REVERSE ENGINEERING IN TRADE SECRETS: A COMPARATIVE ANALYSIS OF INDIA'S 2024 BILL AND THE EU DIRECTIVE

Lalith Swetha, B.A.LL.B. (Hons.), Sastra University

ABSTRACT

Indian law treats reverse engineering as a fair way to learn a trade secret, but it has no statute to say so, relying instead on equity, confidence and contract, while the Law Commission's draft Protection of Trade Secrets Bill, 2024 would make it a lawful means of acquisition without defining the term. This leaves open whether a contract can switch that freedom off, and in a market where software and connected devices are sold in forms competitors can study, an unclear answer exposes both honest competitors and secret holders to risk. The paper argues that the Bill's reverse engineering rule cannot be read alone and must be tested against the Contract Act, the rules of evidence and the Copyright Act's software exceptions before it is enacted. Existing scholarship, including Lemley, Bone, Cohen and Lemley, broadly agrees that reverse engineering spreads know-how and keeps markets competitive, though it accepts limits where copying erases the first mover's lead. These works are largely American or concern the proposed EU Directive, and none compares the Indian draft Bill with the Directive or asks how contract terms, proof requirements and software decompilation exceptions interact in India.

This paper reads Section 4 of the Bill against Article 3 of the EU Directive and its Recitals 16 and 17, with brief reference to US law, to show that the Bill omits the Directive's recitals and its qualifier that a limiting duty be legally valid. It then tests the Bill against Section 27 of the Contract Act, the burden of proof under the Bhartiya Sakshya Adhiniyam, 2023, and Section 52(1)(aa) to (ac) of the Copyright Act, 1957, noting that India has no equivalent of Article 6(2) or Article 8 of the Software Directive. Because no Indian court has ruled on a clause prohibiting reverse engineering, several of its conclusions are predictions rather than settled law. The paper's contribution is to show how these layers fit together and where they leave gaps, so that Parliament can clarify the reach of contractual prohibitions, the allocation of proof and the later use of lawfully decompiled information.

Keywords: pre empt, interoperability, decompilation, directives.

1. INTRODUCTION

Background and significance

Every business has something to keep itself. It could be a recipe, a customer list, a factory process or a block of source code. If a rival hears of it, the lead is lost. Trade secret law is designed to protect such kind of information.

India has no statute on trade secrets. Instead, courts rely on equity, fairness and contract[1]. The Law Commission of India in March 2024 recommended a separate law. It appended the draft Protection of Trade Secrets Bill, 2024 to its 289th Report[2]. The Bill even though in the draft stage raises a question Indian court have seldom faced. What happens when you learn a secret through product disassembly?

The question becomes more urgent each year. Software and connected devices are released to the public in forms that competitors can examine and try. With the advancement of new technology, the scope of what can be reverse engineered continues to be broaden[3].

Statement of Research Problem

The draft Bill says that reverse engineering is a lawful means of obtaining a trade secret but does not define the term. Further, there is no mention about whether a contract can disable that freedom. The EU Directive allows contract to prohibit reverse engineering, but other law can restrict those contracts. India adds a Contract Act that voids restraint of trade and a Copyright Act that permits some software decompilation. Nobody has asked how these layers fit together. This paper asks that question.

Why Trade Secrets Need Protection?

At common law, a person who has a secret has a limited, property – like interest in it as long as it is secret. The holder may seek an injunction for a breach of confidence. Once the secret is

[1] Dep't-Related Parliamentary Standing Comm. on Commerce, *Review of the Intellectual Property Rights Regime in India*, Report No. 161 (2021)
[2] Law Commission of India, *Trade Secrets and Economic Espionage*, Report No. 289 (Mar. 5, 2024) [Law Commission Report].
[3] Gregory S. Bombard and Andrew (A.J.) Tibbetts for Massachusetts *Lawyers Weekly*

out, the right ends. It works nothing like a patent[4].

The law protects secrets because they are commercially valuable. The TRIPS Article 39(2) test is in three parts. The information must be confidential, it must be valuable and its holder must take reasonable steps to keep it so[5]. The Black's law dictionary defines trade secret in practical terms. It is a formula, process or method that is kept secret to have an advantage over competitors[6].

Protection matters because a patent demands disclosure and expires. A small firm with a clever process may prefer secrecy, and it needs legal backing to make that choice work. Yet the law must also leave room for honest competition. Reverse engineering is where those two aims meet.

Scope and Limitation

The paper studies reverse engineering, a legal way to get a trade secret. It compares India (draft Bill and existing law) with the EU with brief reference to the US. It does not cover patent law, economic espionage or criminal remedies. There are two limits that matter. The Bill is not law, so no court has applied it. Further, I could not find any Indian case that directly tests a clause prohibiting reverse engineering. Hence some conclusions are predictions.

Research Methodology

This is a doctrinal study. The primary sources are statutes, the draft bill, EU directives and precedents. The secondary sources are journal articles, the Law Commission's report and commentary. Each provision is closely read and compared with EU text which has been tested against decided cases.

LITERATURE REVIEW

There are 5 peer reviewed works that shaped this paper. The following paragraphs discuss about these papers along with their limitations.

[4] Law Commission Report, *supra* note 2; A. 0. Smith v. Pet. Iron Works, 73 F(2) 531
[5] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39(2), Apr. 15, 1994, 1869 U.N.T.S. 299
[6] *Trade Secret*, Black's Law Dictionary (11th ed. 2019)

1. Samuelson and Scotchmer examine reverse engineering from a legal and economic perspective[7]. They argue that the law should protect it in most settings. It spreads know – how and keeps the market competitive. They also accept limit where copying wipes out the first mover's lead. Their paper is American and precedes the EU Directive. The paper doesn't discuss about contracts that prohibit reverse engineering. I accept their premise and subject it to the test of Indian law. This is relevant here because Section 4 of the Bill depends on the same notion.

2. Lemley defends the treatment of trade secrets as intellectual property rights[8]. He argues that the law reduces the cost of secrecy and encourages companies to invest in information. He acknowledges those rights are limited by reverse engineering and independent discovery. He is focused on US law and does not make comparisons with India or the EU. I use his framings but consider how other systems draw the limit. His view also fits the Bill, which gives holders a statutory right to use, disclose and license their secrets

3. Bone challenges the bedrock of trade secret doctrine[9]. He argues that the familiar justifications of property and contract do not do a very good job of accounting for the rules. His work is theoretical and provides little scope for reverse engineering. This paper is more limited, and more pragmatic. It asks how a reverse engineering rule work when a contract is entered. Any Indian reform should still be able to answer his fundamental challenge: why does the rule exists at all?

4. Aplin criticizes proposed EU Directive before its adoption[10]. She looks at, among other things, how the draft handled reverse engineering and contractual limits. Her article is about the proposal, not the final text, and India is not part of the discussion. Her concerns regarding Recitals 16 and 17 has been duly noted and is read as limits to test rather than settled answers.

5. Reverse engineering is important to software competition and follow – on innovation,

[7] Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 Yale L.J. 1575 (2002)
[8] Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 Stan. L. Rev. 311 (2008)
[9] Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 Cal. L. Rev. 241 (1998)
[10] Tanya Aplin, *A Critical Evaluation of the Proposed EU Trade Secrets Directive*, 2014 Intell. Prop. Q. 257

argue Cohen and Lemely[11]. Their main target is patent. They don't study trade secret statutes or contract terms. I take their argument about software, but have further dwelled into whether trade secret and copyright rules protect or prohibit it. Their concern is especially relevant in relation to a clause that prohibits the study of software that you have lawfully purchase.

Research Gap: None of these works compares the Indian draft Bill with the EU Directive on reverse engineering. None asks how contract, evidence and software decompilation exceptions interact in India. Indian peer – reviewed commentary on the draft Bill is also thin, which is natural for a proposal this recent. This paper tries to fill that gap.

THE TRADE SECRETS BILL

Trade secrets in India are protected under the law of confidence, equity and contract. There is no law covering misappropriation. Parliamentary Standing Committee on Commerce termed the lack of such a provision as a "gap" in the country's IP system[12].

Article 39 of TRIPS obliges the members to protect undisclosed information against dishonest commercial practices[13]. Since then, the US, South Korea and the EU have enacted specific legislation. India has so far avoided that route.

The 22nd Law Commission changed the debate. Its 289th Report, dated 5th March, 2024, recommends a sui generis statute and annexes a draft Bill. There are 13 sections in the draft, arranged in four chapters. Section 2(f) defines a trade secret on TRIPS lines. Section 4 lists the lawful ways to acquire one. Section 13 provides that the Bill supplements existing remedies and does not replace them.

Two features here are important. First, the Commission says, a trade secret is not a monopoly. Others may obtain the same information lawfully. Secondly, the Bill does not define reverse engineering. The Bill is still a recommendation.

[11] Julie E. Cohen & Mark A. Lemley, *Patent Scope and Innovation in the Software Industry*, 89 Cal. L. Rev. 1 (2001)
[12] Dep't-Related Parliamentary Standing Comm. on Commerce, *supra* note 1
[13] TRIPS, *supra* note 5, art. 39

REVERSE ENGINEERING

It is the process of analysing a product to uncover non public information about the product. A purchaser will disassemble the item, test it, analyse its behaviour and determine how it was made. This is generally treated as fair under the Trade Secret Law. The US Defend Trade Secrets Act includes improper means as theft, bribery, misrepresentation, breach of duty of secrecy and espionage. It specifically excludes reverse engineering and independent derivation[14]. The Supreme Court said much the same in Kewanee[15]. A holder cannot stop a person who acquires a product lawfully and studies it.

The Freedom has its limits. The creation of liability through reverse engineering is still possible if the product or the information came through theft, fraud or breach of a non-disclosure agreement. It may also be prohibited by contract, subject to enforceability. Even where the study itself was lawful, a patent may prohibit making or selling the invention.

2. COMPARATIVE ANALYSIS

Section 4 of the draft Bills deals with lawful acquisition, use and disclosure. A person may obtain a trade secret by three methods. The first being independent discovery or creation. The second is observation, study, reverse engineering, disassembly or testing of a product that is public or lawfully in the acquirer's possession if the acquirer owes no duty to limit the acquisition. The third is any other practice that is consistent with honest commercial practices[16]. Section 4 is the sole provision that expressly deals with reverse engineering.

The drafters incorporated Article 3 of the EU Directive[17]. Article 3(1) sets out four lawful routes: (a) independent discovery or creation, (b) observation, study, disassembly or testing of a lawfully held or public product, (c) exercise of workers' information and consultation rights (d) any other practice consistent with honest commercial practices. The operative text does not use the term "reverse engineering." The recitals do[18].

Recital 16 states that reverse engineering of a lawfully acquired product is lawful 'unless

[14] 18 U.S.C. Section 1839(6) (2016) [DTSA]
[15] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974)
[16] Bill, *supra* note 16, Section 4
[17] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, 2016 O.J. (L 157) 1 [Directive 2016/943].
[18] *Id.* art. 3(1).

contractually agreed otherwise'. It further states that the law can limit contractual freedom[19]. Recital 17 raises a different concern. In some industries, products that are launched can be readily reverse engineered. It encourages slavish copying. The Directive does not harmonize the law of unfair competition but it asks national legislators to keep the risk in view[20].

American law arrives at a similar destination by two roads. Reverse engineering is a legitimate method recognised by the Uniform Trade Secrets Act[21]. It is excluded from improper means by the Defend Trade Secrets Act[22]. The American law of contracts favors the drafter. In Bowers, the Federal Circuit upheld a licencing term that prohibited reverse engineering and found that copying law did not pre – empt the license[23].

Both texts also provide a catch – all for honest commercial practice. That language allows courts to incorporate standards of fairness. Indian courts do not have a body of settled cases on what constitutes hones practice in trade secret disputes. Take a software license to see how the test works. The initial requirement is satisfied because the product is public. If the license is up to date, it is lawful to possess. The third element requires absence of a duty to limit acquisition, depends on the license terms. If there is a clause prohibiting disassembly, there may be a "duty to limit the acquisition", and the lawful route closes.

The Directive raises one more question: is that duty of legal effect? The Bill's language does not. Three differences stand out. First, the Bill is very similar to Article 3(1)(b) having also borrowed from 3(1)(a) and 3(1)(b) but leaves out the recitals. The recitals contain the purpose of the contract and the warning of imitation. But a court reading the Bill in isolation will see only the bare rule. Secondly, the Bill mentions a "duty to limit the acquisition." The text omits the words "legally valid" from the Directive. That gap matters. The Directive lays down minimum rules under Article 1(1) and member states are free to go further[24]. However, it also says it must comply with certain listed provisions including Article 3. That is the directive is a floor that national law builds on, whereas the Bill once enacted would be the entire rule applied by the Indian courts.

[19] *Id.* recital 16
[20] *Id.* recital 17
[21] Unif. Trade Secrets Act § 1 cmt. (Unif. L. Comm'n 1985)
[22] DTSA, *supra* note 19, Section 1839(6)(B).
[23] Bowers v. Baystate Techs., Inc., 320 F.3d 1317 (Fed. Cir. 2003)
[24] Directive 2016/943, *supra* note 22, art. 1(1).

3. STATUTORY REVERSE ENGINEERING RIGHTS AND CONTRACTUAL REMEDIES

THE EU POSITION

Reverse Engineering has an unusual place in trade secret law. The EU and India, both treat it as a fair way to learn a secret. They differ on how far a contract can take that freedom away.

The Article 3(1)(b) of the European Union Directive provides that a trade secret is lawfully obtained by observation, study, disassembly or testing of a product. The product must be lawfully in the possession of the acquirer or available to the public. The acquirer also must not be legally obligated to refrain from making the acquisition[25]. This is supported by Recital 16. It makes reverse engineering of a lawfully acquired product a lawful means unless the parties have otherwise agreed. It then states that the freedom to make such agreements may be limited by law[26]. So, a contract can close the door, but not always.

This allows companies to use NDAs, licensing terms and no – disassembly clauses. This is generally the case for hardware, chemical or industrial products, but national contract law applies. The Directive also only lays down minimum rules under Article 1(1), which sets a minimum standard, so member states may offer broader protection, provided they comply with listed provisions including Article 3[27].

The main exception is software. Article 6 of the Directive 2009/24/EC allows decompilation for interoperability. Article 8 makes contrary contract terms null and void. Article 5(3) also protects observing, studying and testing how a program works[28]. In some cases, a clause may run counter to consumer law on unfair terms, and competition law[29].

THE INDIAN POSITION

India works differently. There is no trade secret statute in force. Courts use contract and the

[25] *Id.* art. 3(1)(b)
[26] *Id.* recital 16
[27] *Id.* art. 1(1).
[28] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs, arts. 5(3), 6, 8, 2009 O.J. (L 111) 16 [Directive 2009/24/EC].
[29] [29]Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts, 1993 O.J. (L 95) 29 [Directive 93/13/EEC]; Consolidated Version of the Treaty on the Functioning of the European Union arts. 101–102, 2012 O.J. (C 326) 47

equitable duty of confidence to protect secrets. In its 289th Report, the Law Commission had recommended a Protection of Trade Secrets Bill, 2024 which is in a draft stage[30]. The draft provides that reverse engineering of a lawfully obtained product is an authorised means of acquiring information[31].

Agreements in restraint of Trade are void by virtue of section 27 of the Indian Contract Act, 1872[32]. It is most often used by courts in employment cases. Post – employment non competes are generally considered unenforceable. The confidentiality duties are treated differently. In Desiccant Rotors, a former employee prohibited from using employer's confidential technical information by Delhi High Court[33]. In American Express Bank v Priya Puri, the court set a limit on such claims. The employer had to show real confidential information, not general skill or knowledge[34].

The older Indian cases rests on the equitable duty of confidence. The duty binds a person who receives information in confidence. For someone who lawfully buys a product and studies it receives nothing in confidence, so the duty has little to bite on. That is a reasoned inference, not a holding.

The catch being, none of the case deals with reverse engineering. So, the idea that section 27 would strike down such clause is a fair prediction and not the settled law. A court might uphold a narrow clause between two commercial parties. It might strike a broad clause that locks up publicly available technology.

COMPARING THE TWO

The two systems pull against each other. The EU begins with freedom of contract and other rules may curtail it. India starts with a strong public policy against restraints of trade but the answer for reverse engineering clauses is yet to be tested.

For firms working across border, the governing law of the contract matters as much as the trade secret rules. However, a lawful act of reverse engineering under Indian law may still constitute a breach of a contract enforceable under the law of a member state. Such a risk exists only if

[30] Law Commission Report, *supra* note 2
[31] Bill, *supra* note 16, Section 4
[32] The Indian Contract Act, 1872, Section 27, No. 9, Acts of Parliament, 1872 (India) [Contract Act].
[33] Desiccant Rotors Int'l Pvt. Ltd. v. Bappaditya Sarkar (Del. HC, 2009)
[34] Am. Express Bank Ltd. v. Priya Puri, (2006) III LLJ 540 (Del.)

the contract is binding on the acquirer and if that law treats the clause as valid.

4. EVIDENTIARY REQUIREMENTS FOR PROVING INDEPENDENT REVERSE ENGINEERING

Who must Prove What?

A claimant in an action for misappropriation must prove that:

(i) The information had secrecy

(ii) The information had value

(iii) The information was improperly acquired, used or disclosed by the defendant.

(iv) Reasonable steps were taken to keep it secret

A common response is to assert that the information was obtained by reverse engineering: I bought the product and worked it out by myself. India has no trade secret rule which addresses the allocation of the burden of proof. The general rule is that a party which asserts a fact must prove it. The Indian Evidence Act, 1872 stated this in sections 101 – 103. The Bhartiya Sakshya Adhiniyam, 2023 replaces that Act from 1 July, 2024[35]. Applying the rule, the claimant must prove the wrong. If the defendant pleads a lawful route, they must then lay down the facts upon which they rely. The civil standards apply: the balance of probabilities. At the interim stage, Indian courts ask the usual questions about interlocutory injunctions: a prima facie case, balance of convenience and irreparable harm. A defendant who cannot produce records may find an interim injunction granted against them before the trial.

A second rule is to the same effect. The old Act placed the burden of proof for facts which were especially within the knowledge of a party upon that party, and the new Act retains the rule[36]. How a team built a product is a fact which the defendant knows best. There is no reported decision that settles the points. The directive leaves burden of proof to national procedural law and the Bill's text, is silent too.

[35] The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India) [BSA]
[36] *Id.* Section 109 BSA, formerly Indian Evidence Act, 1872, Section 106].

What good proof looks like?

A strong defence will include four areas. The first is lawful acquisition of the product under investigation in the form of invoices, licenses and serial numbers of the item. The second is a clean path, meaning documentation that no one on the team had access to the subject's secrets previously. The third is a dated trail, exemplified by laboratory results, notes and revision control history. Fourth, a reasonable timeline is crucial to the defense, as the reverse engineering process is notoriously time – consuming and expensive, and any significantly short development window should raise eyebrows.

Industry "clean room" practice can provide the basis for the defense strategy. In this case, one team studies the product and compiles a specification document, while the other, which has no access to the original, uses it to develop a competing product, and a reviewer checks all details exchanged between the teams. It is crucial to identify witnesses in advance, as engineers who worked on the second team can testify to their observations and actions[37]. A key piece of evidence would be the specification document which is carefully kept.

Electronic records and experts

Much of this evidence takes the form of electronic records: logs, notes and emails. Indian courts demand a certificate before accepting electronic records as evidence. The Supreme Court has sets this out in Anvar under Section 65B of the old Act and in Arjun Panditrao more recently[38]. A firm that keeps records but cannot certify them risks losing them as evidence. Expert opinion also pays a role since a judge may not be in a position to compare code or designs without assistance.

Limits of the defence

A defence requires consistency. Suppose an engineer leaves the claimant and joins the defendant. The court will be asking itself whether the reverse engineering merely confirmed what the engineer already knew. A clean process cannot wash a tainted team. These are inference that courts can draw. They are not rules. In practice the evidential burden may well

[37] Compare Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992) (disassembly of a product for study)
[38] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 [VERIFY pinpoint]; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1

be transferred to the defendant once the claimant has shown a close match between the two products and nothing in Indian law says when the shift should take place. A clearer rule would have helped both sides.

5. TRADE SECRET PROTECTION AND THE COPYRIGHT EXCEPTION FOR SOFTWARE DECOMPILATION

The Indian Exceptions

Section 52 of the Copyright Act, 1957 contains certain acts which are exempted from copyright infringement. Section 52(1) contains four clauses on computer programs, and the first three are relevant here. According to (aa) of Section 52 of the Copyright Act, 1957, any lawful possessor of a computer program can make copies or adaptation of the program to use it for the purpose for which it is provided or to make back – up copies. According to (ab) of Section 52, adaption or copy of the computer program can be done if such action is necessary to gain access to the information which is needed to achieve interoperability of an independently created computer program. The information which is necessary to achieve interoperability, which is not otherwise available, can be used. According to (ac) of Section 52, permits observing, studying or testing the functioning of a program to determine the ideas and principles underlying its elements while performing acts necessary for the functions for which it was supplied.[39]It may be noted that the Copyright Act does not define decompilation and interoperability. Moreover, in Copyright Act, the term lawful possessor may be wider term than person having a right to use the computer program in the EU.

The EU Model

The EU Software Directive (originally 91/250/EEC, now codified as 2009/24/EC) is the model. Article 5(3) provides that a right to use a copy may be exercised by observing, studying and testing it to understand its ideas and principles. Article 6 permits decompilation for interoperability subject to certain conditions. Decompilation may be done by a licensee or other person with a right to use a copy, or by someone authorised on their behalf. Information must not be readily available and acts must be confined to the extent necessary[40]. Article 6(2) bars

[39] The Copyright Act, 1957, Section 52(1)(aa), (ab), (ac), (ad), No. 14, Acts of Parliament, 1957 (India) [Copyright Act]
[40] Directive 2009/24/EC, *supra* note 33, art. 6(1

using the information obtained for purposes other than interoperability of an independently created program, passing it on except as necessary for that purpose, or using it to develop, produce or market a substantially similar program or to commit any other copyright infringement[41]. Article 8 declares any contrary terms in a contract between the parties to be null and void[42]. Article 6(3) further protects right holders by providing that the exception is subject to the condition that it must not be to the detriment of the legitimate interests of the right holder of the program which consists or might consists of a conflict with the normal exploitation of the program.[43]

The Court of Justice of the EU has protected users' rights while keeping them within their stated limit. In the case of SAS Institute, it was held that a license could not prevent a lawful user examining a program to ascertain how it worked[44]. In Top system, decompilation was held to be permissible to correct errors but subject to the above conditions[45].

Where Trade Secret Law Enters?

Copyright generally protects expression, not ideas, functionality or algorithms. Trade Secret law therefore often does the heavy lifting for software. Decompilation turn object code into something readable, exposing secrets in the process. Under the draft Bill, acquiring a secret through reverse engineering is lawful if the product is public or lawfully possessed and no duty limits the acquisition. Copyright Act and the Bill agree on the first step.

They may part ways on the next one. Article 6(2) restricts further use of what you discover through decompilation. But Section 52(1)(ab) has no such restriction: it speaks of acts necessary to obtain information and says nothing of their subsequent use. A competitor could decompile for the purpose of interoperability and then use what they learned to create a similar program. Copyright law may not stop them if they take only ideas or functionality, but copying expression would still infringe. A duty, such as a confidentiality term, would be needed for trade secret law to restrict later use. Whether lawful acquisition under Section 4 also protects later use is untested. The interaction between the Bill and Section 52 has not been tested in courts. The safest reading is that lawful decompilation does not give subsequent misuse of such

[41] *Id.* art. 6(2).
[42] *Id.* art. 8
[43] *Id.* art. 6(3)
[44] Case C-406/10, SAS Inst. Inc. v. World Programming Ltd., ECLI:EU:C:2012:259
[45] Case C-13/20, Top Sys. SA v. Belgian State, ECLI:EU:C:2021:811

information a green flag. Section 4 of the Bill speaks of use and disclosure as well as acquisition, which supports this view. Contract adds a third layer. There is nothing in the Indian Act comparable to Article 8. While clause prohibiting decompilation will not turn off the copyright exception, it might provide grounds for a claim for breach. One argument is that Parliament authorised the exception as a matter of policy, so a contract that cancels it should be subject to Sections 23, 24 and 27 of the Contract Act[46]. This is an argument, not a holding. American courts offer the other view. Sega held decompilation to be fair use, while Bowers allowed a contract to take the freedom away[47].

RECOMMENDATIONS

1. Define the term – The Bill should define reverse engineering and keep the list of acts in Section 4. A clear definition would stop arguments over whether testing or observation counts

2. Decide the contract question in the text – Parliament should say whether a contract can restrict reverse engineering. A balanced rule would allow narrow clauses between commercial parties for products and hardware. For software, it would follow Article 8 of the EU Model and protect study, testing and interoperability.

3. Fix the burden of proof – Once a defendant pleads reverse engineering, the defendant should produce the development records. The claimant should keep the overall burden of proving misappropriation. The party who holds the proof should be the one to show it.

4. Align Section 52 with Article 6(2) – The Copyright Act should limit use of information gained through decompilation to interoperability, and it should bar its use to build a substantially similar program.

5. Bring the recitals into the Bill – AN explanatory note or schedule could carry the ideas in Recitals 16 and 17, so courts see why the rule exist and where it stops.

[46] Contract Act, *supra* note 37, Sections 23, 27
[47] *Sega*, *supra* note 43; *Bowers*, *supra* note 28

CONCLUSION

This paper sought to explore how three levels of law fit with one another on reverse engineering: the trade secret rule, the contract rule and the software exception. In short, there is a loose fit, and the gaps fall on those who rely on reverse engineering.

On the first question, the EU allows a contract to close off the ability to do reverse engineering, but allows other law to limit the contract. The Bill follows the Directive's rule but omits the recitals and the words 'legally valid', so it does not say whether a contractual duty must be valid to close the lawful route. The Indian position is untested.

On the second question, Indian law has no trade – secret specific rule on Burden of proof. The general burden rule and the special-knowledge rule suggest that a defendant who pleads reverse engineering would, in practice, need to produce records to support it. The certificate requirement under BSA for electronic evidence would thus be relevant. This too is an inference, not a settled position.

On the third, the Section 52(1)(ab) of Copyright Act permits decompilation for interoperability and clause (ac) permits observing, studying and testing a program, however, Article 6(2)'s limits on later use and Article 8's rule that contrary contract terms are void

Two questions merit further thought. The first is about how Indian courts would interpret "honest commercial practices", given that the term has no settled meaning there. The second is whether machine-learning models and connected devices qualify as a 'product' under Section 4, especially where they are only accessible as a service. These can be probed through their inputs and outputs without being taken apart. That arguably counts as 'testing', but the Bill does not say so. Cross-border firms face a further risk, that they need to consider the governing law of every contract which touches on reverse engineering, as the answer may vary with both the governing law of the contract and the court that hears the dispute.

The Bill should address how it interacts with contract terms and the Copyright Act, and evidential guidance could be left to the Evidence Act or the courts.