

THE PROTECTION OF TRADE SECRETS BILL, 2024 – TESTING THE CONFIDENTIALITY JURISPRUDENCE

ANIRUDHA ASHOK VALSANGKAR*

I. INTRODUCTION

The concept of “confidentiality” has long been recognized and protected by courts in many countries, with causes of action arising from the unauthorized use or disclosure of confidential information. Such causes of action predominantly revolved around breaches of “confidentiality obligations” or the protection of “confidential information” itself. Various judicial decisions from the 18th to the 21st century in common law jurisdictions have applied different principles of law, as the circumstances of each case required, and have protected the underlying “confidential information” or obligations in respect thereof. Over the years, courts have used different legal principles—like those from contract law, tort law, equity, and sometimes property law—depending on the situation and the type of information involved. Since the 1700s, courts have consistently upheld the need to protect sensitive information, whether related to business, government, art, or personal matters, in the past or today, when it involves private or personal information.

While many legal experts have studied how confidentiality laws have developed over time, this article

* Anirudha Ashok Valsangkar, LL.M. (IP), is a practicing Advocate at the Bombay High Court. He received his LL.M. in Intellectual Property Laws from UNH Franklin Pierce School of Law, U.S.A. (Class of 2001) and has over 24 years of experience in IP litigation. Views and Analysis are personal to the author. He can be reached at anirudha.valsangkar@gmail.com

does not focus on that history. Instead, it focuses on the pressing need for a comprehensive statutory framework to safeguard trade secrets and confidential information in India. In doing so, it critically examines the *Protection of Trade Secrets Bill, 2024* (“the Bill”) —a legislative proposal that seeks to codify the protection of trade secrets in India’s rapidly evolving commercial and technological landscape.¹

II. IMPORTANT ISSUES: THE FOUNDATION

In early times, a breach of confidentiality focused on the existence of a contractual confidential relationship between the parties, and in absence of one, a cause of action based on a breach of confidentiality would not succeed. However, as time passed, the jurisprudence on the breach of confidentiality gradually shifted from a focus on a contractual relationship between the parties, to the nature and value of the information, and whether the use of the information was an authorized use or a misuse. Today, a breach of confidentiality is much more than a contractual relationship and the value of the information. The jurisprudence on confidentiality has expanded to engulf:

- i. private information;
- ii. personal information;
- iii. government information;
- iv. unauthorized disclosure of confidential information;
- v. unauthorized access of confidential information;
- vi. unauthorized possession of confidential information;

¹ Law Commission of India, Trade Secrets and Economic Espionage, Report No. 289, 2024, Annexure-I, at 198 [hereinafter Report No. 289] (proposing The Protection of Trade Secrets Bill, 2024 in Annexure-I).

- vii. unauthorized use of confidential information; and
- viii. whether the information affects *in rem* or *in persona*.

It is important to understand exactly what “confidential information” is and how it has been dealt with and protected by various courts to date. Colloquially, “confidential” has many different connotations. The Merriam-Webster dictionary defines “confidential” as one that is intended for or restricted to the use of a particular person, group, or class: private, secret, and interestingly states the first known use of the word to be in 1740.² Black’s Law Dictionary defines “confidential” as, entrusted with the confidence of another or with his secret affairs or purposes; intended to be held in confidence or kept secret.³

It is to be noted that “confidential information” is not defined in any dictionary. Naturally, what follows is that any information that has the attributes of “confidentiality” is “confidential information.” “Confidential information” may be divided, broadly speaking, into four main categories:

- i. trade secrets;
- ii. artistic and literary information;
- iii. government secrets; and
- iv. personal information.⁴

² *Confidential*, MERRIAM-WEBSTER, <https://www.merriam-webster.com/dictionary/confidential> [<https://perma.cc/AJ4R-WMZQ>] (last visited Mar. 31, 2025).

³ “*Confidential*,” BLACK’S LAW DICTIONARY, Black’s Law, [https://www.westlaw.com/Document/Ifeea64ff808411e4b391a0bc737b01f9/View/FullText.html?transitionType=Default&contextData=\(sc.Default\)&VR=3.0&RS=cblt1.0](https://www.westlaw.com/Document/Ifeea64ff808411e4b391a0bc737b01f9/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0) [<https://perma.cc/QCF7-RAE9>] [last visited Feb. 18, 2026].

⁴ TANYA APLIN ET AL., GURRY ON BREACH OF CONFIDENCE § 6.02, (2d ed. 2012).

These categories may at times overlap and thus, “confidential information” is a broad, all-encompassing genus, and trade secrets is merely a specie.

In an action relating to “confidential information” or for breach of confidentiality, the following attributes become relevant:

- i. Quality of Information;
- ii. Relationship;
- iii. Trust;
- iv. Use/Misuse/Springboard;
- v. Unauthorized Access;
- vi. Unauthorized Disclosure;
- vii. *In rem or in persona*;
- viii. Harm / Damages / Unjust Enrichment;
- ix. Tort / Property / Equity / Contract.

One or many of these attributes may be present in a given cause of action. Many landmark cases have demonstrated this fact. *Saltman Engineering Co., Ltd and Ors. v. Campbell Engineering Co. Ltd.* watered down the requirement of needing a contract to exist to even permit an implied confidential relationship, to show that the receiver knew about the confidential nature of the subject matter shared.⁵ Thus, the mandatory requirement of the existence of a contract was forgone, and the focus shifted to the quality of the information and an obligation of confidence imposed on the receiver.⁶ In *Saltman Engineering*, the court relied on a position of law that “if a defendant is proved to have used the confidential information, directly or indirectly obtained from a plaintiff, without the consent, express or implied of the plaintiff, he will be guilty of an infringement of the plaintiff’s rights.”⁷

⁵ *Saltman Engineering Co. v. Campbell Engineering Co.* [1948] 65 RPC 203.

⁶ *Id.*

⁷ *Id.*

Saltman Engineering held that an obligation, based on the confidence, existed and the defendant is bound by “conscience” not to use it.⁸ From this, the jurisprudence started recognizing the equitable principle of “unjust enrichment” by the receiver of the confidential information.⁹

Another facet of the equitable principle of “unjust enrichment” is the Springboard doctrine, which was applied in the law of confidence, in *Seager v. Copydex Ltd.*, wherein the *Seager* court stated:

As I understand it, the essence of this branch of the law, whatever the origin of it maybe is that a person who has obtained information in confidence is not allowed to use it as a springboard for activities detrimental to the person who made the confidential communication, and spring-board it remains even when all the features have been published or can be ascertained by actual inspection by any member of the public.¹⁰

Thus, the court in *Seager* completely waived the requirement that there must be the existence of a contractual relationship, whether express or implied, and recognized the broad principle of equity that those who have received information in confidence shall not take unfair advantage of it.¹¹ The object of the springboard doctrine is merely to ensure that the recipient of confidential information does not obtain an unfair start by misuse of information received in confidence.¹² These principles were later affirmed in *Coco v. A.N. Clark*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Seager v. Copydex Ltd* [1967] 1 W.L.R. 923.

¹¹ *Id.*

¹² CHARLES PHIPPS ET AL., *TOULSON & PHIPPS ON CONFIDENTIALITY* § 6.074, (4th ed. 2020).

(Engineers) Limited, and eventually, three essential requirements for breach of confidentiality were formulated: that the information was of a confidential nature; that it was communicated in circumstances importing an obligation of confidence; and that there was unauthorized use of information.¹³

The three essential requirements for breach of confidentiality were further relaxed in a subsequent decision of the U.K. Court of Appeals in *Imerman v. Tchenguiz and Others*.¹⁴ The Court in *Imerman* recognised that “misuse of private information” was shoe-horned into the law of confidence, and now the law has been extended to apply to cases where the defendant had received the information without the consent of the claimant.¹⁵ It observed the following:

It was only some 20 years ago that the law of confidence was authoritatively extended to apply to cases where the defendant had come by the information without the consent of the claimant. That extension, which had been discussed in academic articles, was established in the speech of Lord Goff of Chieveley in *Attorney General v. Guardian Newspapers Ltd. (No. 2)* [1990] 1 AC 109. He said, at p 281, that confidence could be invoked “where obviously confidential document wafted by an electric fan out of a window...or... is dropped in a public place, and is then picked up by a passer-by.”¹⁶

Thus, the court held that if the law of confidence applies to a defendant who adventitiously, but without authorization, obtains information the claimant expected to be held in confidence, then the law of confidence would also apply to defendants who intentionally, and without

¹³ *Coco v. A.N. Clark (Engineers) Ltd* [1968] RPC 41.

¹⁴ *Imerman v. Tchenguiz and Others* [2010] EWCA (Civ) 908.

¹⁵ *Id.*

¹⁶ *Id.*

authorization, take steps to obtain such information. The court further held that not only unauthorized access to confidential information was treated as a breach of confidentiality, but even unauthorized “looking” at confidential documents was an actionable wrong.

In a recent decision by the Court of Appeal of the Republic of Singapore in *I-Admin (Singapore) Pte. Ltd. v. Hong Ying Ting and Others*, the Court held that the very possession of confidential information amounted to a breach of confidence and would imply “wrongful use” not warranting meeting the traditional third requirement for a breach of confidence.¹⁷ In India, recently, a Constitution Bench of the Supreme Court of India in *Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal* recognized this shift in the analysis for the breach of confidence cause of actions in the context of statutory obligation of confidence under the Right to Information Act, 2005.¹⁸ From the judgments discussed above, it is apparent that it is difficult to establish a bright-line principle in cases involving a breach of confidentiality and “confidential information,” as each case must be decided on its own unique facts and circumstances.

III. INTERNATIONAL OBLIGATIONS: TRIPS

Under Article 39 of the TRIPS Agreement, the member states are obligated to protect “undisclosed information.”¹⁹ Article 39 of the TRIPS Agreement states as follows:

¹⁷ *I-Admin (Singapore) Pte. Ltd. v. Hong Ying Ting and Others* [2020] SGCA 32 (Sing.).

¹⁸ *Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal* (2020) 5 SCC 481.

¹⁹ Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), art. 39, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 [hereinafter TRIPS Agreement] (amended Jan. 23, 2017).

*he Protection of Trade Secrets Bill, 2024 – Testing the
Confidentiality Jurisprudence* **513**

Article 39.1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.

2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices¹⁰ so long as such information:

(a) 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) has commercial value because it is secret; and

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

3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.

Notes:

10. For the purpose of this provision, “a manner contrary to honest commercial practices” shall mean

at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.²⁰

As is apparent, “undisclosed information” is a neutral term, and the term is broad enough to include trade secrets, general confidential business information, commercial and technical information.²¹ Although Article 39 of the TRIPS Agreement does not specify the manner in which such protection is accorded, it lays down minimal obligations of protecting “undisclosed information.”²² Since the TRIPS Agreement relates to the trade-related aspects of intellectual property, it could be argued that the obligation to protect “undisclosed information” imposed under Article 39 could only cover “business information” or “trade secrets”, including data submitted to government agencies, and not other types of information, such as private information.²³ However, it would be desirable to codify the law of confidence so that the jurisprudence is harmoniously applied to all types of “undisclosed information,” whether as a “trade secret” or otherwise.

IV. THE PROTECTION OF THE TRADE SECRETS BILL, 2024 (“THE BILL”):

This article argues that the Bill proposed *vide* Report No. 289 by the Law Commission of India, not only fails to comply with the mandatory obligations under the TRIPS Agreement, but also appears to destabilize the already evolved jurisprudence relating to “confidential

²⁰ *Id.*

²¹ *Id.*; see Report No. 289, *supra* note 1, ¶ 3.1, at 23.

²² TRIPS Agreement, *supra* note 19, art. 39.

²³ *Id.*

information” or “breach of confidentiality.” While explaining the reasons for non-compliance, the provisions of the Bill are tested against established cases to examine if the outcomes would change if the Bill is enacted into law. For this purpose, although comments can be provided in respect of other proposed sections, arguments are limited to Sections 2, 3, and 4 of the Bill.

Firstly, even by its title and the preamble, the Bill applies only to “trade secrets” and not to “undisclosed information,” including data submitted to government agencies, as mandated under Article 39 of the TRIPS Agreement.²⁴ The Law Commission incorrectly alleged in its Report that “there is no need to include data exclusivity within the purview of the proposed legislation on trade secrets.”²⁵ While excluding protection for data submitted to government agencies, the Law Commission not only misinterpreted the provisions of the TRIPS Agreement, but also heavily focused on the importance of ensuring access to medicines, and failed to recognize the corresponding “confidentiality” and related obligations.²⁶ The Law Commission thus appears to have failed to balance conflicting interests. Although the Law Commission Report states that the proposed Bill is suggested as a *sui generis* legislation, the Bill clearly and consciously narrows down its ambit to trade secrets.²⁷ Thus, the Bill fails to propose legislation that would cover the mandated scope under the TRIPS Agreement while addressing Indian concerns about access to medicines. Conversely, the Bill also fails to specify whether other forms of “undisclosed information” that are not covered by the Bill would still be protected under common law. Additionally, the Bill fails to specify the modalities of resolving the conflict between the

²⁴ See Report No. 289, *supra* note 1, Annexure-I, at 198.

²⁵ *Id.* ¶ 8.34, at 194.

²⁶ See, e.g., *id.* ¶ 3.20, at 38, ¶ 5.46, at 128, ¶ 8.20 at 186, ¶ 8.35, at 195.

²⁷ *Id.* ¶ 8.4, at 177.

common law and the proposed Bill. While adopting a *sui generis* legislation, the proposed Bill was an opportunity to codify a law of confidence that would cover a broad range of “confidential information” and clarify what would be considered “breaches” or “misappropriation.” Instead, the Bill is vague and leaves its provisions open for interpretation by courts.

The definition of a “trade secret” in Section 2(f) of the Bill is almost *pari materia* (except for Section 2(f)(iv)) with the second paragraph of Article 39 (Article 39.2) of the TRIPS Agreement.²⁸ This reveals yet another fallacy. Article 39.2 defines the minimal obligations of protecting “information” or “undisclosed information.”²⁹ By adopting the definition of “undisclosed information” for “trade secrets” the Bill treats both as interchangeable, and creates confusion in the understanding of the fundamental jurisprudence, interpretations, and application of the settled law on confidence.³⁰

Secondly, Section 3 of the Bill interestingly uses the word “holder” to refer to the “proprietor” or the “owner” of the trade secrets.³¹ This is reflective of the Law Commission’s efforts to specifically use “holder” to avoid recognizing trade secrets as a form of “property” and the owner thereof, as “proprietor,” as the Law Commission believes that it cannot have “property-like” conception even though this is the case with other intellectual property.³² This has far-reaching implications, including for taxation and stamp duties payable on instruments dealing

²⁸ Compare *id.* Annexure-I § 2(f), at 199 (defining “trade secret”), with TRIPS Agreement, *supra* note 19, art. 39.2 (defining “undisclosed information”).

²⁹ TRIPS Agreement, *supra* note 19, art. 39.2.

³⁰ See *id.*; Report No. 289, *supra* note 1, Annexure-I § 2(f), at 199.

³¹ Report No. 289, *supra* note 1, Annexure-I § 3, at 200 (discussing the holder of trade secret).

³² See *id.* ¶ 8.7, at 178.

with “trade secrets.” Further, Section 3 of the Bill, while fundamentally appearing to create a negative right in favour of a holder, fails to achieve the underlying objects by not providing an ‘exclusive right to prevent third parties’ in favour of the holder.³³ This is despite the fact that Article 39.2 provides for a “possibility of *preventing* information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices” with some exceptions outlined therein.³⁴ A provision along the lines of Section 48 of the Patents Act, 1970 ought to have been suggested to ensure the objects of the legislation are achieved.³⁵ From the general scheme of Sections 3, 4 and 5 of the Bill, it is evident that “lawful acquisition” would not amount to infringement of the rights of the holder of trade secret.³⁶ Section 4 of the Bill appears to break-down what is “lawful acquisition” rather than providing clarity on interplay between the holder’s rights and lawful acquisition, breaches or misappropriation.³⁷ The Bill thus appears to put the “holder” and the “lawful acquirer of information” on an equal footing.

Sections 4(1) and (2) appear to be exceptions to Section 4(3), although they have been arranged conversely.³⁸

From an enforcement perspective, Section 3(3) appears relevant, along with the definitions section. The language suggested by the Bill “to prevent further misappropriation or disclosure of trade secret in the public domain” clearly implies that, in an enforcement action,

³³ *See id.* Annexure-I § 3, at 200.

³⁴ TRIPS Agreement, *supra* note 19, art. 39.2.

³⁵ *See* The Patents Act, 1970, § 48 (India).

³⁶ *See* Report No. 289, *supra* note 1, Annexure-I § 3–5.

³⁷ *Id.* Annexure-I § 3, at 200.

³⁸ *Id.* Annexure-I § 4, at 200 (discussing how a trade secret may be lawfully acquired).

“accidental disclosure” or “unlawful disclosure” can be restrained by the holder.³⁹

Turning to the critical part of the enforcement, as to what amounts to “misappropriation”, it is important to note that Article 39.2 of the TRIPS Agreement enables preventing information from being “disclosed to others,” “acquired by others,” and “used by others,” without the consent of the person controlling the “undisclosed information.”⁴⁰ If the Bill is considered alongside Article 39 of the TRIPS Agreement, and hypothesized with the landmark cases discussed above, to determine if their outcomes would have changed or stayed the same, then their outcomes may appear as follows.

The *Saltman* verdict is a “used by others” case and would therefore be in consonance with the Article 39.2 mandate of the TRIPS Agreement.⁴¹ Testing the *Saltman* facts at the touchstone of the provisions of the Bill, it would appear that the *Saltman* verdict would most likely fall under Section 2(d)(ii)(III) of the Bill, where it stipulates “misappropriation” to be also when “use without consent by a person who . . . is in breach of a contractual or *any other duty to limit the use of the trade secret.*”⁴²

The *Seager* verdict appears to be a “used by others” case and the Article 39.2 wording of the TRIPS Agreement would enable the courts with the flexibility to incorporate the Springboard doctrine, thus keeping the *Seager* outcome intact.⁴³ Testing the *Seager* facts at the touchstone of the provisions of the Bill, however, it would appear that the

³⁹ *Id.* Annexure-I § 3(3), at 200.

⁴⁰ TRIPS Agreement, *supra* note 19, art. 39.2.

⁴¹ *Saltman Engineering Co. v. Campbell Engineering Co.* [1948] 65 RPC 203.

⁴² Report No. 289, *supra* note 1, Annexure-I, § 2(d)(ii)(III), at 199 (emphasis added) (defining misappropriation).

⁴³ *Seager v. Copydex Ltd* [1967] 1 W.L.R. 923 (discussing springboard injunctions).

Bill does not provide comfortable flexibility for the courts to incorporate the Springboard doctrine to ensure that the *Seager* verdict is intact. It seems that at this time Section 2(d)(ii)(III) may also have to be relied on; however, the Bill does not provide the flexibility to incorporate the Springboard doctrine into this Section.⁴⁴ The *Seager* verdict may change if the *Seager* facts are applied to the said provisions of the Bill.

The decision of the Court of Appeals in *Imerman* would differ had it been decided under the Bill.⁴⁵ Considering the facts of *Imerman*, the “private information” sought to be protected in *Imerman* would not even qualify as a “trade secret” as defined under Section 2(f) of the said Bill.⁴⁶ The facts of the *Imerman* verdict were that the claimant’s husband shared an office and a computer system with his wife’s brother, the defendant.⁴⁷ When the marriage broke down and the wife petitioned for divorce, the defendant, fearing that the husband would conceal his assets to prevent the wife from obtaining a fair financial settlement, accessed the claimant’s computer without his permission and copied information and documents stored there.⁴⁸ The printed out material was handed to his solicitor, and the privileged documents therein were removed.⁴⁹ The remaining files were to be used in the divorce proceedings in relation to her application for ancillary financial relief.⁵⁰ The *Imerman* court granted an injunction in favour of the claimant from use of such “confidential documents.”⁵¹ The Bill clearly

⁴⁴ See Report No. 289, *supra* note 1, Annexure-I, § 2(d)(ii)(III), at 199.

⁴⁵ *Imerman v. Tchenguiz and Others* [2010] EWCA (Civ) 908.

⁴⁶ Report No. 289, *supra* note 1, Annexure-I § 2(f), at 199.

⁴⁷ *Imerman v. Tchenguiz and Others* [2010] EWCA (Civ) 908.

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.*

fails to protect “private information” within the scope of the *Imerman* facts. The court in *Imerman*, while discussing the historical development of this branch of law, recognized that ‘misuse of private information’ was shoe-horned into the law of confidence.⁵² If enacted, the Bill would not be applicable to such “private information,” and it would also raise doubts on the general jurisprudence on the law of confidence.

Similarly, if the provisions of the Bill are applied to the recent decision of the Court of Appeal of the Republic of Singapore in *I-Admin (Singapore) Pte. Ltd.*, it may not be held in the same manner.⁵³ In *I-Admin (Singapore) Pte. Ltd.*, the Court of Appeal of the Republic of Singapore affirmed the jurisprudence that the very possession of confidential information amounted to a breach of confidence and would imply “wrongful use” not needing to meet the traditional third requirement for breach of confidence.⁵⁴ It is pertinent to note that the Bill does not stipulate “possession” itself to be a “misappropriation.”⁵⁵

V. AN EXAMPLE:

The proposed legislation should, at a minimum, ensure the protection of all types of information shared in confidence, along with the corresponding obligations. A useful analogy to illustrate the core elements of “confidentiality” could be that of a bank locker wherein the “contents” kept in the bank locker would be akin to ‘confidential information.’ It is irrelevant whether the nature of the “content” in the locker is valuable or not (value being relevant to the owner thereof). What is

⁵² *Id.*

⁵³ *I-Admin (Singapore) Pte. Ltd. v. Hong Ying Ting and Others* [2020] SGCA 32 (Sing.).

⁵⁴ *Id.*

⁵⁵ See Report No. 289, *supra* note 1, Annexure-I § 4(1)(b), at 200.

relevant is that the content is shielded from unauthorized access, and such confidential information should be protected irrespective of whether it comprises personal data, official records, or seemingly trivial material. The critical factor is that reasonable safeguards are in place.

Any attempt by an unauthorized third party, including bank officials or similar actors—whether bound by contract or not—to open, access, inspect, retain/possess, or disclose the contents of the locker, even without physically removing or duplicating the contents, would constitute a breach of confidentiality. Exceptions could include instances in the public interest or contrary to public policy.

Unfortunately, the Bill fails to address many of the complex dimensions of confidentiality and does not appear to adopt a forward-looking or sufficiently protective approach for the protection of confidential information or trade secrets.

VI. CONCLUSION:

The discussion above makes it apparent that not only does the Protection of Trade Secrets Bill, 2024 fail to comply with Art. 39 of the TRIPS Agreement, but it will also tend to create confusion in the application of the jurisprudence of the law of confidence. Enacting legislation only to cover part of the law of confidence (i.e., trade secrets) may not be in the best interests of the country. With a vague statute like this Bill, much of the job is left to the courts to interpret. With a long-standing requirement to codify the law of confidence, this would be India's best opportunity to legislate a *sui generis* legislation that not only meets international commitments but also reduces the burden of an already overburdened court system.