LEGAL STATUS OF TRAINED MODEL WEIGHTS IN INDIA: COPYRIGHT, TRADE SECRET OR NEITHER?

Rishita Sangroha, LLM, University Institute of Legal Studies,
Chandigarh University, Mohali, Punjab, India.

Dr. Ranjana Sharma, Associate Professor, University Institute of Legal Studies,
Chandigarh University, Mohali, Punjab, India.

ABSTRACT

The main aim of this research is to explore the legal status and protection of trained model weights in the Indian legal system. It aims to examine the possibility of copyright protection for trained model weights under the Copyright Act, 1957, and/or protection as trade secrets based on breach of confidence and contractual obligations. It further aims to identify the existing legal gaps and propose an effective framework for their protection.

Methodology: The study is doctrinal and analytical in nature, which involves a review of relevant statutory provisions, judicial decisions, legal reports, policy documents and scholarly literature. It also conducts a comparative study of the legal strategies taken in the United Kingdom, the European Union and the United States to gain insight into the way in which the protection of trained AI model weights is dealt with in various jurisdictions.

Findings: The study concludes that the trained model weights do not comfortably fit into the existing categories of copyright protection under Indian law, mainly because of their functional nature and the uncertainty of human authorship. Moreover, India does not have a specific trade secret law, which makes it difficult to ensure effective protection of model weights, especially if they are published, extracted via APIs, or made available by unauthorized third parties. The current legal landscape offers limited safeguards and does not sufficiently cover the specific issues of trained AI models.

Research finding: The research finds that the existing Indian legal framework does not provide for complete protection of trained model weights as copyrights nor as trade secrets. It suggests a balanced legal solution, including statutory clarification of copyright protection, the adoption of specific trade secret legislation, and the recognition of model parameters as confidential information and the implementation of adequate protection for research, transparency and accountability. This would help

safeguard technological innovation and commercial interests, as well as ensure fair competition and the ongoing advancement of Artificial Intelligence.

Keywords: Artificial Intelligence, Model Weights, Copyright Protection, Trade Secrets, Intellectual Property Rights, Breach of Confidence, Indian Legal Framework, Generative AI.

I. Introduction

The cost of training a frontier language model can be many millions of dollars, and the developer ends up with a file of numbers. The numbers are known as weights or parameters and they make a model architecture and a dataset into a system that can write, translate or predict. They are duplicated, licensed, leaked, tweaked and, more and more, published to the public. A law that doesn't define what a weight file is, doesn't define who owns it, doesn't define who can copy it, and doesn't define when it's wrongful to copy it. Indian law has thus far been drafted in terms of inputs and outputs of AI systems. The policy discussion on training data is far along and the courts and the Ministry of Electronics and Telecommunications are involved[1].

The government of India, through the IT Ministry (MeitY) is taking steps to tackle deepfakes and outputs.[2] The trained model in the middle has received virtually no attention. There is no category in the Copyright Act, 1957 which names it and India does not have any trade secret law, though the Law Commission has proposed it. [3]

In this paper, three questions are asked. First, is it possible for trained weights to be a copyright work under the Act of 1957? Secondly, are they able to be protected as a trade secret or as confidential information, and against whom? Thirdly, if neither regime is a

good fit, what would provide developers with certainty without a monopoly on mathematics or a closed research? The main thesis is that weights are a poor fit for copyright, and a poor fit for confidence law, and the right answer today is "neither, fully". The paper fills that void and

[1] *ANI Media Pvt. Ltd. v. Open AI Opco LLC*, CS(COMM) 1028/2024 (Del. HC, order dated 24 July 2026) (Amit Bansal J.). See also Department for Promotion of Industry and Internal Trade, Government of India, *Working Paper on Generative AI and Copyright – Part 1: One Nation, One Licence, One Payment* (8 Dec. 2025).
[2] Ministry of Electronics and Information Technology, Government of India, [notification/advisory on synthetically generated information – insert exact title, number and date]; *see* The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.
[3] Law Commission of India, *Trade Secrets and Economic Espionage* (Report No. 289, 5 Mar. 2024).

suggests a plan to address it.

The study is of a doctrinal nature. Part II is an explanation of what weights are. Copyright and confidence law are tested in Parts III and IV. Part V examines allied regimes, Part VI examines other jurisdictions, Part VII presents the gap map and Part VIII presents the proposed framework, and Part IX addresses likely objections.

The literature on AI and IP has focused on three issues: the copyrightability of AI training data, the copyrightability of AI products, and the regulation of platforms. In most Indian writing, the status of the trained artefact has been accorded secondary importance, possibly because the matter has not yet gone to court. The comparative scholarship, particularly on memorisation, demonstrates that the question is not avoidable; whether a model has a copy or not determines the consequences of distributing it. In this paper, therefore, the focus is moved from the data that is fed into the model to the model itself, and this paper contributes to the Indian debate.

II. What Are Model Weights?

A neural network is a mathematical function that has a fixed architecture, but a very large number of adjustable numerical values. Training is an optimisation process in which the values are continually adjusted so that the outputs of the model are closer to the training data. The final model can be broken down into four components: architecture, training code, training data and weights. Each has its own set of legal arguments. It's obvious that code is a computer program. The design is mostly an advertised concept. Third party works and personal data may be included in the data. The weights are the leftover from the process and are the only component that can't be recreated without running the entire costly training session again.

The legal analysis is driven by three features of weights. First, they are created by an automated process, not by a human, but humans select the architecture, data and hyperparameters. Secondly, they are functional: a weight file is not meaningful to a reader, and its meaning is entirely in what it makes a machine do. Thirdly, weights are not completely separable from their training data. Studies indicate that models can memorise and regurgitate parts of the training material, such as personal information, when prompted appropriately.[4] It is debated

[4] Nicholas Carlini *et al.*, "Extracting Training Data from Large Language Models", *30th USENIX Security Symposium* 2633 (2021), arXiv:2012.07805.

whether this means that the model is a "copy" of the training data.

The distribution of weights is also very different. Closed weight developers have the file stored on their servers and offer access via an interface. It is published by open-weight developers, typically with a licence that limits some uses. Open weights don't necessarily have to be open source, and a legal regime is required to cover both types of open release.

III. Weights and the Copyright Act, 1957

A. The statutory categories

Original literary, dramatic, musical and artistic works, cinematograph films and sound recordings are covered by copyright[5]. The only thing that could be a literary work would be weights. The Act also expands this definition to cover "computer programmes, tables and compilations including computer databases". A computer programme is "a set of instructions in words, codes, schemes or in any other form which can be used to make a computer perform a specified task.

Weights don't fit into any of these boxes. They are not directions. The inference code is the instructions, and the weights are the numerical data that the instructions use. A competing interpretation would regard the weight file as a "table" or a "computer database[6]", because it is a huge array of numbers. That argument is superficially convincing but it is too much. Any numerical result from an automated process, for example from a sensor log or a simulation result, would be a literary work. Indian courts have never given such a broad interpretation to s. 2(o), and it is better to say that the statutory words apply to tables and compilations that reflect human selection or arrangement.[7]

B. Originality and human authorship

The Supreme Court has said that a work must be the product of "modicum of creativity" that is the result of the author's skill and judgment, and has rejected the "sweat of the brow" test and a requirement of novelty[8]. It takes a lot of money to train a model, but it is not enough to spend money and make it creative. The numerical values are not predetermined by the author, but are

[5] The Copyright Act, 1957 (Act 14 of 1957), s. 13(1).
[6] The Copyright Act, 1957 (Act 14 of 1957), s. 2(o).
[7] *Eastern Book Co. v. D.B. Modak*, (2008) 1 SCC 1 : AIR 2008 SC 809.
[8] *Eastern Book Co.*, *supra* note 7.

determined by gradient descent. Upstream, in architecture design, dataset curation and training recipes, human creativity is present, but these decisions do not affect the content of any specific weight value.

However, developers can refer to the special rule in the Act regarding computer-generated works. The author of a literary work is the "person who causes the work to be created" for a literary work that is "computer-generated[9]". On a literal interpretation, the developer who is running the training job creates the weights and would thus be the author and, under s., the creator of the weights. 17, the first owner[10]. The argument is present in the text and cannot be ignored. The weakness of it is that s. 2(d)(vi) specifies the person who created a computer-generated work, but does not state that an output that lacks any creative input is a work in the first place. The Indian authorities on originality still require a human contribution. In the United States, however, there is no such thing, and it has been assumed that human authorship is required.[11]

C. Function, merger and term

If weights were a work, the protection would be light. Copyright protects expression and not ideas, methods or functional results, and where an idea can be expressed in only a handful of ways the expression merges with the idea[12]. A competitor who trains its own model on the same data with the same architecture will obtain different numbers, so copyright would not be infringed. The statutory term is also out of sync: literary works are protected for the life of the author plus sixty years, or sixty years after publication if the author is a company or anonymous[13]. Commercial weights are not good for more than a few years. An exclusive right so long tied to a fast depreciating technical asset is not a welcome return on investment, but an invitation to strategic litigation.

D. The converse question: are weights copies of the training data?

A second copyright question points the other way. A work that a model has memorized could be an infringing copy, and the weight file could be an infringing copy, and the consequences

[9] The Copyright Act, 1957 (Act 14 of 1957), s. 2(d)(vi).
[10] The Copyright Act, 1957 (Act 14 of 1957), s. 17(a).
[11] *Thaler v. Perlmutter*, 130 F.4th 1039 (D.C. Cir. 2025), *cert. denied*, No. 25-449 (U.S. 2 Mar. 2026).
[12] *R.G. Anand v. Delux Films*, (1978) 4 SCC 118 : AIR 1978 SC 1613.
[13] The Copyright Act, 1957 (Act 14 of 1957), ss. 22, 23(1).

would be for those who store, import or distribute it. In Getty Images v. Stability AI, the High Court of England and Wales ruled that model weights can be an "article", but that the weights for Stable Diffusion were not an "infringing copy", since they did not store or contain the claimant's images[14]. That conclusion was based on the court's findings with the model before it, and is not applicable to all models, as extraction studies have demonstrated that there are models that hold recoverable fragments[15]. The question is open in India. No decision is reported on the legal nature of weights, and the Delhi High Court is hearing a suit filed by a news agency against an AI developer, which includes training and output claims[16]. The statutory licence proposed by DPIIT is only about the input and does not address the output, which is the model.[17]

IV. Weights as Trade Secrets or Confidential Information

A. The Indian position without a statute

India does not have any statute that deals with trade secrets. Article 39(2) of the TRIPS Agreement obliges members to protect undisclosed information, which is secret, has commercial value because it is secret, and has been subject to reasonable steps to keep it secret, but does not specify how this should be done[18]. India has fulfilled this obligation by the common law of confidence, which is based on English equity, and by contract. The English formulation demands information of a quality of confidence, given in circumstances that import an obligation of confidence, and its unauthorised use[19]. Indian High Courts have issued injunctions on this basis, even against former employees[20] and licensees. The Supreme Court has applied confidentiality covenants in employment[21], and has applied a test to post-employment restraints based on s. The Indian Contract Act, 1872, provides for 27 conditions.[22]

[14] *Getty Images (US) Inc. v. Stability AI Ltd.*, [2025] EWHC 2863 (Ch), para. 600 (Joanna Smith J.), *appeal pending*, CA-2026-000007 (Eng. CA).
[15] Carlini *et al.*, *supra* note 4; Milad Nasr *et al.*, "Scalable Extraction of Training Data from (Production) Language Models" (2023), arXiv:2311.17035.
[16] *ANI Media Pvt. Ltd.*, *supra* note 1.
[17] DPIIT, *supra* note 1.
[18] Agreement on Trade-Related Aspects of Intellectual Property Rights, 15 Apr. 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, art. 39(2), 1869 U.N.T.S. 299.
[19] *Coco v. A.N. Clark (Engineers) Ltd.*, [1969] R.P.C. 41 (Ch.); *Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd.*, (1948) 65 R.P.C. 203 (C.A.).
[20] *Diljeet Titus v. Alfred A. Adebare*, 2006 (32) PTC 609 (Del.).
[21] *Niranjan Shankar Golikari v. Century Spinning & Mfg. Co. Ltd.*, AIR 1967 SC 1098.
[22] The Indian Contract Act, 1872 (Act 9 of 1872), s. 27; *Superintendence Co. of India (P) Ltd. v. Krishan Murgai*, (1981) 2 SCC 246 : AIR 1980 SC 1717.

The Law Commission's 289th Report made a recommendation for a statute and attached a draft Protection of Trade Secrets Bill, 2024, which sets out a definition of a trade secret along the TRIPS lines and offers injunctions, damages and confidentiality in court proceedings[23]. The Bill has not been enacted, to the best knowledge of the authors. The current status of the Bill should be verified from official sources before relying on it.

B. Do weights qualify?

Closed-weight models are able to accommodate the three elements easily. The file is not widely known, its value is in its secrecy, and developers take reasonable measures to protect the file with access controls, encryption, and employee agreements and rate-limited interfaces. The confidence route also has a real plus: It does not need originality or human authorship. The most prominent trade secret law experts defend it on the basis of the value of the investment, and the wrongfulness of the methods used to acquire information, rather than any creative contribution[24]. This is a more appropriate theoretical basis for a machine-generated asset than copyright.

C. Where the protection runs out

The challenge is the restrictions of the doctrine. Four stand out. One, secrecy is lost once published. The information is no longer confidential as against the world once the weights are released, even in the face of a restrictive licence, and only the licence binds the licensees[25]. The duty of confidence does not attach to a downstream recipient who gets the file from a mirror. Secondly, confidence is a personal obligation and not a property right. It acts against the confidant and against one who knowingly takes from the confidant, but not against a stranger who obtains the information innocently or independently, with notice.

Thirdly, model extraction and distillation. If a competitor asks for a commercial model at scale and trains a model based on the outputs, they do not get the weights. The information retrieved is behaviour, and is available to all paying users. Whether that behaviour is confidential is questionable, and the competitor might have entered into no contract that prohibits that behaviour. Terms of service can be delivered to the contracting user, but are a poor tool against

[23] Law Commission of India, *supra* note 3, Annexure, The Protection of Trade Secrets Bill, 2024.
[24] Robert G. Bone, "A New Look at Trade Secret Law: Doctrine in Search of Justification", 86 *Cal. L. Rev.* 241 (1998); Mark A. Lemley, "The Surprising Virtues of Treating Trade Secrets as IP Rights", 61 Stan. L. Rev. 311 (2008).
[25] *Coco*, *supra* note 20.

a determined counterparty overseas. Fourthly, reverse engineering and independent development are not wrongs. This is explicitly stated in European law[26], and Indian courts have never disagreed. There are also limited remedies: no statutory damages scheme and no specific criminal offence, and owners must rely on interim injunctions which are difficult to police across borders.

D. Ownership between developer, employees and contractors

Where there is protection, who owns it? Section 17 of the Copyright Act provides that 'the employer shall be the first owner of a work made by an employee under his contract of service'[27]. However, if a contractor/consultant/research collaborator has created the work, the opposite applies. Often model creation will involve working with academic partners, and outsourcing data annotation and cloud provision. This means that it can be difficult to identify who owns the copyright. In relation to confidentiality, this will not be an issue. The relationship between the parties will depend on the circumstances of disclosure of confidential information and what was agreed within the contract. Therefore, it is important that the parties creating collaboration agreements, specifically include provisions relating to ownership of weights, fine-tuned derivatives and checkpoints, as default provisions will not provide much guidance.

V. Allied Regimes

Patents: The Patents Act, 1970 specifically excludes "a mathematical or business method or a computer programme per se[28]" from being patentable. Although it may be possible to patent a technical process using the trained model, the weights cannot.

Information Technology Law: Section 43 of the Information Technology Act, 2000 creates a civil liability for downloading/copying/extraction of data from a computer resource without the permission of the owner/person in charge. Section 66 criminalises such acts if performed dishonestly/fraudulently[29]. This means that if someone were to break into the servers, the developer would have a remedy available to them regardless of the ownership of the weights. However, this does not provide any protection against legal recipients or extraction via normal

[26] 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, art. 3(1)(b), 2016 O.J. (L 157) 1.
[27] The Copyright Act, 1957 (Act 14 of 1957), s. 17(c) (employer first owner of a work made in the course of employment under a contract of service or apprenticeship, "in the absence of any agreement to the contrary"); *cf.* s. 17(a).
[28] The Patents Act, 1970 (Act 39 of 1970), s. 3(k).
[29] The Information Technology Act, 2000 (Act 21 of 2000), ss. 43(b), 66.

queries.

Data Protection: The Digital Personal Data Protection Act, 2023 deals with processing personal data in digital format. It places obligations on data fiduciaries and provides a right to erasure[30]. If the model can be made to expose personal data, the developer may have obligations to the model. This provides a minimum standard for the developer and limits how freely they can claim the weights as a trade secret. There is a conflict between the right to erasure and how difficult it is to erase information from the trained weights. This has not been considered in the Rules[31].

Contract & Licensing: In practice, contract is the main tool used by developers to control the weights. Open weight licences often have restrictions on the scale of commercial use and prevent the outputs from being used for Models can be trained however they must agree to attribute or use properly. The enforceability of these lies in offer, acceptance and consideration. They must be properly formed using either click-wrap or download-wrap agreements. If the term prevents trade then section 27 of the Contract Act will apply. Damages are given under sections 73-74[32]. There must be evidence of loss or a reasonable estimate. Overall this provides a very flexible but uncertain alternative to a property right.

There is nothing that can be done if third parties are not party to the agreement.

VI. Comparative Perspectives

United Kingdom

In Getty, we have our first major decision regarding the status of weights. It creates uncertainty as to the nature of weights, by deciding that they are articles but not infringing copies, as they do not contain a copy of the training works[33].

European Union

The Trade Secret Directive sets out what constitutes protected information (modeled on TRIPS). It also provides that reverse engineering of a product acquired legally is a legitimate

[30] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 12(3).
[31] The Digital Personal Data Protection Rules, 2025, G.S.R. [insert no.] (E) (notified 14 Nov. 2025).
[32] The Indian Contract Act, 1872 (Act 9 of 1872), ss. 27, 73, 74.
[33] *Getty Images*, *supra* note 15, paras. 596–602.

way of acquiring trade secrets[34]. This must be addressed through remedies such as injunctive relief and damages. There is also the Artificial Intelligence Act which places obligations on general purpose model providers to be transparent. They must include a copyright policy and a summary of their training content[35]. This protects confidential information that has been obtained by authorities. This would be the most beneficial to take from India as weights are kept confidential, however there is transparency requirements around their inputs.

United States

The Defend Trade Secrets Act, 2016 creates a federal civil cause of action for misappropriation of trade secrets. A trade secret is defined as information that is protected by reasonable measures and has an independent economic value[36]. Alongside the human authorship requirement set out in Thaler[37], American developers will mainly rely upon trade secrets and contract law to protect their weights.

Overall, countries which have a statute (European Union and United States) provide certainty regarding the confidentiality route. No major country have classified weights as a copyright work. As India does not have a statute or judicial decision, it provides the least certainty.

VII. The Gap Map

A summary of how different regimes treat trained weights can be seen in Table 1. They can all be seen to protect nearby concepts (code, confidentiality between the two parties, computer security, personal information) but none protect the weight itself.

There are three scenarios to consider:

Scenario one involves an employee stealing the file containing the closed weight and placing it onto their own drive, then offering it to the competitor. This is reasonably well protected by law as they have a duty of confidence and the act is likely prohibited by contract. There is also protection via s.43 of the Information Technology Act for a civil remedy. It would be realistic to apply an interim injunction and stop the employee and any knowingly receiving party. There

[34] Directive (EU) 2016/943, *supra* note 27, arts. 2(1), 3(1)(b), 12, 14.
[35] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), arts. 53(1)(c)–(d), 78, 2024 O.J. (L) 1689.
[36] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified at 18 U.S.C. 1836, 1839(3)).
[37] *Thaler*, *supra* note 12.

is not much protection from copyright.

Scenario two involves the competitor asking the commercial model millions of times, building up their own smaller model. There is no file theft, breach of confidentiality or copying of work. If the competitor agreed to terms and conditions that prohibit this behaviour then there are remedies to protect the model. However, if the competitor cannot be sued in India then there is no real claim to make. The law does not state anything about whether it should be considered a wrong.

Scenario three involves the developer publishing weights with restrictive licensing. A third party then host the weights on a mirror site without the licensing restrictions. There is no confidentiality and there is questionable copyright on the weights. The mirror site would not be bound by the licence. The developer may have copyright on the code and licence text but the weights are circulating freely. This shows that currently the law will only really protect the model if the wrongdoer is an insider, which is the easiest scenario.

Table 1: Treatment of trained weights under Indian law

Regime	What it protects	Why it fails for weights
Copyright Act, 1957	Code, documentation, curated datasets with creative selection	Weights are not instructions; no human authorship of values; functional; term mismatch
Equity / breach of confidence	Secret weights against confidants and knowing recipients	Ends on publication; no right against innocent or independent acquirers; weak against extraction
Contract and terms of service	Obligations between parties and licensees	Privity; difficult to enforce abroad; does not bind third parties
IT Act, 2000, ss. 43, 66	Unauthorised access and copying of data from a computer	Does not reach lawful recipients or ordinary querying
Patents Act, 1970, s. 3(k)	Technical processes using a model	Computer programme per se and mathematical methods excluded
DPDP Act, 2023	Personal data processed in or memorised by a model	Protects individuals, not developers; erasure from weights unresolved

Draft Trade Secrets Bill, 2024	Would codify the secrecy route	Not enacted; silent on models, open weights and extraction

VIII. A Proposed Framework

A sustainable framework should not grant a new exclusivity in numerical files. Instead we need a method which ensures a reliance on current methods of maintaining secrecy.

There should also be clarity on what can't be copyrighted. The following are proposed:

1. Clarity on copyright: The Parliament or Copyright Office needs to state that there is no copyright protection in trained parameters but there will be protection in source code, documentation and curated datasets that meet the Eastern Book standard. This eliminates confusion around s. 2(d)(vi), the discrepancy in sixty year term and avoids property rights in mathematics.

2. Trade Secret Bill with reference to models: The Protection of Trade Secrets Bill, 2024 should be passed. A clause should be included to confirm that model parameters, training recipes and hyperparameters can be considered trade secrets. 'Reasonable steps' should be understood to mean technical solutions including access control, rate limiting and logging as well as the licence.

3. Open weights: If a developer chooses to give away weights under a licence they should still have protection on the parts they haven't made public such as training data pipelines and fine tuning recipes. The weights given away can only be protected by the licence. There shouldn't be any statutory protection that limits their usage of something allowed under the licence. This helps maintain research benefits.

4. Extraction: Any attempt to bypass access control or steal credentials to gain access to a model or train a rival model should be included in improper acquisition. Anything done in good faith, to allow interoperability or for security testing should be protected. As with computer programmes there should be exceptions in place. Using the public interface in an ordinary way shouldn't be considered a wrong if it's used in accordance with the terms. 5. Threshold for memorisation: Weights shouldn't be considered to contain a copy of the work unless it can be reasonably easily and accurately extracted. If it exceeds the threshold then those that store or

distribute them will be vulnerable to claims of infringement under s. 51[38]. Any licence under the DPIIT scheme should be understood to cover training and not distributing models that store extractable copies. If it falls below the threshold as in Getty, This will ensure that weights are not infringing copies. It maintains consistency between the legal framework and the practical application of models.

6. Accessible transparency: This should be ensured by allowing courts and regulators access to view the weights/logs of models in confidentiality clubs and in camera hearings. Large model developers should publish some level of summary of the source material they used to train from (European style). Including whistleblower protections (as recommended by the Law Commission[39]). Thereby ensuring transparency of the inputs used.

7. Consistency with data protection and enforcement: The Data Protection Board should issue guidance on erasure and extractable personal data. Disputes should be heard by commercial courts with specialist benches and technical experts. Interim injunctions should require evidence of actual steps taken towards maintaining secrecy. To prevent misuse of the secrecy route to stifle legitimate competition.

This is an unobtrusive framework. None of these points require Parliament to define AI, nor do they rely on any specific architecture. All can be implemented individually. As the DPIIT's statutory licensing and trade secret Bill are already being considered by policymakers, points 2 and 5 can be implemented as amendments/additional notes within current proposals. This also respects the constitutional requirement that any restrictions on free speech or research should be very specifically applied. If a broad IP right was granted on trained parameters it could cause a chilling effect on academic research and open source development.

IX. Objections and Limits

There are four issues with this framework. Firstly, there is a concern that increasing confidentiality for weights will mean less accountability as black-box models cannot be audited. This can be overcome as there is provision in element 6 for models to still be confidential from competitors but have a mechanism to allow court access and regulation. Furthermore, the law currently allows confidential documents to be reviewed behind closed

[38] The Copyright Act, 1957 (Act 14 of 1957), ss. 2(m), 51.
[39] Law Commission of India, *supra* note 3 (recommending whistleblower immunity rather than a mere defence).

doors. Secondly, there is a concern that the threshold for memorisation will be difficult to assess. Whilst it is true this threshold doesn't need to be perfectly assessed. It will simply provide an objective measure of reasonable effort and can be applied by courts using expert evidence.

Thirdly, there is a concern around enforcing the framework against foreign developers and copyists. Whilst a framework cannot be developed to fully overcome this issue, having clear laws in India will improve the position of Indian developers in foreign courts. Additionally, Indian courts will have a strong basis to make interim orders against those with an Indian presence. Finally, there is a concern that the framework will place too much of a burden on small developers and universities. Developers are intentionally excluded from obligations such as registering, licensing or auditing. The transparency requirement in element 6 should only be applied to those over a certain size/capacity threshold.

There are some limitations to the framework. Firstly, the framework does not determine if training on copyrighted works is legal. This is covered by the DPIIT proposal and current litigation[40]. Secondly, the framework does not cover copyright over model outputs.

This has been left until the second part of the DPIIT's work. Finally, the framework assumes models will have a technical nature. If future architectures change how training data is stored then the threshold will need to be reviewed. Therefore, it is recommended that it is reviewed periodically by a group with technical members.

X. Conclusion

In relation to the question in the title, the answer is no. The weights will not be entirely protected by copyright and trade secret as the weights do not easily lend themselves to copyright protection as they are functional, are automatically generated and questionable as to authorship. We do not want to give monopoly rights over such weights. In terms of confidence law, this is less problematic in theory. However, it requires contractual agreements, keeping the information confidential and personal obligations. This means it has issues with disclosure, innocent third parties and extracting from public facing interfaces. The draft legislation and AI copyright ideas also relate to similar issues, and the model is not defined.

[40] DPIIT, *supra* note 1; *ANI Media Pvt. Ltd.*, *supra* note 1.

This framework does not create a new property right. However, it clearly defines the boundary between copyright and provides confidentiality as a statutory right which works for models. There is a principled test regarding memorisation, and a balance between confidentiality and transparency. However, given the fast moving nature of the relevant material in India, you should check the status of the DPIIT proposals, Trade Secrets Bill and ongoing litigation in the Delhi High Court.

BIBLIOGRAPHY:

A. Statutes, Rules and Bills (India)

Copyright Act, 1957 (Act 14 of 1957).

Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

Digital Personal Data Protection Rules, 2025, G.S.R. [insert no.] (E) (notified 14 Nov. 2025).

Indian Contract Act, 1872 (Act 9 of 1872).

Information Technology Act, 2000 (Act 21 of 2000).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended).

Patents Act, 1970 (Act 39 of 1970).

Protection of Trade Secrets Bill, 2024 (draft), Annexure to Law Commission of India, *Trade Secrets and Economic Espionage* (Report No. 289, 2024).

B. International and Foreign Legislation

Agreement on Trade-Related Aspects of Intellectual Property Rights, 15 Apr. 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.

Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (U.S.).

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.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024 O.J. (L) 1689.

C. Cases (India)

ANI Media Pvt. Ltd. v. *Open AI Opco LLC*, CS(COMM) 1028/2024 (Del. HC, 24 July 2026).

Diljeet Titus v. *Alfred A. Adebare*, 2006 (32) PTC 609 (Del.).

Eastern Book Co. v. *D.B. Modak*, (2008) 1 SCC 1 : AIR 2008 SC 809.

Niranjan Shankar Golikari v. *Century Spinning & Mfg. Co. Ltd.*, AIR 1967 SC 1098. *R.G. Anand* v. *Delux Films*, (1978) 4 SCC 118 : AIR 1978 SC 1613.

Superintendence Co. of India (P) Ltd. v. *Krishan Murgai*, (1981) 2 SCC 246 : AIR 1980 SC 1717.

D. Cases (Foreign)

Coco v. *A.N. Clark (Engineers) Ltd.*, [1969] R.P.C. 41 (Ch.).

Getty Images (US) Inc. v. *Stability AI Ltd.*, [2025] EWHC 2863 (Ch) (appeal pending, CA2026-000007).

Saltman Engineering Co. Ltd. v. *Campbell Engineering Co. Ltd.*, (1948) 65 R.P.C. 203 (C.A.).

Thaler v. *Perlmutter*, 130 F.4th 1039 (D.C. Cir. 2025), *cert. denied*, No. 25-449 (U.S. 2 Mar. 2026).

E. Reports and Government Documents

Department for Promotion of Industry and Internal Trade, Government of India, *Working Paper on Generative AI and Copyright – Part 1: One Nation, One Licence, One Payment* (8 Dec. 2025).

Law Commission of India, *Trade Secrets and Economic Espionage* (Report No. 289, 5 Mar. 2024).

Ministry of Electronics and Information Technology, Government of India, [notification/advisory on synthetically generated information – insert title, number and date].

F. Articles

Bone, Robert G., "A New Look at Trade Secret Law: Doctrine in Search of Justification", 86 *Cal. L. Rev.* 241 (1998).

Carlini, Nicholas *et al.*, "Extracting Training Data from Large Language Models", *30th USENIX Security Symposium* 2633 (2021), arXiv:2012.07805.

Lemley, Mark A., "The Surprising Virtues of Treating Trade Secrets as IP Rights", 61 *Stan. L. Rev.* 311 (2008).

Nasr, Milad *et al.*, "Scalable Extraction of Training Data from (Production) Language Models" (2023), arXiv:2311.170