the title of an agreement is not essential, a lawyer should not be misled by the innocuous labels of the other party's documents. Check the agreement to see if it mentions technological or financial confidentiality. Be wary of terms such as IP assignment responsibilities, non-compete agreements, non-hire provisions, etc. If these terms are taken for granted, they might have significant ramifications for the firm.
- **Make the agreement extensive:** By making the agreement exhaustive, there is less likelihood of confusion and no need to remodel the agreement again. Include even minor features or updates that the firm may do in the future.
- **Please limit the number of disclosures:** It is preferable to limit the number of disclosures between parties so that only required and vital information is revealed between parties working together while maintaining confidentiality.
- **Define a time period:** A formal non-disclosure agreement will never leave the duration of the duty to maintain confidentiality to chance or others' interpretation.
- **One-way NDA vs reciprocal NDA**: Understand the parties' requirements, and determine whether the party will reveal more information and whether it will be a one-

way disclosure. Any information the other party must also disclose is; Requirement to have a reciprocal agreement.

- **Conflicting Concerns and Risk Minimisation Approach:** Wording that is good for your client defensively may compromise on the enforcement side; for example, Confidential Information requires marking of information disclosed as 'Confidential,' which increases the client's burden of compliance while decreasing the likelihood of compliance. A risk-reduction strategy would require confidentiality labelling with a 30-day grace period on spoken disclosures.
- **Restriction on copying**: Copying the vital data allows one party to access the other party's business model, source codes, and client information, allowing them to reproduce the organisation. This is a severe issue that might jeopardise the party's future business; thus, it is best to limit data copying.
- **Transfer of ownership clause**: Parties should watch "transfer of ownership provisions" in NDAs in collaboration agreements. Assume a corporation is building software for a manufacturing company that it plans to market once the partnership agreement expires. However, as part of the agreement, the NDA may impose confidentiality on the intellectual property (IP) of such a program, assuming ownership of the same. This is a huge red flag since an NDA should limit the exposure of secret information rather than transfer ownership.
- **Avoid disclosing commercial secrets**: Trade secrets must be safeguarded at all times. Once the responsibilities are fulfilled, NDAs do not provide indefinite protection.
- **Indemnity for violation of confidentiality**: Please see below for an example provision providing indemnity for a breach of privacy. Each party agrees to indemnify and hold the other party harmless from and against any loss, liability, damage, claim, cost, and expense (including legal fees) arising from any breach or non-performance by the Parties or their Representatives of any of the obligations under this agreement, including, without limitation, the obligations regarding the use and safeguarding of Confidential Information.

- **Injunction for violating confidentiality**: Please see the sample clause below for remedies for breach of privacy.

"Receiving party acknowledges that any misappropriation of any of the Confidential Information in violation of this agreement may cause Disclosing Party irreparable harm, the amount of which may be difficult to ascertain, and therefore agrees that the Disclosing Party shall have the right to apply to a court of competent jurisdiction for an order enjoining any such further misappropriation and for such other relief as the Disclosing Party deems appropriate. This right of the Disclosing Party is to be in addition to the remedies otherwise available to the Disclosing Party."

CONCLUSION

In Conclusion, even a simple NDA requires some confidence before we get into an arrangement. If you're having trouble discussing the details of the deal with a third party and they're unwilling to compromise due to their stubbornness. A lawyer should realise that dealing with such a party will be difficult and advise the client appropriately. Breach of confidentiality may be protected under privacy regulations; the terms confidentiality and privacy are roughly identical. Confidentiality is a legal term that refers to the responsibility of confidence that exists between a data collector and a data subject. This might be due to several conditions or regarding various categories of information, such as work, medical, or financial information. An obligation of confidence offers the data subject the right not to have his information used for other purposes or divulged without his agreement unless there are other compelling public-interest grounds. That is when information is used for a purpose other than the one for which it was intended.