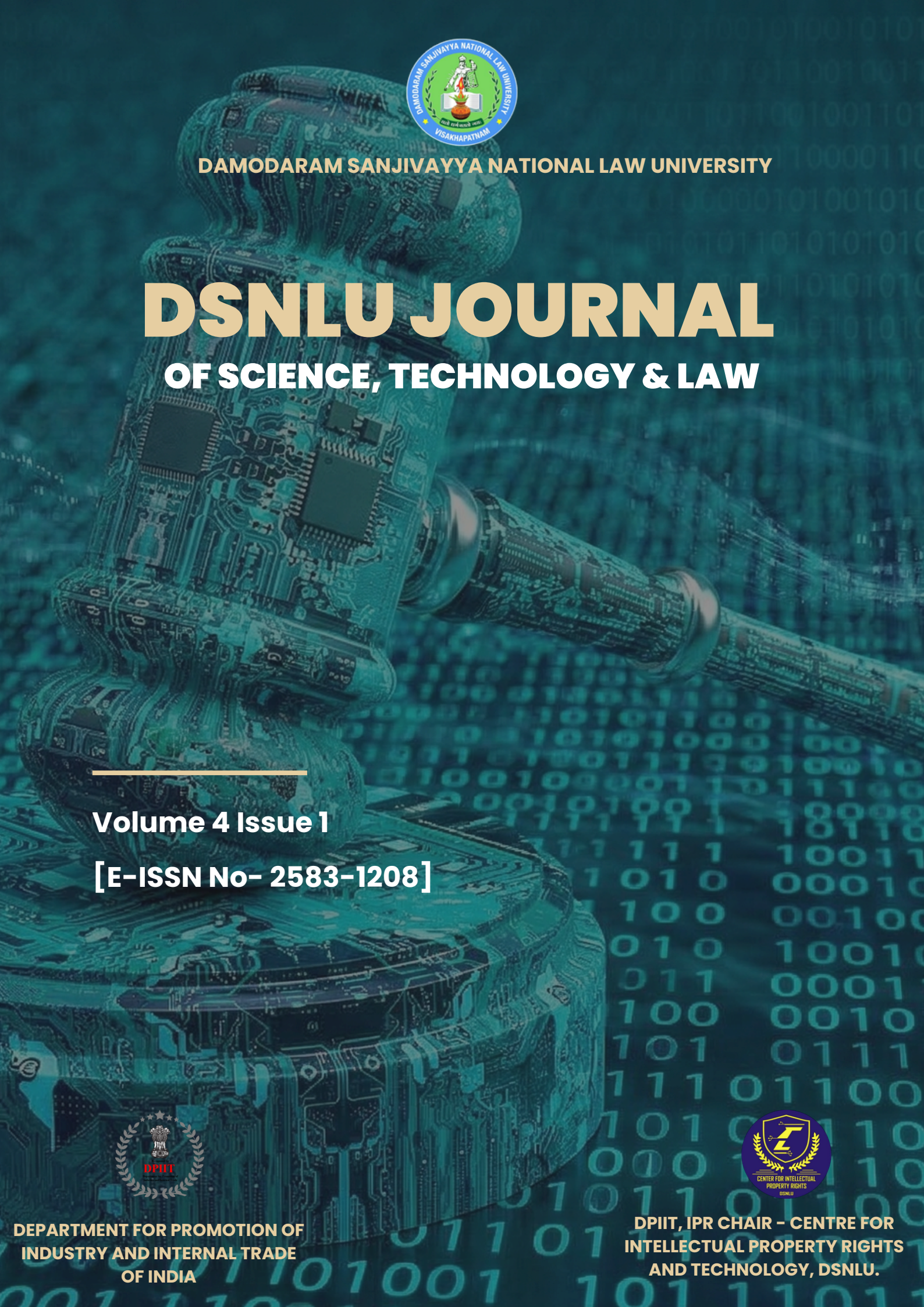


DAMODARAM SANJIVAYYA NATIONAL LAW UNIVERSITY

# DSNLU JOURNAL

## OF SCIENCE, TECHNOLOGY & LAW

Volume 4 Issue 1

[E-ISSN No- 2583-1208]

DEPARTMENT FOR PROMOTION OF INDUSTRY AND INTERNAL TRADE OF INDIA

DPIIT, IPR CHAIR - CENTRE FOR INTELLECTUAL PROPERTY RIGHTS AND TECHNOLOGY, DSNLU.

## ADVISORY BOARD

1. Prof. (Dr.) T. Ramakrishna, Professor of Law, Chair Professor (IPR), NLSIU, Bangalore, ramakrishna@nls.ac.in.
2. Prof. (Dr.) N.S. Gopalakrishnan, Professor of Law, HRD Chair on IPR School of Legal Studies, Cochin University of Science and Technology, Cochin. https://tspasia.org/council-and-advisors/prof-dr-n-s-gopalakrishnan-b-sc-ll-m-ph-d/

## CHIEF PATRON

Hon'ble Sri Justice P. Narasimha
Judge, Supreme Court of India, Visitor, DSNLU, Visakhapatnam

## PATRON

Hon'ble Sri Justice Dhiraj Singh Thakur
Chief Justice, High Court of Andhra Pradesh and Chancellor, DSNLU Visakhapatnam

## EDITOR IN-CHIEF

Prof. D. Surya Prakasa Rao
Vice Chancellor, DSNLU

## EDITOR

Dr. Dayananda Murthy C.P
Chair Professor, DPIIT-IPR Chair, DSNLU,
Faculty Convenor, Centre for IPR and Technology, DSNLU.
Email- dmurthy@dsnlu.ac.in.
https://dsnlu.ac.in/faculty/dr-dayananda-murthy/

## FACULTY EDITORIAL BOARD

1. Prof. Dr. M. Sakthivel
   https://www.tnnlu.ac.in/Faculty/Sakthivel
   Email- sakthi@tmnlu.ac.in
2. Dr. E. Prema Shayam
   https://chennai.vit.ac.in/member/dr-prema-e/
   Email- prema.e@vit.ac.in
3. Ishant JainProf.
   https://hyderabad.nmims.edu/faculty-and-research/faculty/full-time/ishant-jain/
   Email- ishant2311@gmail.com

## STUDENT EDITORIAL BOARD

Ms. Divya Sri Chandakanna, Ms. Jotsna Chalamcharla, Ms. Kurra Samskruthi Yadav, Ms. Payal Prajapat, Ms. Pallavi Awasthi, Ms. Vinamratha Marri, Mr. Komanabelli Kishore, Mr. Saurabh Sharma, Mr. Somu Harsha.

# Information and Disclaimer

Damodaram Sanjivayya National Law University shall be the sole copyright owner for all the articles, short notes, case and legislative comments published in this journal. For any purposes except for the purpose of research, teaching, private study or criticism, no part of this journal should be copied, adapted, abridged, translated, shared or stored in any physical, electronic or online format without the prior permission from the University. The University, Advisory Board or Editors are not responsible for any of the views expressed by the contributors and for errors. If any of the information published in journal is incorrect or misrepresented, the authors shall be solely responsible for the same.

**Published by the Registrar**

DAMODARAM SANJIVAYYA NATIONAL LAW UNIVERSITY

© All rights reserved.

**Citation for the Volume** – 4 (1) DSNLU J. SCI. TECH. L. (2026)

# FOREWORD

It is with great pride and intellectual anticipation that I present to the academic community the Fourth Volume, First Issue of the *DSNLU Journal of Science, Technology & Law*, published under the auspices of the Centre for Intellectual Property Rights and Technology (CIPR&T). This peer-reviewed, double-blind, open-access journal bearing ISSN 2583-1208 continues its endeavour to contribute rigorously to the ever-evolving interface of law, technology, and innovation.

In an era where the digital and the biological, the algorithmic and the artistic, intersect with increasing intensity, intellectual property rights (IPR) have emerged not merely as legal entitlements but as vital instruments of socio-economic and technological empowerment. This issue, themed *"Contemporary Issues of Intellectual Property Rights and Technology"*, explores this dynamic intersection with scholarly depth and foresight. The compilation is a timely response to a global reality where traditional legal frameworks are constantly tested by technological disruptions and where the law must remain both rooted and responsive.

This volume brings together critical discussions on sub-themes of contemporary significance including *AI-generated works and copyright, semiconductor innovation, trade secrets in the age of algorithms, patent law challenges, plant varieties, geographical indications, and the nuanced interplay between data protection and IP in the digital era*. These topics, each a subject of vigorous academic and policy discourse, find here an integrated platform of analysis, critique, and proposition. As the world embraces the Fourth Industrial Revolution, with artificial intelligence, quantum computing, and biotechnology reshaping human activity, questions around the ownership, regulation, and ethical deployment of knowledge assets become increasingly complex. For instance, as the law grapples with whether an AI can be considered an author or inventor, we are reminded of Lawrence Lessig's observation that "code is law", that technological architecture itself governs behaviour, often more effectively than legal norms. It is thus incumbent upon legal scholarship to interrogate, adapt, and preemptively design frameworks that balance innovation with accountability.

At DSNLU, we believe that academic journals such as this serve not merely as repositories of scholarship but as catalysts of discourse and bridges between the academic, professional, and policymaking communities. The articles in this volume do not claim finality, but rather stimulate debate and encourage deeper investigation. I commend the contributors for their clarity of thought, the editorial team for their diligence, and the peer reviewers for upholding the rigour that this journal demands. To the readers — scholars, practitioners, students, and policymakers — I hope this issue proves to be not only informative but inspiring. May it provoke new questions, challenge established positions, and contribute to a legal environment that is intellectually vibrant and socially relevant. In the words of Alvin Toffler, "The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn." It is through journals like this that we continually renew our commitment to that process.

Prof. D. Surya Prakasa Rao
Hon'ble Vice chancellor, DSNLU

## FOREWORD

It gives me immense pleasure to present the Fourth Volume, First Issue of the *DSNLU Journal of Science, Technology & Law*, a flagship publication of the Centre for Intellectual Property Rights and Technology (CIPR&T), Damodaram Sanjivayya National Law University (DSNLU). As the Faculty Convenor of the DPIIT-IPR Chair and CIPR&T, I am proud to witness the continued evolution of this journal as a platform for meaningful scholarship at the intersection of law, innovation, and public policy. The Centre for Intellectual Property Rights and Technology at DSNLU was established with the vision of fostering advanced research, dialogue, and capacity-building in areas that are redefining the frontiers of law in the 21st century. The Centre works closely with academic institutions, legal practitioners, policymakers, and industry stakeholders to promote a comprehensive understanding of the role of intellectual property rights (IPRs) in a rapidly transforming digital and technological landscape.

This issue's theme, *"Contemporary Issues of Intellectual Property Rights and Technology"*, captures the pulse of present-day legal challenges. The sub-themes ranging from *AI-generated works and copyright, the implications of semiconductor innovation, trademarks, plant varieties, GIs, and industrial designs, to patents, data protection in the digital era, and trade secrets vis-à-vis algorithmic intelligence*, provide an expansive view of the evolving IP ecosystem. Each contribution offers a distinct lens, highlighting both the possibilities and predicaments that define the future of intellectual property. The rise of artificial intelligence and autonomous creation compels us to revisit fundamental concepts such as authorship, inventorship, and originality. With data as the new oil and algorithms as invisible architects of decision-making, the law must now answer questions it was never originally designed to confront. This is precisely where academic research must lead the way not only by analyzing doctrinal developments, but by anticipating future disruptions and proactively proposing solutions.

The articles in this volume represent the collective efforts of scholars deeply engaged with these complexities. I am heartened to see contributions that are not only analytically sound but also oriented towards practice and policy relevance. The editorial team, with their unwavering commitment to quality and scholarly rigour, deserves commendation for upholding the high standards that CIPR&T has always aspired to. As the DPIIT-IPR Chair, I believe our responsibility extends beyond research and teaching; it includes nurturing platforms that invite critical thought, spark interdisciplinary engagement, and influence the contours of legal development. This journal is one such endeavour, a space where law meets technology, and ideas shape outcomes. I invite all readers, students, researchers, legal professionals, and policymakers, to engage with the articles in this issue with curiosity and critical thought. May the insights offered here inspire further dialogue, innovation, and reform in the ever-evolving fields of intellectual property and technology law.

Dr. Dayananda Murthy C.P,
Faculty Convenor,
DPIIT-IPR Chair, DSNLU,
CIPR&T, DSNLU

# Index

**Short Articles** **Pg No.**

1. Augmented Reality and Virtual Reality: The Legal Issues in Content Creation 01

- *Amritanshu*

2. Protecting Performer's Digital Likeness in the Deepfake Era: A Comparative Analysis of Intellectual Property, Personality Rights, and Privacy Protections in India and the UK 19

- *Aranya Nath & Anisha Sen*

3. The Future of Open Source: Is AI Too Powerful Too be Free? 34

- *Jotsna Chalamcharla*

4. Interplay Between Data Privacy Regulation and Anti- trust Practices in New Economy and an Analysis of the Digital Competition Bill 50

- *Mythri Raj*

5. Intellectual Property and Biotechnology: Navigating the Evolving Landscape of Microorganism Patenting in India 63

- *Dr. Fakkiresh S. Sakkarnaikar & Kunjal Arora*

6. Beyond NDAs: Reimagining Trade Secret Protections For Collaborative AI Research In India 73

- *Hemant Singh & Himanshu Singh*

**Long Articles**

7. Counterfeit Goods in the Digital Era: A Legal Analysis Of Trademark Enforcement and E-Commerce Platform Liability in India 89

- *Aditi Prabhu & Navya Joshi*

8. The Unsung Cognizance: Navigating the Indian Legal Landscape and Procedural Conundrum of Non – Conventional Trademarks 111

- *Amuktha Malyada Gudla & Lammata Ashish Kumar*

9. Authorship Dilemma in AI-generated Works: An Analysis of the Concerns Related to Copyrights and Creativity as posed by Generative AI 128

- *Dr. Alamdeep Kaur*

10. Intellectual Property and Labour Rights in India's Film Industry: A Legal Perspective 152

- *Aniket Jadhav*

11. The Double-Edged Sword of Patent Thickets: Challenges and Opportunities in the Tech Industry 171

- *Sangeeth Krishna*

12. Trade Secrets in the AI Era: Legal Challenges and the Need For Reform 188

-*Shardul Makhare & Tanushree Patil*

13. The Role of NFTs in Geographical Indications Protection and Branding 211

- *Rishab Tomar*

[This page was left blank intentionally]

# AUGMENTED REALITY AND VIRTUAL REALITY: THE LEGAL ISSUES IN CONTENT CREATION

*[1]


## Abstract

*AR/ VR technology known as mixed reality is an immense technology that is the essence of the modern virtual world and is used in different industries i.e. gaming, entertainment, training, and health industries. But also has legal issues that can only be resolved by restricting under certain criteria to safeguard the interest of the public at large. In this article, we have discussed the issues related to content creation in different IPR Laws i.e. copyright laws as how user-generated content can be infringement of rights, patent law in which there are issues faced between the rights of inventor and ownership, and the trademark rights that can be infringed by branding beyond boundaries. The issues faced in Data protection by infringing the piracy of individual and in what way we can work as to mitigating from the liability of infringing of Digital rights. The solutions to it are TOS/ EULA for getting the permission of individuals and the fair use doctrine. The evolution of technology is essential but has to be used under the Ambit of law.*


**KEY WORDS**- User-generated content, branding beyond boundaries, Privacy, TOS/EULA, Fair use doctrine

[1] Amritanshu, 3rd year B.A.LL.B, Babu Banarasi Das university, amritanshu541@gmail.com.

## I. Introduction

Augmented reality and Virtual Reality are immersive technologies also known as Extended reality. AR blends the virtual world with the real world and enhances the user's experience.[2] On the other hand, VR through computer technology creates a stimulated environment that visualizes the user's three-dimensional experience, using Google or a head-mounted display (HMD).[3] The AR/ VR market growth in the year 2023 is around 142.39 billion and is expected to grow at the rate of 32.9% from the year 2024 to 2030. The technology grows because of the demand for improving visual information in the gaming and entertainment industry.[4] This article aims to identify the liability of content creators and what are the safety measures to be taken to create an infringement. Technology should be used under the ambit of law to safeguard individuals' rights.

## II. Concept of augmented reality and virtual reality

### *1. Augmented Reality*

Augmented reality is the real-time integration of digital information with the user's surroundings. AR users by perceptual information experience a real-world environment, unlike VR, in which an artificial environment is created.[5] There are many uses existent with AR, from entertainment to decision-making processes. It is used for providing either some additional information to the user or visually changing the environment by enhancing its quality. The ability of AR to combine digital and three-dimensional (3D) with a person's perception of reality is its main advantage.[6] Through the devices i.e., a smartphone, glasses, or headset, they provide sound, visual elements and other sensory information to the user.[7]

Although AR emerged in the latter part of the 21st century, its origins can be traced back to pioneer Ivan Sutherland, who invented the "*Sword of Damocles*" at the University of Salt Lake City in the 1960s. The gadget was a three-dimensional display attached to the head that served as a pair of

[2]Joshua Gans and Abhishek Nagaraj, The Economics of Augmented and Virtual Reality, ARXIV (May 26, 2023) https://arxiv.org/abs/2305.16872.
[3]*Id.*
[4]Extended Reality Market Size & Trends, GRAND VIEW RESEARCH https://www.grandviewresearch.com/industry-analysis/extended-reality-xr-market-report.
[5]Augmented Reality (AR), TECHTARGATE (Feb 29, 2024) https://www.techtarget.com/whatis/definition/augmented-reality-AR.
[6]*Id.*
[7]*Id.*

glasses for 3D viewing.[8] The prototype of AR was developed in 1901 when Frank L. Baum developed a device known as a character marker.[9] The device was comprised of a sizable electronic viewfinder designed to overlay data about the subjects it was intended to focus on. The renowned filmmaker and inventor Morton Hellig invented a gadget he called Sensorama, a little more than 50 years after that one was invented.[10] This gadget used sound effects like wind, seat vibrations, and surround sound to simulate an immersive 3D virtual reality experience. With the help of Hellig's invention, users could virtually stroll through San Francisco by watching footage of the area combined with extra features to create the most lifelike experience.[11]

Multiple technological innovations can be used independently or in combination to create an augmented reality. They include; General Hardware, Display, Sensor and input devices, and Software.[12]

### *2. Virtual Reality*

The process of creating a three-dimensional (3-D) visual or other sensory environment through computer modeling and simulation is known as virtual reality (VR). Business (virtual meetings), education (medical, safety, or military training), and entertainment (video games, in particular) are among the applications of virtual reality. Within the reality-virtuality continuum, VR is a crucial technology. Because of this, it differs from other digital visualization approaches like augmented reality and augmented virtuality.[13]

In 1968, American computer scientist Sutherland and his student Bob Sproull created The Sword of Damocles, a virtual reality headgear (VRHMD). With the only ability to display basic virtual wire-frame shapes, this head mount was extremely basic and was connected to a computer instead of a camera.[14] Since the tracking system tracked head movements, these 3D models altered

[8] History of Augmented reality, SVARMONY, https://svarmony.com/blog/history-of-ar/.
[9] What Is Augmented Reality (Ar)? Origin and Evolution, GARCIA REQUEJO (Dec 15, 2022) https://garciarequejo.com/en/what-is-augmented-reality-ar-origin-and-evolution/.
[10] *Id.*
[11] *Id.*
[12] Augmented Reality – The Past, The Present and The Future, INTERACTION DESIGN FOUNDATION (Sept 23, 2020) https://www.interaction-design.org/literature/article/augmented-reality-the-past-the-present-and-the-future.
[13] Virtual reality, WIKIPEDIA https://en.wikipedia.org/wiki/Virtual_reality.
[14] History of VR – Timeline of Events and Tech Development, VIRTUAL SPEECH (Oct 17, 2024) https://virtualspeech.com/blog/history-of-vr.

perspective. Being too heavy for users to wear comfortably and hanging from the ceiling, the development never happened beyond a lab project. Instead, users had to be strapped in.[15] Although this was the first example of a VR device that looked anything like what we know and use today the idea of "virtual reality" had been proposed as early as the 1860s in literature and art.[16] The components that are responsible for the representation of the VR environment to the user and digital software that helps a user interact with the digital environment are the Lenses, screen Latency, Frame rate, and position tracking.[17]

## III. Legal issues relating to content creation

AR/VR is an immense technology that has a wider scope in today's modern era and new companies are using it for different purposes, but if it is not used under the law can cause infringement on the rights of individuals. The legal issues that can arise while using AR/VR technology are discussed in this section of the article.

### *1. Intellectual Property Issues*

The emergence of AR/VR technology has grown in several new sectors i.e., business, innovation, the court of law, and consumers. The rise of the internet necessitated cyber law in the 1990's, these new legal issues also require legal scrutiny because the law is ever-evolving with technologies.[18] The technology can lead to the infringement of IP rights, such as copyright law, patent law, and trademark law, which are stated further in this section of the article. Rapid growth in technology should have to be under the ambit of law as there should be a balance between development and the rights of individuals.

#### *a. Copyright law*

According to Section 2(d) of the Copyright Act, the person who caused the work to be created is listed as the author of that work.[19] However, in the context of AR and VR, the owner will vary

[15] *Id.*
[16] When was Virtual Reality invented?, PEBBLESTUDIOS (Aug, 2017) https://pebblestudios.co.uk/2017/08/when-was-virtual-realityinvented/#:~:text.
[17] *Id.*
[18] Intellectual Property Concerns in Augmented Reality, TTCONSULTANTS (Mar 29, 2023) https://ttconsultants.com/intellectual-property-concerns-in-augmented-realityar/.
[19] The Copyright Act, 1957, § 2(d).

from technology to technology based on their peculiar circumstantial arrangements. If there are significant similarities between the two pieces, this would occur, and a holistic comparison of the works is required.[20] The code of AR/VR can be protected as a literal work under the Indian Copyright Act, 1957,[21] but the non-literate part of the code is excluded by the protection under this code. Some non-literate parts are protected as cinematograph work which is consistent and repetitive.[22] In the case of *Eastern Book Co. (EBC) in v. DB Modak and another*, wherein the court adopted the American "*modicum of creativity*" and the court laid down the English "*Sweet Bowl*" theory.[23] When the expression and idea are merged, the work cannot be copyrightable, which is known as the *merger doctrine*. The necessity is to fix the risk of copying work, copyright law is essential to safeguard the monetary benefit of artistic production, not for mere creativity.[24] With respect to AR there are four elements that can cause copyright infringement, 1) expression is encoded, 2) the medium needs to be physical, 3) expression can be conveyed to others, and 4) can appreciable time persist unaltered. All three depend on the medium of expression that the author encodes and the first one is creativity.[25] In the case of VR *FireSabhre v. Sheehy*, the court laid down that someone who could modify original work of the author with or without consent, is not subject to transitory to be copyrighted in that situation.[26] The same is applicable to AR games also i.e., when using copyrighted images although audiovisuals will depend on the user, whether the presentation is not in a colloquial sense fixed as copyrighted instruction determines the copyrighted art and sound the player interacts with.[27] The copyright law protects the artistic work of individuals from the technology of metaverse but if they do not fulfill the criteria can breach the modicum of originality.

*i.* User-generated content liability

---

[20] Augmented Reality & Virtual Reality; Copyright, IP & More, NAIK NAIK(Oct 10, 2023). https://naiknaik.com/2023/10/10/augmented-reality-copyright-ip-more/#:~:text=

[21] Anjali Bhaskar, Beyond Physical Reality: Intellectual Property Concerns in Augmented and Virtual Reality, 3 INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION 597, (597-99) (2020), The Copyright Act, 1957, § 2(o)&13(1)(a).

[22] *Id.*, The Copyright Act, 1957 § 2(f).

[23] *Id.*

[24] Mma Afoaku, The Reality of Augmented Reality and Copyright Law, 15 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 111, (117-19) (2017).

[25] *Id.*

[26] *Id.*, FireSabre Consulting LLC v. Sheehy, (2013) 497 N.Y.S.2d 30.

[27] *Id.*

The creation of an object involves the copying of text, data, and images, this restricts the creation of new internet-based content.[28] There is a crucial gap between the copyrighted and non-copyrighted UGC because not all the content is copyrighted in the leading case of *Bleistein v. Donaldson Lithographing,* it was held that *the copyrightability of work cannot be determined solely on the originality of artistic merit*.[29] Like in the Bleistein case the low threshold copyrightability pertaining in the case of *Feist Publications, Inc v. Rural telephone service Co.* that *there must be a modicum of creativity, not just de mininis* but does not defines the same.[30] The *dark side of Moon/Wizard of Oz* the UGC have to include mash-up, and a sufficient originality degree will constitute derivative work.[31] With the metaverse technology, it is easy to copy user-generated content, which can infringe on an individual's copyright. The liability may arise when published content of the people is copied.[32] *The Digital Millennium Copyright Act* (DMCA) takes down content that is allegedly copyrighted, but the AR/VR owner can be protected from copyright infringement under the DMCA if it falls under the exception of safe harbor.[33] When the intermediary publishes user-generated content without the consent of the individual it violates copyright implications proactively.[34]

The internet intermediary can be held liable for user-generated content under copyright infringement if the content is copyrighted.[35] A safe harbor exception is provided under section 79 of IT act for internet intermediaries in third-party action.[36] In the case of *Myspace v. Super*

---

[28]Sipho Mudau, The Copyright Protection Of Online User-Generated Content, UNIVERSITY OF CAPE TOWN (Sept 15, 2014) https://open.uct.ac.za/server/api/core/bitstreams/95b32609-2151-4421-8125-88454712bbd9/content.

[29]Steven Hetcher, User-Generated Content and the Future of Copyright: Part One-Investiture of Ownership 10 VANDERBILTJ. OF ENTERTAINMENTAND TECH. LAW 863 (884-86) (2021), Bleistein v. Donaldson Lithographing (1903) 188 U.S. 239.

[30]*Id.*, Feist Publications, v. Rural Telephone Service Co, (1991) 499 U.S. 340.

[31]*Id*., derivative work, defined as a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted. A work consisting of editorial revisions, annotations, elaborations, or other modifications which, as a whole, represent an original work of authorship.

[32]Robert Bateman**,** Legal Issues with User Generated Content, TERMSFEED https://www.termsfeed.com/blog/legal-issues-user-generated-content/.

[33]*Id.*

[34]Vaidehi Sharma, IP and usage Rights for User-Generated Content (UGC), FASHION LAW JOURNAL June 20, 2024 https://fashionlawjournal.com/ip-and-usage-rights-for-user-generated-content-ugc/.

[35]Sanidhya Bajpai**,** Intermediary Liability in Copyright claim over User-Generated Content, CSIRP NLIU (March 24, 2023) https://csipr.nliu.ac.in/copyright/intermediary-liability-in-copyright-claim-over-user-generated-content/#:~:text.

[36]*Id*, The Information Technology Act, 2000, § 79.

*Cassettes,* it was provided that the Internet intermediary could be held liable if he posted copyrighted content, other than provided by safe harbor but had to comply with conditions under the guidelines of internet intermediaries and section 79 of the IT act.[37]

*b. Trademark law*

A representation of the world can be created and altered by developers and creators this is possible only by the immense technologies like AR and VR.[38] A user can frequently take on the role of a developer and produce a VR or AR representation that is made available to the general public. These depictions are frequently intended to modify or enhance actual environments, which inevitably include common objects covered by Trademarks.[39] For instance, if a brand does not have a trademark in the virtual world, a third party would try to register it in goods and services for metaverse classification, and the brand owner cannot sue for trademark infringement.[40] The law that covers trademarks in the real world has the same legal implications in content uploaded by AR/VR technologies. To establish the Trademark infringement the following points, have to be proved;[41]

- For trademark protection, the mark should be eligible.
- He owns the mark
- By using the mark by the defendant confusion arises with respect the goods and services as to the origin or sponsorship.

Section 29 of the Trademark Act refers to infringement of the trademarks that are registered and protected.[42] This section protects the interest of the proprietor or owner of the Trademark from any kind of infringement. The trademark can be challenged when there is an infringement of damaging

[37] *Id.*, Myspace Inc v. Super Cassettes Industries Ltd, (2017)236 DLT 478 (DB).
[38] Ryan N. Phelan, Barrett Spraggins, IP Aspects of Augmented Reality and Virtual Reality Technologies, AIPLA (2022) https://www.aipla.org/list/innovate-articles/2022-paper-for-aipla-augmented-reality(ar)-virtual-reality(vr)-committee.
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] The Trade Marks Act, 1999, § 29.

the goodwill, malice intention, or without the consent of the owner.[43] In AMF Inc. v Sleekcraft Boats, the use of the mark has to be consented to and to be used under the discretion of the owner.[44]

In *Rogers V. Grimaldi*,[45] It was held that to strike a balance between trademark infringement and the right to free speech in the First Amendment, the *Second Circuit developed a two-factor test*. To find trademark infringement, the use of a trademark must have either '*no artistic relevance to the underlying work*' or '*explicitly misleading*' as a source of the work. But, in India, the *freedom of speech and expression* does not prevail over the right of trademark in infringement cases.[46]

i. Branding beyond boundaries

There are many brands that started providing their goods and services in AR and VR, and brands like Nike, Gucci, and Prada registered their Trademark related to virtual goods.[47] Over the next three years, the social commerce industry is expected to increase from $492 billion in 2021 to $1.2 trillion in 2025 internationally.[48] To enrich customer engagement and streamline the shopping experience various brands are integrated with AR and VR powered software. Although this enhances the consumer experience, it may also increase the likelihood of subsequent trademark disputes and burden on the justice system.[49] In particular, as brands integrate more deeply with AR and VR platforms, the complexity is in distinguishing between virtual and physical trademark use, which raises concerns about the extent of protection in augmented space.[50]

A game called City of Heroes was developed by NC Soft, in which user could create their own character, select avatars, and alter the outfits of those characters. That being said, there was a strong resemblance between character and their outfits, those of Marvel comics characters. Marvel consequently filed a lawsuit against NC Soft, alleging that NC Soft had committed trademark

[43] Abhinay Bhattacharya, Trademark infringement issues in virtual reality, IPLEADERS (Oct 21, 2020) https://blog.ipleaders.in/trademark-infringement-issues-in-virtual-reality/.
[44] AMF, Inc. v. Sleekcraft Boats, (9th Cir.1979) 599 F.2d 341.
[45] *Id.*, (2d Cir. 1989) 875 F.2d 994.
[46] Sumedha Tewari, Trademark infringement in the Metaverse: An Indian Perspective, NUJS IPTLS (Apr 4, 2022) https://nujsiplaw.wordpress.com/2022/04/04/trademark-infringement-in-the-metaverse-an-indian-perspective/.
[47] Maddi Gambone and J.D. Candidate, Branding Beyond Boundaries: The Future of Trademarks and Advertising in Augmented Reality 9 THE UNIVERSITY OF CINCINNATI INTELLECTUAL PROPERTY AND COMPUTER LAW JOURNAL 150 (153-57) (2024).
[48] *Id.*
[49] *Id.*
[50] *Id.*

infringement and duplicated it without consent. It was held that Marvel's claim was rejected by the court, which also made it very evident that NC Soft had not violated any law because the mark had not been used in any trade and commerce pertaining to goods and services.[51] Thus, it is difficult to prove trademark infringement as in the virtual world, there is no selling of goods and services of trademark products through virtual platforms.[52]

*c. Patent law*

In recent years, AR/VR technology has proliferated, and with that rapid advancement comes the need to safeguard the creative ideas that are propelling it forward. Patents related to AR and VR are essential for protecting these concepts.[53] Patent applications for AR/VR innovations cover a broad spectrum of topics, such as advancements in software and hardware as well as novel and enhanced user interface techniques.[54] For instance, Meta has filed over 250 patents for their headset and avatars.[55] A person may claim a patent for the inventions that are claimed to be true and the first inventor of the invention of that person.[56] The number of patent filings in AR/VR has exponentially grown over the last decade in India and so in other jurisdictions i.e. China, the US, Europe, etc.[57] The inventor finds it difficult to keep pace with innovation and the latest trends, and to access the potential impact of these developments on their patent, as the technology continues to advance and new applications emerge.[58] The inventor must be engaged with their peer and industry experts to review and update their patent so that it will be competitive and remain relevant.[59]

[51] *Supra* Note 42, Marvel V NC Soft CV 04-9253RGKPLAX, 2005.
[52] *Id.*
[53] Shivang Khandelwal, Muskaan Mandhyan, and Aryan Jain, Seeing Is Believing: The Future Of IP In AR/VR, MONDAQ (Mar 31, 2023) https://www.mondaq.com/india/patent/1299888/seeing-is-believing-the-future-of-ip-in-arvr.
[54] *Id.*
[55] *Id.*
[56] The Patent Act, 1970, § 6(1)(a).
[57] Amit kumar and Pallavi Sinha, Augmented and Virtual Reality Innovations and Patent Trends, Sagaciours Elevate, https://sagaciousresearch.com/blog/augmented-virtual-reality-innovations-and-patent-trends/.
[58] J.D. Houvener, Patenting in Virtual (VR) and Augmented (AR) Reality, Bold Patents (Feb 22, 2023) https://boldip.com/blog/patenting-in-virtual-vr-and-augmented-ar-reality/.
[59] *Id.*

The Alice test's first step is described by the apex court that we have to determine whether the patent-ineligible concept is in direct relation to the issue claimed while determining the Supreme Court is "tread carefully".[60] Naturally, it is a challenging esoteric question to determine whether a claim is merely using or applying an ineligible concept or is truly "directed to" that concept; however, this question forms the basis of the first step of this test.[61] The Federal Circuit also reminds us that step one of Alice must be regarded as a "meaningful" step in reaching this conclusion and that under this step, significant class claims will not be deemed directed for the patent-ineligible concept. *Enfish LLC v Microsoft Corp* stated differently, that the initial step of the Alice test does not establish an exceptionally difficult standard to meet.[62] *Amdocs (Lebanon) Ltd. v. Broadcast Telecom, Inc*.[63] According to Judge Reyna's dissent.

*i.* Inventor vs. Ownership issues

Patent considerations pertaining to inventorship and ownership in collaborative research between companies can be highly complex and unique, and they can have a significant impact on a patent's value.[64] By engaging in suitable research and licensing arrangements prior to the creation of an invention that results from teamwork, one can increase the likelihood of securing robust patents. A disastrous outcome may result from improper consideration of inventorship and improper agreement-making.[65] In *Falana v. Kent State University*[66], it was held that initially who developed a method would not be the inventor of the later developed invention. The inventors are regarded as the patent owners unless there is an agreement stating otherwise. Co-inventors also function as co-owners in the event that there are any.[67] There should be a balance between the rights of the inventor and the owner of AR/VR technology to safeguard patent rights and the smooth functioning of technology.

---

[60] Applying Step One of the Alice / Mayo Test, (Bitlaw) https://www.bitlaw.com/guidance/patent/applying-step-one-of-Alice-Mayo-test.html.
[61] *Id.*
[62] *Id.*, Enfish LLC v Microsoft Corp (2016) 822 F.3d 1327.
[63] *Id.*, (2016) 841 F.3d 1288.
[64] MaryAnne Armstrong 1, Gerald M Murphy Jr, Inventorship and Ownership Considerations and Pitfalls with Collaborative Research, PMC NCBI NLM NIH (Apr 26, 2012) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4025834/.
[65] *Id.*
[66] *Id.*, (Fed. Cir. 2012) 101 USPQ2d 1414.
[67] *Id.*

The general rule, the inventor is the owner unless the contrary appears;

- When an invention is conceived, ownership passes to the assignee. In this scenario, ownership was previously assigned by the inventor to a third party under the terms of an assignment agreement. In the work-for-hire relationship and employee-employer relationship, this is standard practice.
- When ownership of an invention is assigned by the inventor after it is conceived, ownership is transferred to the assignee on the date of the assignment. This is typical when a financial amount is taken into account when making an assignment.
- According to law, ownership of the invention shall have to be vested in a third party (not the inventor); in this instance, the assignment occurs at the time, the invention was conceived. This is frequently the case in work-for-hire relationships (to a lesser extent) and employee-employer relationships (where employers own inventions rather than employees' inventions) in many different countries.

In accordance with US law, under certain legal restrictions, one co-owner or inventor may sell the patented invention without the other co-inventor's consent or by paying them royalties.[68] This makes it crucial for a business or academic institution to confirm that the rightful owner of an invention is in place.[69] In India, unless there is a valid agreement to the contrary, each registered person has the right to exercise the rights granted by section 48 for their own benefit without having to give consideration to the other person or persons. This applies to situations where two or more people are listed as grantees or proprietors of the patent.[70]

The patent technology licensing has a numerous rights but less than as compared to the ownership, i.e. the right is restricted to the field of use, time, and geographical areas, a patent owner will be in a contractual agreement that, the patent licensee will not be sued for the infringement if, causes to use, offer to sell, sell or import of inventions.[71] Until and unless acts within the licensee's obligation or under the boundaries of the licensee agreement. The patent owner may grant the exclusive license in which no person (patent owner or any person to whom the license is granted)

[68] *Id.*, 35 USC §262.
[69] *Id.*
[70] The Patent Act, 1970, § 50(2).
[71] Ownership/Assignability of Patents and Applications, UPSTO https://www.uspto.gov/web/offices/pac/mpep/s301.html .

shall compete with the exclusive licensee.[72] It protects the patent technology from being infringed or disclosure that can cause damage to the patent owner.

*d. Data protection act*

The VR headset, AR smart glass camera, and other devices related to the immense technology collect a wide range of personal data such as eye, head, and facial movement as well as voice recording, this information can identify their feelings and even deduce what they think.[73] This raises an important question regarding user consent and privacy in the collection of personal information.[74] This could be subject to vulnerability since hackers could take advantage to steal personal information or intimate cyberattacks against other network-connected devices.[75] Article 32(a) of GDPR provides that there should be *pseudonymisation and encryption of personal data* and the other clauses talk about how we can secure the data of individuals.[76] These security concerns should be mitigated to ensure the integrity and safety of AR and VR technology. The international privacy laws i.e., GDPR and the *Children Online Privacy Protection Act (COPPA)*.[77] Generally, the age is restricted to under 13 years, by refraining from using any kind of metaverse object, the local authorities and institutions should comply with whether the user would agree with the terms and conditions in the privacy policy.[78] For disclosing the personal information of the child, and including the consent of any material changes in collection, the parental consent is required.[79]

Personalized advertisement and the privacy of users become imperative in navigating the ethical landscape, there should be a balance between the two.[80] Section 43-A of the IT Act is read with "*(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) rule, 2011 (SPDI Rules)"* states that if there is negligence at the time of holding sensitive

[72] *Id.*

[73] Sonika Sharma, VR and AR: Data Privacy Risks for 2024, INFOSECTRAIN (Mar 13, 2024) https://www.infosectrain.com/blog/vr-and-ar-data-privacy-risks/.

[74] *Id.*

[75] *Id.*

[76] The General Data Protection Regulation, Art. 32(a).

[77] VR Permission and Waiver Forms, EDACUTORS IN VR (Sept 25, 2019) https://educatorsinvr.com/2019/09/25/vr-permission-and-waiver-forms/.

[78] *Id.*

[79] The Children Online Privacy Protection Act, 1998, § 312.5.

[80] *Id.*

information or the personal data while maintaining reasonable security practices and procedures that can cause losses, then compensation has to be paid for such negligence.[81] Data privacy concerns are stated in a recent example, in the game Pokemon Go when launched in 2016, requested full access to the permission erroneously for Google account of the user to create an account in the game, the data collection and privacy policy provision are subject to scrutiny.[82] The use of Avatars in the digital representation of users within a virtual environment increases the privacy and identification risk through personal trades i.e., race, gender, aesthetics, and age.[83]

i. Disclosure of personal information to the third party

A privacy concern that is primary from object data related to individuals is autonomy and anonymity. A significant amount of data can reveal about the users' lives with sensitivity varying from level to level.[84] Article 9 of the GDPR, prohibits to process the sensitive data and personal information for any use without consent.[85] The data observed that user can provide i.e., biological or health information to shopping history or web browser, can easily infer or directly reveal data that may be expected to be kept private, such as the live location, demographic location, and what they do in their free time. For some users, it can lead to harmful discrimination.[86] Section 164 HIPAA provides the rule of privacy as the *standard for the privacy of individually identifiable health information*, to ensure that patients' data is secured which may involve liaising with several departments.[87] There should be clear guidelines for AR/VR on how they process data and store applications, as well as by whom and when they can be accessed to mitigate the risk of privacy.[88] The platform of multiuser AR/VR raises the question of to what extent third-party doctrine and other investigators extend to the legal framework and record users' activity fully or partially in

[81] Ashita Sahay and Kiran Patel, Virtual Reality: Exploring Boundaries and Limitless Possibilities, Bar and Bench (Aug 11, 2023) https://www.barandbench.com/law-firms/view-point/viewpoint-virtual-reality-exploring-boundaries-limitless-possibilities, The Information and Technology Act, 2000, § 43-A.

[82] AR & VR: Privacy And Autonomy Considerations In Emerging, Immersive Digital Worlds, IAPP https://iapp.org/media/pdf/resource_center/fpf_report_augmented_virtual_reality_recommendations.pdf.

[83] Vítor Bernardo, Extended reality, (EDPS) https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/extended-reality_en.

[84] Ellysse dick, Balancing User Privacy and Innovation in Augmented and Virtual Reality, ITIF (Mar, 2021) https://www2.itif.org/2021-ar-vr-user-privacy.pdf.

[85] The General Data Protection Regulation, Art 9.

[86] *Id.*

[87] The Health Insurance Portability and Accountability Act, 1996, § 164.30.

[88] *Id.*

virtual space. New regulations should be introduced by the policymaker for comprehensive user data in AR and VR and to access the information warrant should be required.[89]

When the personal data possessed is business-related then it is critical, with perspective to the company. This is important when data is possessed from the AR/VR software or when provider runs the server, rather than from the end device itself.[90] Article 44 of GDPR, which permits the transfer of personal data to a third country or international organization, is applicable when the server holding the data is located outside of a third country and that country does not have an adequate level of data protection in accordance with the decision of the EU commission.[91] In Germany, the companies in pursuance with the work council introduced AR/VR technology for monitoring the behavior of employees *under section 87(1)(6) of the Works Constitution Act (BetrGV).*[92] The involvement of work council enables to processing of data by company agreement to establish a legal basis, unlike it would not be solely permissible through *Section 26(1)(1) of the Federal Data Protection Act (FDPA) or Article 6(1)(1)f of GDPR*.[93]

## IV. Solution to the legal issues.

The owner of AR/VR technology faces legal challenges as aforeseen in the above section but there are some ways that can be granted to the owner protection from infringement and will not violate a right of individuals. The owner has to work in accordance with the legal framework, and under the ambit of law for the creation of any new feature in technology by not infringing the rights of the person.

### *1. Terms of service or end-user licensing agreement*

When any user begins to use the virtual software or the platform then the rules and rights of *terms of service or end user licensing agreement ("TOS/EULA")* have to be agreed by the person (user).[94] If any right is created in the world by any activity, is to be assigned to the platform in

[89] *Id.*
[90] Albrecht Von Wilucki, Working in the metaverse: What legal issues do virtual and augmented reality create?, BUSE (Mar 28, 2023) https://buse.de/en/blog-en/labor-law/working-metaverse-legal-issues-virtual-augmented-reality-create/.
[91] *Id.*, The General Data Protection Regulation, ART 44.
[92] *Id.*
[93] *Id.*
[94] *Supra* Note at 23, (119-20).

accordance with the terms of using the platform.[95] Thus the platform owns the right to create anything within it and through the TOS/EULA holds a right to own licenses for specific rights. The owner of the platform controls rights that the user can exploit.[96] Second Life, a VR game which is created by Linden Labs applied a different approach, the user gets all the rights of their creation.[97] In respective second life contains TOS then also requires a license for the creation of all types of Linder labs in creation, although it possesses all rights for the work.[98] The TOS or EULA is essential for the protection of work from any sought of infringement, other than it protects the rights of individuals. There are multiple benefits to using EULA for both users and software providers.[99] It offers legal protection to the provider by outlining the terms and conditions for using it, which reduces the liability risk in case of software manufacturing and misuse and safeguards intellectual property rights.[100] Further, it helps the user to understand the scope of the software and its limitations with the help of including details about usage restrictions, data privacy, and updates.[101] The protection under EULA totally depends on the draftsman to ensure that all terms and conditions essential for the user to read, are visible and nothing that can infringe the right of an individual, if not mentioned in the agreement, for safeguarding the liability of the software provider.

2. ***The defense of the fair use doctrine***

The Trademark Act, 1999, Section 30, offers a defense against a claim of trademark infringement; however, in order to qualify, the use of the trademark must be legitimate (section 30(1)(a)), not based on whether it is detrimental to the older trademark for destructiveness.[102] There are two types of defenses as fair use i.e. nominative fair use and descriptive fair use.[103] When an individual is accused of using a product in an unauthorized manner to determine its quality, purpose, or origin while providing services or goods, they are protected by descriptive fair use under section

[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] Tithi Agarwal, What is an End-User License Agreement (EULA)?, TRACKOBIT (Aug 29, 2024) https://trackobit.com/blog/what-is-an-end-user-license-agreement-eula.
[100] *Id.*
[101] *Id.*
[102] *Supra* Note at 45.
[103] *Id.*

30(2)(a).[104] Conversely, Nominative Fair Use is defined as the use of marks when they are "*reasonably necessary*" to illustrate how compatible the goods are with the trademark goods or, in accordance with section 30(2)(d), to ridicule, denounce, or comment on them.[105]In case, *New Kids on the Block v. News Am Publ'g Inc.,*[106] the three-prong test was given by the court, 1) it should not be identifiable without trademark use, 2) it should be necessary for the identification, 3) there would not be any anything done by the user that indication of endorsement or sponsorship, with respect to trade by trade holder. In *Tata Sons v. Greenpeace International*, the defendant used the Tata trademark in their video game Paceman. The court applied a test very similar to the Rogers test, laying down that communicative or commercial intent needs to be considered before deciding on an infringement and also dwelt on the relation between free speech and trademark law. Since the game was to criticize Tata, there was no infringement.[107]

Section 52 of the Copyright Act, provides the defense against copyright infringement.[108] In the case of *Civic Chandran v. Ammini Amma*, the fair use concept was explained that "*it may be reasonable that only the extract or quotation from the work alone will be permitted as fair use and not the re-production of the whole or substantial portion".*[109]There are some essentials to determine whether the re-productive work is infringement or not 1) The relation between criticism and quantum of work taken. 2) The intention behind taking it. 3) and the completion of likelihood between the two works. The court would consider these points if fall under the following category.[110]

## V. Conclusion & suggestions

The AR/ VR technology also known as mixed reality is an immense technology that is essential for enhancing the gaming industry and entertainment. It has to be used under the ambit of law to

[104]*Id*, The Trade Marks Act, 1999, § 30(2)(a).
[105]*Id*, The Trade Marks Act, 1999, § 30(2)(b).
[106] Bhavya Solanki and Medha Bhatt, Virtual Reality, Augmented Reality and Trademark Law: How Freely Can Imagination Run?, SPICYIP (July 20, 2022).
[107]*Supra* Note at 45, Tata Sons Limited vs Greenpeace International & Anr,(2011) DLT 705.
[108] The Copyright Act 1957, § 52.
[109] Mihir Wagh, Fair Dealings And Fair Use: Critically Analysing The Copyright Exemption Doctrines In Place In India And The United States, MANUPATRA(Aug 29, 2022)https://articles.manupatra.com/article-details/FAIR-DEALINGS-AND-FAIR-USE-CRITICALLY-ANALYSING-THE-COPYRIGHT-EXEMPTION-DOCTRINES-IN-PLACE-I.
[110]*Id.*

ensure that no person shall be deprived of their right, the infringement can be caused in the form of copyright, patent, trademark, and data protection act infringement. The user shall have the consent of the person or company whose character has been used in the AR/VR technology. It enhances the surroundings in the virtual world or depicts the person to be in the virtual world but violates the privacy of the public at large when they use human behavior by way of collecting personal information which can cause massive destruction to the individual and also violates the fundamental right i.e. right to the privacy of the individual. The user has to agree with the *Terms of Service (TOS) and comply with the end user licensing agreement (EULA)* which can mitigate the owner of technology from the infringement. When the person uses any patented, trademarked, or copyrighted item without the permission of the owner then the rights of the person can be infringed. Instead, if with the consent of the owner, the work is taken or inconsistent with *fair use doctrine* then the owner of technology can be mitigated with the IP infringements. The personal data and original work of individuals have to protect the rights of individuals ensuring the balance between development in technology and the personal interest of the public at large.

[This page was left blank intentionally]

# PROTECTING PERFORMERS' DIGITAL LIKENESS IN THE DEEPFAKE ERA: A COMPARATIVE ANALYSIS OF INTELLECTUAL PROPERTY, PERSONALITY RIGHTS, AND PRIVACY PROTECTIONS IN INDIA AND THE UK

*[1]

**Abstract**

*This paper examines the effectiveness of existing intellectual property (IP) laws, personality rights, and privacy protections in protecting performers' digital likenesses against deepfake technology in India and the UK. Deepfake technology poses significant challenges for IP and privacy protections, particularly in the entertainment industry. The study uses a comparative legal analysis approach to review statutory laws, judicial precedents, and regulatory guidelines in the UK & India. Findings indicate that while both countries provide IP protection and personality rights, significant gaps exist in addressing unauthorised digital likeness manipulation through deepfakes. The study suggests that amending IP and privacy laws to include digital likeness protections specific to deepfakes would be beneficial. The study indicates neither jurisdiction guarantees enough protection for performers' digital likenesses in the deepfake age.*

**Keywords:** Deepfake technology, Performer's Digital Likeness, Intellectual Property Rights, Personality Rights, Privacy

[1]Aranya Nath, Ph.D Scholar, Damodaram Sanjivayya National Law University, subhamitanath002@gmail.com & Anisha Sen 4th year , anishasen005@gmail.com B.A.LL.B KIIT School of Law

## I. Introduction

In the age of Artificial Intelligence, Deepfake Technology creates a challenging issue for today's generation in various sectors. The authors of this study article present essential information to readers on the legality of deepfake technology in India and the UK. Deepfake technology enables the synthetic manipulation and generation of hyper-realistic videos and images. By using deep learning algorithms, deepfakes can convincingly replace one person's likeness with another's, making it difficult to distinguish real content from fabricated media. Although deepfakes can have numerous applications in film production or creative arts, they pose considerable issues in media and entertainment, especially regarding performers' rights. Therefore, to understand the legality that hampers the artist creation in the media and entertainment sector, researchers would like to redress: To what extent are India's and the United Kingdom's present intellectual property rules at safeguarding performers against deepfake misuse? Are personality rights sufficiently recognised and enforced in both jurisdictions to prevent the illicit use of digital resemblance? How important do privacy regulations play in safeguarding performers' digital identities, and how do they fall short in the case of deepfakes?

Furthermore, what are the significant legal gaps in each country's approach, and what changes could be required to bolster safeguards for performers' digital likenesses in the age of deepfake technology? The research is to seriously assess the efficacy of existing intellectual property, character, and confidentiality protections for performers' digital resemblance in India with the United Kingdom. By examining the legal frameworks in both nations, this study aims to uncover legislative strengths, limits, and possible vulnerabilities that expose performers to exploitation via deepfake technology. This comparative approach will shed light on how each country's legal system addresses the protection of digital likenesses if current laws adequately protect performers, and where legislative reform may be necessary. Key concerns to be addressed include the limitations of IP protections for deepfake content, the broad spectrum of personality rights in managing likeness, and the role of privacy laws in protecting personal identification in digital media.

Lastly, the researcher identifies and evaluates the protections available to performers under intellectual property, personality rights, and privacy frameworks by reviewing legal precedents and extant laws in India and the United Kingdom. This research will focus on every jurisdiction's

approach to digital likeness safety, particularly how well the laws handle the issues brought by deepfake technology. Finally, this comparative approach will assist in assessing best practices and alternative frameworks that might strengthen safeguards for performers in both nations, providing insights that may be useful in other jurisdictions experiencing comparable difficulties.

## II. Deepfake Technology and Its Implications for Performers

Deepfakes are synthetic media produced with artificial intelligence and deep learning techniques, notably Generative Adversarial Networks (GANs). These neural networks create material while another assesses its realism, producing incredible media that can seamlessly replace one person's appearance with another in a photograph or video. The technique entails training models on large datasets of the target person's face, voice, or emotions, which enables the technology to replicate exact movements, gestures, and speech patterns.

Deepfakes present hazards to the media, entertainment, and advertising industries. They can save production expenses by allowing filmmakers to digitally resurrect or change an actor's look to play multiple roles. Advertisers may develop engaging advertisements by combining real and artificial components to enhance the narrative. However, the misuse of deepfakes has significant concerns, such as promoting false narratives, undermining prominent individuals' reputations, or producing deceptive advertising.

For performers, the unlawful recreation of their digital likeness using deepfakes poses a considerable concern. Deepfakes enable the accurate replication of a performer's visage, voice, and movements, allowing the creation of content that seems genuine but is not. Such illegal reproductions can result in deception since performers may be depicted promoting items, making remarks, or acting in scenarios they would never agree to. Beyond commercial application, deepfakes have been used in more invasive ways, such as making non-consensual erotic content containing performers' likenesses, which can harm their reputations and personal lives. As deepfake technology advances, the risk of abuse advances, underscoring the urgent need for legal frameworks that ensure performers retain agency over their digital likenesses and are safeguarded from the different types of digital deception enabled by deepfake technology.

## III. Intellectual Property Rights in Deepfakes

Deepfakes, which are classified into four usage categories, may help tiny start-up businesses with sales and marketing, comedy or parody, revenge porn, and political campaigns. A neighbourhood boutique selling customised dresses may profit from a deepfake application that enables buyers to try on the outfits, making purchasing decisions easier. Deepfakes may also be humorous or satirical, as evidenced in the viral "TikTok films of Tom Cruise licking a lollipop only to discover chewing gum in the centre." Thousands of forged votes emerged in Ohio in 2016,[2] fuelling fears among voters that elections had been manipulated. The image and identity of the individual who discovered the phony votes were proven to be a deepfake.

Revenge pornography consists of sexual representation photographs and films made public by an angry former partner, which can have major long-term negative consequences in one's personal and professional life. Women are exposed to deep-fake videos.[3] The report of the United Nations Sustainable Development Goals has estimated that more than 85% of women are subjected to such kinds of deepfake videos owing to gender biases.[4]

In the future, ethical issues about deepfakes used for revenge pornography and politics necessitate a reconsideration of whether deepfakes deserve stronger intellectual property protection. Deepfakes used to produce meaningful material, marketing, and customization of social media posts in local dialects, for example, are inventive and imaginative, necessitating an increased balanced discussion of the subject.

The justification for Deepfakes raises questions about the control of free speech, since an outright ban can indicate controlling the freedom of speech, a practice contradictory to democracy, free expression, and trust. It poses three concerns:

a) Are Deep Fakes legally covered by the copyright regime?
b) How may exceptions and constraints help to balance the deepfake debate?

[2]Why the Manoj Tiwari deepfakes should have India deeply worried, https://theprint.in/tech/why-the-manoj-tiwari-deepfakes-should-have-india-deeply-worried/372389/ (last visited Oct 21, 2022).
[3]Revenge pornography - Women, ISEA, https://www.infosecawareness.in/concept/women/revenge-pornography (last visited Nov 11, 2024).
[4]Edvinas Meskys et al., *Regulating Deep Fakes: Legal and Ethical Considerations*, (2019), https://papers.ssrn.com/abstract=3497144 (last visited Feb 8, 2024).

c) Concerning the wake of deepfakes between freedom of speech and IP protection, as specified in the Constitution of India be balanced?

The interconnections of copyright, personality rights, and privacy rights have grown complicated in the digital age. Copyright law focuses on safeguarding creative works, but does not fully handle the illicit use of a person's likeness, which is more directly tied to personality rights. Privacy rights safeguard against the illicit collection and broadcasting of personal information, but they do not directly address the commercial use of one's appearance. Deepfake technology crosses these lines by producing synthetic media that can violate copyright (if the content contains copyrighted information), personality rights (via illicit use of resemblance), and privacy rights (by entering private life).

### *1. Protection of Certain Aspects of Personality Rights under IP Laws and Other Laws*

Personality rights, sometimes known as the right of publicity, are the rights that individuals have to control the commercial use of their name, image, likeness, or other aspects of their identity. These rights are especially significant for celebrities and public figures, whose identities are highly valued financially. The scope of personality rights varies by jurisdiction, but they often include the right to forbid the fraudulent exploitation of one's identity for financial gain. In some legal countries, personality rights are regarded as a subset of privacy rights; in others, they are viewed as distinct legal guarantees. The emergence of deepfake technology poses a substantial danger to personality rights since it allows for the production and spread of realistic but illicit representations of persons, possibly leading to manipulation and usage without their permission.

"Article 21 of the Indian Constitution comes closest to maintaining personal rights in India. Subsequently, the legislation excludes the economic part of personality rights. Indian courts used to rely on provisions under copyright and trademark law to preserve certain aspects of personality rights." Passing off has been used to safeguard personal rights in various circumstances. While IP Laws may appear acceptable, numerous features and complexities remain neglected, rendering them ineffective.[5] The courts have overlooked these realities and granted remedies, leaving just a

[5]Agitha T.G & N.S. Gopalakrishnan, *The Imperial Copyright Act 1911 and the Indian Copyright Law* 116 (2013).

few personality traits protected under the current intellectual property regime. In certain scenarios, courts have read personality rights as a well-known trademark protection.[6]

In "*D.M. Entertainment v. Baby Gift House*,[7] the case concerned the financial consequences of personality rights, & the court granted relief by citing trademark law challenges, including passing off and fraudulent endorsement. This case underlines the necessity for a full understanding of the rights and complexities that underpin personality rights in India."

### *2. Existing Legal Instruments for the Protection of IP Rights*

The court granted an injunction against infringement of a registered mark in a well-known personality under trademark and passing off. This was because the plaintiff's caricature was obscured by the preview of the products provided, resulting in an infringement of the registered mark. Exploiting a well-known personality's distinctive identifying attribute is also an act of unfair competition that warrants a passing-off claim. Illicit exploitation of their uniqueness also creates a deception that the plaintiff has licensed or has a relationship with the defendant's goods or services, similar to fraudulent endorsement.[8]

In exceptional circumstances, the court may use copyright to protect personality rights, even if the Act does not explicitly specify the same. Certain provisions of the Copyright Act might be beneficial remedies against personal rights violations. "Section 2(qq) of Copyright Act 1957,[9] for example, performer if personality falls within the scope of its performer definition, Section 38 of the Copyright Act 1957 where performer rights are indicated, forbids the unauthorised marketing of one's performance. Section 57 of the Copyright Act 1957 also provides ethical safeguards in some situations and forbids the unauthorised marketing of one's performance. Section 57 provides ethical safeguards in specified cases.[10]"

[6]Recent Jurisprudence on Personality Rights in India - S. K. SRIVASTAV & CO, LAW FIRM, (Jul. 4, 2024), https://srivastavandco.com/recent-jurisprudence-on-personality-rights-in-india/ (last visited Nov 11, 2024).
[7]Daler.pdf, https://spicyip.com/docs/Daler.pdf (last visited Nov 24, 2023).
[8]Aranya Nath & Sreelakshmi B., *Deepfakes on Copyright Law- Inadequacy of Present Laws in Determining the Real Issues* (2024), http://ir.nbu.ac.in/handle/123456789/5250 (last visited Jun 26, 2024).
[9]CopyrightRules1957.pdf, https://www.copyright.gov.in/Documents/CopyrightRules1957.pdf (last visited Jun 29, 2023).
[10]Section 57 in The Copyright Act, 1957, https://indiankanoon.org/doc/1710491/ (last visited Jun 14, 2024).

In "*Titan Indus. Ltd. v. Ramkumar Jewellers*,[11] the court attempted to address the plaintiff's entitlement to be the first creator of the work while considering the plaintiff's personality as a performer. Along with copyright, the court established elements constituting liability for infringement of the publicity right, with the first being validity, which requires the plaintiff to have an enforceable right in their persona or identity, and the second being identifiability, which requires the celebrity to be recognisable from the defendant's illegal usage. Infringement of the publicity right does not need proof of confusion or untruth if the personality is identified.

Finally, only celebrities have the right to be awarded personality protection based on the traits mentioned above.

### *3. Provisions under the Information Technology Act*

The Information Technology Act of 2000 cyber law in India to regulate cyberspace, has provisions dealing with cybercrimes. However, due to the non-comprehensive nature of coverage of cybercrimes under the IT Act of 2000, the Act alone cannot regulate deepfakes. Some provisions of the IT Act that relate to dealing with deepfakes are explained below. *"Under the IT Act, cybercrime is committed if deepfakes are inappropriate or abused. Section 67 of the Act provides for penalties for the electronic publication or transmission of obscene material, and if the deepfake created is inappropriate, it would attract this provision." "Section 67A of the Act outlines the penalties for publishing or transmitting material in electronic form that contains a sexually explicit act or conduct, and thus a deepfake that contains a sexually explicit act will attract penalties."*[12] Section 67B of the IT Act criminalises the publication or transmission of material in electronic form that depicts children engaging in sexually explicit acts or conduct, and will apply to deepfakes involving children. The deepfake maker shall be punishable for the offence, under the provided "Section 66C of the IT Act, 2000, if the deepfake content uses any unique identification feature, such as electronic passwords, of a person in a fraudulent manner. It includes a foreign country's identity. In addition, section 66D of the Act penalises computer usage to commit fraud through

[11] Titan Industries Ltd. vs. M/S Ram Kumar Jewellers, CS(OS) No.2662/2011.

[12] Cyber Lawyer, *Section 67 of Information Technology Act: Punishment for Publishing or Transmitting Obscene Material in Electronic Form*, INFO. TECHNOLOGY LAW (Sep. 18, 2014), https://www.itlaw.in/section-67-punishment-for-publishing-or-transmitting-obscene-material-in-electronic-form/ (last visited Nov 10, 2022).

impersonation[13]." *Under "Section 69A, the Central Government has the authority to direct the intermediary to block any such deepfake content if it determines that doing so is necessary for preserving the independence and territorial integrity of India, maintaining India's national security, and fostering cordial relations with other nations*[14]*."* Apart from the computer-related offence, the IT Act punishes for privacy infringement.

"Section 66E of the Act outlines the penalties for violating a person's right to privacy as follows: if the accused person intentionally or knowingly photographs, publishes, or transmits an image of a private area of another person without that person's consent, the accused person is subject to a sentence of imprisonment of up to three years or a fine of up to two lakh rupees, or both, depending on the severity of the offence. Another provision in the IT Act that deals exclusively with cyber defamation is Section 66A sending any information via a computer resource that is excessively offensive or has a menacing nature or is to create annoyance, discomfort, danger, obstruction, insult, injury, criminal intimidation, hostility, hatred, or ill will is punishable by this section." However, the Apex Court in "*Shreya Singhal v. Union of India*" [15] nullified this section of the IT Act, making it obsolete. Thus, this provision holds no value in addressing deepfakes.

The previous provisions were mainly to deal with deepfake makers. The IT Act also provides for the liabilities of intermediaries. Since intermediaries host deepfake content, Section 79 of the Act regulates their liability[16]. After a discovery or court order, the intermediary may remove the content. In *"Myspace Inc. v Super Cassettes Industries Ltd*[17]*, the Court ruled that intermediaries must remove copyright-infringing information upon private party complaints without a Court order. Currently, intermediaries are only required to advise users about not posting certain kinds of harmful/unlawful content. Recent IT Rules 2021 establish a legal requirement for intermediaries*

[13]Section 66D of Information Technology Act: Punishment for cheating by personation by using computer resource, Facebook, Fake Profile, https://www.itlaw.in/section-66d-punishment-for-cheating-by-personation-by-using-computer-resource/ (last visited Nov 10, 2022).

[14]Section 69A in The Information Technology Act, 2000, https://indiankanoon.org/doc/10190353/ (last visited Nov 10, 2022).

[15]Shreya Singhal vs U.O.I on 24 March, 2015, https://indiankanoon.org/doc/110813550/ (last visited Nov 4, 2022).

[16]Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, SSRN JOURNAL (2011), http://www.ssrn.com/abstract=2038214 (last visited Jul 28, 2024).

[17]My Space Inc. vs Super Cassettes Industries Ltd. on 23 December, 2016, https://indiankanoon.org/doc/12972852/ (last visited Nov 4, 2022).

*to conduct fair attempts to prevent users from posting such content. The new clause will ensure that the intermediary's obligation is not a formality."*

### *4. Provisions under GDPR Provisions*

In UK, unlike in other countries, personality rights are not formally recognised as an independent constitutional concept. Instead, safeguards against the abuse of an individual's image, particularly in the context of deepfake technology, are handled by a combination of privacy laws, data protection rules, and tort law. The General Data Protection Regulation (GDPR), adopted into UK legislation by the Data Protection Act of 2018, is critical in this context. The GDPR, [18]offers strong protections for personal data, which includes any information relating to an identified individual, giving people a legal basis to dispute the illicit development and dissemination of deepfakes. The GDPR requires that personal data be processed lawfully, fairly, and transparently, and individuals have the right to access, correct, and remove their data. This paradigm has played an important role in judicial rulings addressing privacy concerns using digital technology. [19]

## IV. Personality Rights and Privacy Protections for Performers

Personality rights contrast greatly between India and the United Kingdom, with India having no particular statute controlling these rights, but courts recognising them under a patchwork of intellectual property and privacy laws. Enforcement of these rights is uneven due to the absence of a specialised legal framework, frequently based on larger concepts of privacy and reputation. In contrast, the UK does not explicitly recognise personality rights as a separate legal concept, instead dealing with illegal likeness usage through the common law tort of passing off. This strategy protects performers by banning illicit use of their image or appearance, but it is only applicable in cases where there is a danger of deception or reputational injury. Privacy laws in India and the United Kingdom provide specific protection for performers' digital identities, although within the wider context of data protection and the right to privacy. In "*Justice K.S. Puttaswamy v. Union of India*[20]", India's Supreme Court proclaimed the right to privacy a fundamental right, setting an

[18]GDPR_FINAL_EPSU.pdf, https://www.epsu.org/sites/default/files/article/files/GDPR_FINAL_EPSU.pdf (last visited Dec 16, 2023).
[19]Thomas Linden et al., *The Privacy Policy Landscape After the GDPR*, 2020 PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES 47 (2020).
[20]MANU_SC_1044_2017, http://www.manupatracademy.com/legalpost/manu-sc-1044-2017 (last visited Mar 23, 2025).

important precedent for individual privacy rights. However, India lacks adequate data protection legislation geared toward digital identity, making it difficult to handle the subtle challenges raised by deepfake technology.

The General Data Protection Regulation (GDPR)[21] framework includes significant privacy safeguards, including rights to sensitive information, which might be considered to include features of digital likeness in some environments. However, the extent to which GDPR adequately protects performers against deepfake misuse is debatable, given that it was not specifically designed to handle the complexities of digital identity manipulation in media and entertainment. Both nations have difficulties keeping up with deepfake improvements, as present legal safeguards were not created with digital manipulation in mind.

## V. Legal and ethical challenges in addressing deepfake technology

Ethical Issues: Questioning or raising the issue of deepfake technology raises serious questions of ethics, at least about consent, personal autonomy, and widespread public deception. For performers, creating and distributing deepfakes without permission violates their sense of authority as their reputation is used for reasons they never approved. This manipulation undermines the use and control that someone can have over their identity and probably leads to reputational harm, emotional distress, and possible financial loss. Besides, deepfakes distort public perception. They create a completely hazardous landscape of misinformation where individuals and performers are laid out in false or misleading situations. This fictional duplication conflicts with the borderline between reality and fiction in this age of digital consumption of content; concerns are raised about responsible utilisation of technologies and mechanisms of consent to protect people from exploitation.[22]

Regulatory and Legislative Gaps: The lacunas of the present law and regulatory regimes in India and the UK expose performers to deepfake misuse. India provides some protection for performers under copyright and privacy laws, but there are no particular regulations addressing the issue of digital likeness exploitation or deepfake creation. As such, the measure of protection remains

[21]Data Protection Principles: Core Principles of the GDPR, https://cloudian.com/guides/data-protection/data-protection-principles-7-core-principles-of-the-gdpr/ (last visited Nov 11, 2023).
[22]Nithesh Naik et al., *Legal and Ethical Considerations in Artificial Intelligence in Healthcare: Who Takes Responsibility?* 9 FRONT SURG 862322 (2022).

inconsistent. The other difference is that Indian courts have recognised personality rights with statutory support hence offering a piecemeal approach dependent on judicial interpretation. In the UK, although data protection laws under GDPR in the UK provide certain protections against privacy violations, they fail to tackle the manipulation of digital identities or personal rights. Moreover, the challenge both countries face is regulating technology as neither has developed an overarching approach to regulating deepfake technology.[23]

This leads to the so-called regulatory lag with no clear legal remedy for performers, and such policies must focus on the deepest ethical and practical concerns relating to the deepfakes.

Case Laws and Precedents: Many landmark cases in the jurisdictions of India and the UK indicate a challenge that legal responses to deepfakes and likeness rights pose. For example, in contrast, "*Titan Industries Ltd. v. Ramkumar Jewellers*[24]", in which unauthorised use of a celebrity's image or name highlighted how the judiciary wanted personality rights but only provided celebrities with limited protection. Few direct cases are filtering through to court about deepfakes, so much of the law remains open. Cases in the UK about the right to privacy, such as *Douglas v Hello!* built an important foundation for future cases regarding digital likeness, but remain largely underdeveloped within the law landscape around deepfakes. Neither of the jurisdictions has had a high-profile case with the subtleties of deepfakes technology, leaving significant ambiguity to the enforceability and adequacy of current legal protections for performers' digital identities.[25]

## VI. Comparative analysis and key findings

### *1. India Vs. UK: A Comparative Analysis:*

Each is only partially a solution, but each is otherwise uniquely distinctive in handling intellectual property, personality rights, and privacy generally applicable to deepfakes. India remains more judicially invested in personality rights; its privacy standards are less developed than the UK's GDPR protections. In contrast, there are no statutory personality rights in the UK; it gives broad privacy protection under the GDPR, which could indirectly protect against the misuse of deepfakes

[23]Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means**, 28 INFORMATION & COMMUNICATIONS TECHNOLOGY LAW 65 (2019).

[24]Titan Industries Ltd. vs M/S Ramkumar Jewellers on 26 April, 2012.

[25]Nicole Moreham, *Douglas and Others v Hello! Ltd. The Protection of Privacy in English Private Law*, 64 THE MODERN LAW REVIEW 767 (2001).

through a structured consent and data management framework. Neither of these countries has developed a strong legal framework targeting digital likeness or deepfake technology. There are elements in each country that might be extended to help fill that gap.

Each jurisdiction's strengths and disadvantages are listed below: India's court recognition of personality rights remains a foundation upon which numerous performing artists can seek justice for the illicit utilisation of their likenesses. However, India's lack of appropriate regulations and inadequate data privacy protections do not fully enable it to combat the potential of deepfake abuse. On the other hand, the UK's GDPR framework provides extremely robust privacy protection, especially data consent, potentially offering protection against illegal digital likeness creation.

Nevertheless, the UK's lack of personality rights and reliance on the tort of passing off restricts its ability to protect performers comprehensively. Both jurisdictions demonstrate the need for targeted deepfake legislation to close existing gaps and strengthen protections.[26]

Lessons and Best Practices: Both countries may take lessons from each other with best practices. India should adopt comprehensive data protection laws like GDPR to strengthen digital identity protections and insist upon further clarity while obtaining consent. Recognition of personality rights in the statute may provide even stronger protections for performers than are obtained now. On the contrary, the UK may formalise personality rights to more directly address the challenge of illicit exploitation of likeness. Specific anti-deepfake regulations in both countries would ensure the rights for recourse against illegal use of performers' digital likenesses, and create more robust legal frameworks that can address the deepfake technology-related challenge, be it ethical or legal.[27]

## VII. Recommendations and proposed framework for digital likeness protection

It proposes a comprehensive framework for digital likeness protection in India and the UK, addressing the challenges posed by deepfake technology. In India, a robust framework should be

[26]Augustian - PROTECTION OF PERSONALITY RIGHTS IN INDIA ISSUES .pdf, https://www.nlunagpur.ac.in/PDF/Publications/5-Current-Issue/4.%20PROTECTION%20OF%20PERSONALITY%20RIGHTS%20IN%20INDIA.pdf (last visited Jun 14, 2024).

[27]Latham & Watkins LLP, *India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison*, GLOBAL PRIVACY & SECURITY COMPLIANCE LAW BLOG (2023), https://www.globalprivacyblog.com/2023/12/indias-digital-personal-data-protection-act-2023-vs-the-gdpr-a-comparison/ (last visited Nov 11, 2024).

developed to recognise and protect digital likenesses under personality rights, extending these protections to the digital realm. This could involve creating a distinct legal category for digital likeness rights, preventing illicit use or replication of a person's image, voice, and mannerisms, particularly in the deepfakes.

In the UK, while privacy laws offer a degree of protection, personality rights should be statutorily recognised to provide a clearer basis for performers to safeguard their likenesses. Specific provisions addressing the illicit creation of digital likenesses through technologies like deepfakes would create a more comprehensive legal landscape, ensuring effective protection against identity exploitation. In the deepfake era, a model framework for performance protection must include individual statutory personality rights, consent management systems, privacy safeguards, civil and criminal liability, and cross-border enforcement. Technology, such as artificial intelligence systems which identify deepfake content, can play an important role in safeguarding performers in the digital age. Collaboration among technology firms, industry groups, and legal experts might result in formulating guidelines for the ethical use of digital likenesses, ensuring that performers have a clear, enforceable way to claim their rights. Industry-specific standards of behaviour, supported by legislative frameworks and technical solutions, might encourage responsible content development while discouraging the exploitation of digital likenesses. [28]

## VIII. Conclusion

The research looks at the legal and ethical issues of securing performers' digital likenesses in the age of deepfake technology. It highlights substantial gaps in current legal systems in India and the United Kingdom since neither nation has a comprehensive legal structure designed to defend against the exploitation of digital likenesses. The study underlines the necessity for specific legislative reforms and international coordination to protect performers' rights in the digital age. Current studies should focus on developing globally for digital likeness protection, investigating the link between intellectual property and privacy, and investigating the role of emerging technologies like artificial intelligence and blockchain in preserving and protecting digital likenesses. It is essential to explore the larger societal consequences of deepfakes, such as the influence on public trust and media integrity, and how legal systems might evolve to prevent these

[28] Augustian - PROTECTION OF PERSONALITY RIGHTS IN INDIA ISSUES .pdf, *supra* note 136.

threats. Further study into the role of internet platforms in promoting the spread of deepfakes will be critical in determining how these firms might help safeguard performers. As deepfake technology advances, a dynamic and adaptive legal framework becomes increasingly important.

[This page was left blank intentionally]

# THE FUTURE OF OPEN SOURCE: IS AI TOO POWERFUL TO BE FREE?

*[1]

**Abstract**

*The future of open-source AI is at a turning point. While OpenAI has driven innovation, collaboration, and accessibility, concerns over security, misinformation, and ethical risks have sparked increasing restrictions. As AI systems grow more powerful, the debate intensifies: Should AI remain freely accessible, or does its potential for harm require stricter control?*

*This paper explores the shift from open-source to proprietary AI, analyzing why leading companies are limiting access to their AI models. OpenAI, once committed to transparency, now restricts its most advanced models, while Meta's Llama models, though open, come with usage restrictions. The discussion also examines the legal and ethical dimensions of AI governance, particularly the EU AI Act, which introduces a risk-based framework to regulate AI systems. While high-risk AI models face strict compliance measures, low-risk open-source AI continues to thrive with fewer restrictions.*

*The debate is no longer just about technology but about power, ethics, and control. Open AI fosters transparency and progress, but without safeguards, it can be misused for cyberattacks, deepfakes, and bias. Proprietary AI, on the other hand, limits innovation and centralizes control among tech giants. The future likely lies in regulated openness—a model where AI remains accessible yet governed by ethical, legal, and security safeguards. Striking this balance is crucial to ensuring that AI continues to be a tool for progress rather than a source of harm. The choices made today will define the role of AI in shaping our world.*

**Key Words:** Open Source, Proprietary AI, EU AI Act.

[1] Jotsna Chalamcharla, 4th year B.A.LL.B, Damodaram Sanjivayya National Law University, jssjotsnachalamcharla@dsnlu.ac.in

## I. Introduction

Open-source technology has long been a driving force behind innovation, powering everything from small applications to large-scale enterprise systems. It has fostered collaboration, transparency, and rapid technological advancement, with major contributions to fields like software development, cybersecurity, and cloud computing. In 2025, open-source is poised to revolutionize technology like never before, reshaping industries and accelerating progress.[2]

Artificial intelligence (AI), particularly generative AI (GenAI) and large language models (LLMs), has emerged as a transformative force across industries. Companies worldwide are leveraging AI-powered automation to boost efficiency and reduce costs. In August, Amazon announced that it saved 4,500 years of programming time through automatic code generation, showcasing Open-Source AI's potential to revolutionize workflows and development processes.[3]

As open-source AI continues to gain momentum, concerns regarding its security, ethical implications, and potential misuse are also growing. The unrestricted accessibility of advanced AI models raises fears about their potential exploitation for malicious purposes, including misinformation, cyber threats, and automated disinformation campaigns. Furthermore, as companies increasingly integrate AI into critical operations, ensuring compliance with legal and ethical standards becomes a major challenge. This leads to a pressing question: Can AI remain open while ensuring safety, ethical use, and preventing misuse? Or has AI become too powerful to be freely available? As the debate over open-source AI intensifies, the challenge lies in finding a balance—one that preserves the benefits of open collaboration while mitigating the risks associated with unrestricted access to powerful AI models.

[2]Rick Dagley. **"**Open Source Trends and Predictions 2025 From Industry Insiders**."***ITPro Today*, Jan 14 2025. https://www.itprotoday.com/software-development/open-source-trends-and-predictions-2025-from-industry-insiders (Last visited on January 16 2025).

[3]Amazon Web Services, **"**Amazon Q Developer Just Reached a $260 Million Dollar Milestone**."***AWS Blog*, Aug. 2024, https://aws.amazon.com/blogs/devops/amazon-q-developer-just-reached-a-260-million-dollar-milestone (Last visited on January 16 2025).

## II. The OPEN-SOURCE Philosophy and Its Role in AI

### 1. *Understanding Open Source*

Originally a software development methodology, open source has evolved into a broader philosophy emphasizing openness, decentralization, and collaboration.[4] It extends far beyond software, shaping progress in fields like science, education, healthcare, government, and industry. The open-source movement is built on foundational principles that make it highly effective and influential[5], including: Encouraging collective contributions from diverse stakeholders, Promoting accountability among contributors, Ensuring free access to knowledge and technology, Rewarding valuable contributions regardless of hierarchy, Strengthening technological progress through global cooperation, Enabling contributors to guide projects and benefit mutually. The impact of open source is evident in transformative innovations like Linux, Kubernetes, cloud computing, and the internet itself, which were all built on these principles.

### 2. *The Significance of Open Source in AI*

Does the open-source approach remain relevant in today's AI-driven world? Absolutely. The philosophy of open collaboration is crucial in shaping artificial intelligence (AI), fostering advancements while ensuring accessibility and transparency.

#### *a. What Defines an Open-Source AI Model?*

According to the Open Source Initiative, an AI system is truly open source only when users enjoy four core freedoms: they can use it for any purpose, study how it works, modify it for their own needs, and share both the original and modified versions without undue restriction. These freedoms require that developers release not just the source code but also the model parameters and meaningful information about the training data, because without these elements users cannot genuinely understand, audit, or adapt the system. In contrast to proprietary systems such as

[4] OA Resources, "The History and Evolution of Open Source Software**."***OA Resources*, available at https://www.oaresources.org/history-evolution-open-source-software (Last visited on December 26 2024).
[5] Gordon Haff, How Open Source Ate Software, (2nd Edition, 2021), https://link.springer.com/book/10.1007/978-1-4842-6800-1 (Last visited on December 26 2024).

ChatGPT, open-source AI has enabled researchers, universities, and companies to experiment, reproduce results, and build new applications on top of shared models and tools, which strengthens innovation, transparency, and collective oversight in the AI ecosystem.

The rapid rise of open-source AI is evident through several key statistics that highlight its widespread adoption and impact. Hugging Face, one of the leading platforms for AI research and collaboration, now hosts over 50,000 freely accessible AI models, enabling developers to leverage pre-trained systems for various applications.[6] Similarly, Google's TensorFlow, an industry-standard machine learning library, has been downloaded over a million times, demonstrating its extensive use in research and industry alike.[7]

The open-source AI community on GitHub has also expanded significantly, with over 100,000 repositories dedicated to AI projects[8], fostering a culture of innovation and knowledge sharing. Additionally, the pace of AI development has accelerated, with more than 100 new AI models being added daily across various open-source platforms. The release of Meta's Llama 2[9] further exemplifies the transformative power of open-source AI, sparking breakthroughs in medical research, environmental monitoring[10], and AI-driven accessibility solutions worldwide.

*b. The Evolution of Open-Source AI Through Key Milestones*

The journey of open-source AI has been marked by key technological breakthroughs that have reshaped the landscape of artificial intelligence. In 2015, Google took a monumental step by releasing TensorFlow, making deep learning frameworks accessible to developers globally.[11]

---

[6] Hugging Face, **"**Hugging Face Hub Documentation,"*Hugging Face*, https://huggingface.co/docs/hub/en/index (Last visited on December 27 2024).

[7] PyPI Stats, **"**TensorFlow Download Statistics**,"***PyPI Stats*, https://pypistats.org/packages/tensorflow (Last visited on December 26 2024).

[8] Nilay Patel, **"**GitHub CEO on AI, Copilot, and the Future of Open Source**,"***The Verge*, August 19 2024, https://www.theverge.com/24221978/github-thomas-dohmke-ai-copilot-microsoft-openai-open-source (Last visited on December 28 2024).

[9] Meta AI, **"**BiMediX: Built with Llama**,"***Meta AI Blog*, https://ai.meta.com/blog/bimedix-built-with-llama (Last visited on December 27 2024).

[10] Llama**, "**Llama Impact Grants**,"***Llama.com*, available at https://www.llama.com/llama-impact-grants (Last visited on December 28 2024).

[11] Google**, "**TensorFlow: Google's Latest Machine Learning System,**"***Google Open Source Blog*, Nov. 9, 2015, https://opensource.googleblog.com/2015/11/tensorflow-googles-latest-machine.html (Last visited on December 28 2024).

OpenAI followed in 2016 by launching its first set of open-source AI tools, further expanding opportunities for research and innovation.[12]

In 2017, the introduction of PyTorch revolutionized deep learning, making AI development more flexible and intuitive.[13] Hugging Face, in 2019, changed the field of natural language processing (NLP) with its open-source transformers, which are now integral to AI-powered text generation and translation.[14] The launch of Stable Diffusion in 2022 disrupted the AI-generated image market, allowing artists and developers to create high-quality visuals without relying on proprietary systems.[15] Most recently, Meta's Llama 2, released in 2023, set a new benchmark for open-source large language models (LLMs), enabling widespread innovation across industries.[16]

### 3. *Applications of Open Source AI in the Real World*

The influence of open-source AI extends far beyond research and development—it is actively transforming industries and solving real-world problems. In healthcare, AI-powered medical imaging tools are enabling earlier disease detection, improving diagnosis accuracy, and enhancing patient care.[17] Agriculture is also benefiting from open-source AI, with farmers using machine learning models to monitor crop health, optimize resource use, and increase yield efficiency.[18]

In climate science, AI models are helping scientists track deforestation, analyze climate change trends, and develop sustainability solutions.[19] Education has been greatly impacted as well, with universities worldwide integrating open-source AI tools into their curriculums, providing students

[12] Brockman, Greg, et al., **"**OpenAI Gym**,"***arXiv Preprint*, arXiv:1606.01540, 2016, https://arxiv.org/abs/1606.01540 (Last visited on December 29 2024).
[13] PyTorch, "2024 Year in Review,"*PyTorch Blog*, available at https://pytorch.org/blog/2024-year-in-review (Last visited on December 29 2024).
[14] Hugging Face, "Transformers Documentation,"*HuggingFace*, https://huggingface.co/docs/transformers/main/en/index. Last visited on December 28 2024.
[15] Stability AI, **"**Stable Diffusion Public Release**,"***Stability AI*, Aug. 22, 2022, https://stability.ai/news/stable-diffusion-public-release (Last visited on December 28 2024).
[16] Meta, **"**Llama 2: Open Foundation and Fine-Tuned Chat Models**,"***Meta Newsroom*, July 18, 2023, available at https://about.fb.com/news/2023/07/llama-2 (Last visited on December 28 2024).
[17] Meta, *Supra* note 7.
[18] Llama, *Supra* note 8.
[19] *Id.*

with hands-on experience in machine learning and data science.[20] Furthermore, open-source AI has significantly contributed to accessibility, with developers creating AI-powered tools to assist people with disabilities, improving communication and daily life for many individuals.

### 4. *The Benefits of Open Source AI*

The open-source model accelerates development cycles, with bug fixes and feature improvements being implemented significantly faster than in proprietary systems. Open-source AI provides significant cost advantages, both in direct savings and indirect financial benefits. On average, enterprises save over $230,000 annually on licensing fees by leveraging open-source models instead of proprietary solutions.[21] By reducing dependency on vendor-specific technologies, businesses gain greater flexibility while lowering training costs through freely available community resources. Additionally, open-source AI allows for scalable deployments without the high costs associated with premium pricing tiers. Beyond direct savings, organizations experience a 60% reduction in development time by utilizing pre-trained models, significantly accelerating AI implementation.[22] Maintenance costs also see a 40% decrease, thanks to the continuous improvements and support provided by the open-source community.[23] Furthermore, by avoiding vendor lock-in, companies eliminate long-term contractual expenses, enabling greater financial and operational flexibility in AI adoption. This democratization of AI fuels cross-industry innovation, enabling breakthroughs in fields like healthcare, finance, and autonomous systems through knowledge-sharing and collaborative problem-solving.[24] Ultimately, the global participation and continuous community-driven improvements make open-source AI a key driver of technological advancement, ensuring that AI development remains inclusive, sustainable, and widely accessible.

---

[20] EvoLLLution, **"**AI Integration in Higher Ed Curriculums: How Kogod Did It in Six Months**,"** *Changing Higher Ed*, https://changinghighered.com/ai-integration-in-higher-ed-curriculums-how-kogod-did-it-in-six-months (Last visited on December 29 2024).

[21] Manuel Hoffmann, Frank Nagle & Yanuo Zhou, **"**The Value of Open Source Software**,"** Harv. Bus. Sch. Working Paper No. 24-038, 2024, https://www.hbs.edu/ris/Publication%20Files/24-038_51f8444f-502c-4139-8bf2-56eb4b65c58a.pdf. (Last visited on January 16 2025).

[22] *Id.*

[23] Linux Foundation, **"**The Value of Open Source Software Is More Than Cost Savings**,"***Linux Foundation Blog*, https://www.linuxfoundation.org/blog/the-value-of-open-source-software-is-more-than-cost-savings (Last visited on January 17 2025).

[24] *Supra* note 8.

### 5. *Future Prospects of Open Source AI*

As open-source AI continues to evolve, several emerging trends are set to reshape the future of AI development. Domain-Specific AI Models are expected to become more prevalent, with tailored models designed for healthcare, finance, and scientific research. These specialized models will enhance accuracy and efficiency in solving industry-specific challenges.

Multimodal AI is another major trend, integrating text, images, and video to enable AI systems to understand and generate more complex outputs. Federated Learning, which allows AI models to be trained across multiple devices without sharing sensitive data, is gaining traction as a privacy-preserving technique. Ethical AI Development will remain a priority, with ongoing efforts to ensure AI systems are transparent, fair, and aligned with societal values. Finally, decentralized AI is emerging as a countermeasure to the increasing dominance of big tech in AI development.

## III. The risks of open-source ai: too powerful to be free

Despite its benefits, the open-source AI movement faces several critical challenges that could hinder its long-term sustainability and responsible deployment. Addressing these issues is essential for ensuring that AI remains a force for good rather than a tool for exploitation.

The rapid pace of AI innovation makes it difficult to ensure consistent quality and security across open-source models. Unlike proprietary AI, which undergoes rigorous internal testing and validation, open-source AI models often rely on community-driven reviews, which can be inconsistent. Maintaining trust and reliability in these technologies requires the development of standardized benchmarking frameworks, comprehensive testing protocols, and detailed documentation. Encouraging community-led audits and reviews is essential to detect vulnerabilities early and enhance overall security.

### 1. *Security Threats, Privacy Risks and Potential for Malicious Use*

While open-source AI has democratized access to cutting-edge technology, it also presents serious security risks. Without proper safeguards, generative AI can become a powerful tool for cybercrime. The open and collaborative nature of open-source AI increases the risk of security breaches and data privacy violations. Since anyone can modify and redistribute AI models, there

is little control over how they are used or misused. Unauthorized access to sensitive training data can lead to potential privacy breaches, while the exploitation of AI models for cyberattacks, such as AI-powered phishing scams, remains a significant concern.

Open-source AI models can be weaponized to create sophisticated phishing scams, deepfakes, and financial fraud schemes. Some malicious browser extensions use AI to alter copied cryptocurrency wallet addresses, redirecting funds without the user's knowledge. Deepfake technology is being exploited for identity theft and social engineering attacks, making it harder to distinguish real content from fake.[25] AI-driven tools like FraudGPT and WormGPT, which are based on the open-source GPT-J model by EleutherAI, are now widely available on dark web markets, enabling cybercriminals to craft sophisticated phishing scams and malware.[26]To counteract these risks, cybersecurity policies must evolve to include AI-specific safeguards, real-time fraud detection mechanisms, and robust user verification protocols.

Additionally, open-source image and video synthesis models, such as Stable Diffusion, have been exploited to create abusive and misleading content, raising concerns about the ethical use of AI.[27] As these models improve and become more accessible, their misuse in fraud, identity theft, and political disinformation campaigns is expected to rise. Without strict oversight and security measures, open-source AI could fuel an unprecedented wave of AI-powered cyber threats.

Lack of robust access controls makes it difficult to restrict harmful modifications, and insufficient security audits allow vulnerabilities to persist undetected. To mitigate these risks, organizations must implement secure data handling protocols, enforce strict authentication measures, and conduct frequent vulnerability assessments to ensure AI models are not exploited for malicious purposes.

[25] Andy Greenberg, **"**GitHub's Deepfake Porn Crackdown Still Isn't Working,"*WIRED*, Jan. 30, 2024, https://www.wired.com/story/githubs-deepfake-porn-crackdown-still-isnt-working (Last visited on January 17 2025).
[26] Associated Press, "Justice Department Warns AI Is Fueling a Surge in Child Sexual Abuse Images,"*AP News*, May 8, 2024, https://apnews.com/article/ai-child-sexual-abuse-images-justice-department-42186aaf8c9e27c39060f9678ebb6d7b (Last visited on January 18 2025).
[27] *Id.*

### 2. *Commercialization and Intellectual Property Battles*

Despite being labelled as open-source, many AI models do not provide all the components required for full transparency. Some models only share pre-trained weights but restrict access to training data and algorithms, creating licensing complications. Businesses using these models for commercial purposes may unknowingly violate licensing agreements, leading to intellectual property disputes.

AI-generated content ownership remains a gray area, as models trained on copyrighted materials may inadvertently replicate proprietary data. As AI-generated content becomes more widespread, companies will need clearer guidelines on copyright, licensing, and commercial use of AI-generated outputs. Legal uncertainties surrounding AI ownership and intellectual property rights pose a challenge for organizations aiming to develop and commercialize AI solutions.[28]

### 3. *Ethical Challenges*

One of the biggest risks of open-source AI is its lack of oversight, which can lead to biased or discriminatory outputs.[29] Since open-source models lack centralized quality control, they may unintentionally perpetuate racial, gender, or socio-economic biases present in their training data.[30] Addressing this issue requires developing ethical AI frameworks, implementing bias detection tools, and ensuring diverse datasets to prevent discrimination.

### 4. *Regulatory Challenges*

Governments worldwide are struggling to regulate open-source AI, as these models can be freely modified and distributed without legal oversight. The rapid pace of AI advancements often outstrips existing regulatory frameworks, making it difficult to address issues such as accountability for AI-generated misinformation, unauthorized use of copyrighted data in AI training, and enforcement of ethical AI deployment guidelines.

---

[28] Reuters, **"**Legal Primer on Open GenAI Models**,"***Reuters Legal Industry*, Aug. 15, 2024, https://www.reuters.com/legal/legalindustry/legal-primer-open-genai-models-2024-08-15 (Last visited on January 16 2025).

[29] OpenCV, **"**Thoughts on AI Ethics**,"***OpenCV Blog, Jan 10 2025,* https://opencv.org/blog/thoughts-on-ai-ethics (Last visited on January 14 2025).

[30] *Id.*

Regulatory bodies must collaborate with AI researchers and industry leaders to create adaptable legal frameworks that balance innovation with responsible AI governance. Without clear regulations, companies and developers may face legal uncertainty regarding the ethical and commercial use of open-source AI. The EU has recently enacted the AI Act first of its kind the world to regulate the AI.

## IV. The EU AI act and its impact on open-source AI

The EU AI Act is the world's first comprehensive artificial intelligence legislation, designed to regulate AI development and deployment. Its primary goal is to ensure the responsible use of AI, balancing innovation with risk management.[31] For the open-source AI community, the Act introduces specific regulations, particularly for high-risk AI systems and general-purpose AI (GPAI) models.[32] While limited-risk AI systems have fewer compliance obligations, developers of high-risk and systemic-risk AI models must adhere to strict transparency and documentation requirements.[33]

### 1. *Risk-Based Classification of AI Systems*

The EU AI Act classifies artificial intelligence systems into five risk levels based on their potential impact on human rights, safety, and fundamental freedoms. AI systems posing an unacceptable risk, such as those that scrape facial images without consent, are strictly prohibited. High-risk systems that affect public safety or essential services must comply with stringent transparency, documentation, and risk assessment requirements. Limited-risk systems, like chatbots and generative AI tools, must inform users they are interacting with AI-generated content to prevent deception. Minimal-risk systems face only standard legal obligations as they pose little to no threat. A new category, systemic-risk models, covers certain powerful general-purpose AI systems—those trained with over 10 FLOPs requiring developers to provide detailed technical documentation on training, testing, and evaluation due to their broad societal influence.

[31] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, 2024 O.J. (L 311) 1.
[32] EU AI Act, 2024, Art 53.
[33] EU AI Act, 2024, Art 53.

### 2. *Stricter Regulations for High-Risk Open-Source AI*

For open-source developers working on high-risk AI models, the EU AI Act imposes significant compliance requirements. These include risk assessments, detailed documentation, and transparency measures to ensure that AI models are not misused for unethical or harmful purposes.[34] However, the regulation allows flexibility for low-risk open-source AI projects, ensuring that compliance requirements do not become a barrier to innovation.[35]

### 3. *General-Purpose AI (GPAI) Model Regulations*

The EU AI Act directly regulates general-purpose AI (GPAI) models, which are trained on large datasets and can perform multiple tasks. Large language models (LLMs), such as GPT-4, Llama 3, and Gemini, fall under this category.[36] Developers modifying or fine-tuning these models must also ensure compliance with AI Act obligations.

### 4. *AI Stack Classification*

The EU AI Act sets rules for both general purpose AI models and the applications that use them. At the model level it applies to broad general purpose AI models trained on large and varied data that can handle many tasks, and developers who create or significantly modify such models must meet duties of documentation, transparency, and risk control. At the system level it applies to specific AI systems that rely on these models to produce outputs or make decisions, such as chatbots or apps built on large language models, and the obligations at this level change depending on how risky the particular system is judged to be.

### 5. *Compliance Requirements for Open-Source AI Developers*

Developers working on limited-risk AI systems must comply with the following requirements[37].Clearly inform users that they are interacting with an AI system. Since not all users

[34] EU, AI Act, 2024, Art 16.
[35] EU, AI Act, 2024, Art 52.
[36] Umberto Nizza, "What Do AIs Think About the AI Act? An Experimental Analysis of the EU Approach on Artificial Intelligence**,"** 36 *Eur. Bus. L. Rev.* (forthcoming 2026), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1234567 (posted Nov. 20, 2024).
[37] EU AI Act, 2024, Art 50.

have technical expertise, this disclosure must be clear and thorough. AI-generated content (audio, images, videos, text) must be labeled as artificially generated or manipulated in a machine-readable format. Watermarking tools, such as Gradio's built-in features, can help meet this requirement. If an AI system generates deepfakes or other synthetic content, the deployer must disclose its use. For artistic works, this disclosure should be made in a way that does not interfere with the user experience.

#### 6. *Obligations for Open-Source Non-Systemic Risk GPAI Models*

For open-source GPAI models that do not present systemic risk, developers must comply with specific obligations under the AI Act.[38] Developers must provide a detailed summary of the content used to train the model, following an AI Office-approved template. Developers must ensure compliance with EU copyright laws. If copyrighted content is used for AI training, developers must respect opt-out requests from content creators. Developers should integrate opt-out mechanisms, such as respecting website robots.txt files or using tools like Spawning's API, which helps creators prevent their content from being used for AI training. Compliance measures will be refined through industry guidelines and codes of practice, expected by May 2025. Developers should stay updated on these evolving regulations.

## V. Striking a balance: the future of open-source AI

### 1. *Regulated Open Source*

Open-source AI promotes collaboration and accelerates technological advancement by making models and tools accessible to a broad audience. However, this openness necessitates robust legal and ethical frameworks to prevent misuse and ensure responsible development. The European Union's AI Act exemplifies such an approach, imposing transparency, risk assessment, and data protection requirements on AI systems, including open-source models. Organizations must

[38] EU AI Act, 2024, Art 53.

conduct thorough risk assessments, implement necessary safeguards, and maintain detailed documentation to comply with these regulations.[39]

### 2. *Hybrid Licensing Models*

To navigate the tension between openness and security, hybrid licensing models have emerged. These models grant access to AI technologies while imposing specific restrictions to mitigate potential risks. For instance, certain open-source AI licenses may limit commercial use or require adherence to ethical guidelines, thereby balancing the benefits of openness with the need for control over sensitive capabilities. Clear and enforceable licensing agreements are critical for protecting the rights of developers and users, ensuring that AI technologies are utilized responsibly.[40]

### 3. *Community-Led Initiatives in Open-Source AI*

The success of open-source AI is not just about technology; a global community of contributors drives it. Various initiatives have emerged to ensure AI remains transparent, ethical, and inclusive. AI Fairness 360, an open-source toolkit maintained by IBM, helps detect and mitigate bias in AI systems, promoting fair and unbiased decision-making.[41] Papers with Code is another vital initiative, linking AI research papers to their corresponding open-source implementations, making academic findings more accessible to developers.

Anthropic's Constitutional AI focuses on aligning AI with human values, ensuring that AI systems operate ethically and responsibly.[42] Meanwhile, Stability AI Community, the team behind Stable Diffusion, fosters innovation in generative AI, enabling artists, researchers, and developers to

[39] A&O Shearman, **"**Zooming in on AI #16: Open Source Artificial Intelligence**,"***A&O Shearman on Tech*, https://www.aoshearman.com/en/insights/ao-shearman-on-tech/zooming-in-on-ai-16-open-source-artificial-intelligence (Last visited on January 15 2025).

[40] *Id.*

[41] IBM**, "**AI Fairness 360**,"***IBM Research*, https://ai-fairness-360.org. (Last visited on January 4 2025).

[42] DigitalOcean, "Top Open-Source AI Platforms," *DigitalOcean Resources*, https://www.digitalocean.com/resources/articles/open-source-ai-platforms (Last visited on December 30 2024).

create new applications powered by AI-driven creativity.[43] These initiatives highlight the importance of collaboration in shaping AI's future.

#### 4. *AI Sandboxing*

AI sandboxing involves creating controlled environments where AI models can be developed, tested, and evaluated before public release. These sandboxes allow developers to assess the performance, safety, and ethical implications of AI systems in a contained setting, reducing the risk of unintended consequences upon deployment. By simulating real-world scenarios, sandboxing facilitates the identification and mitigation of potential issues, ensuring that AI models meet established standards before they are widely accessible.[44]

## VI. Conclusion

The shift towards proprietary AI underscores a fundamental challenge in the AI industry: how to balance accessibility, innovation, and security. Open-source AI has historically fuelled technological advancements by fostering collaboration and transparency. However, as AI systems grow more powerful, concerns over misuse, cybersecurity threats, and ethical dilemmas have led to increasing restrictions on AI accessibility. The debate continues, should AI remain fully open, be partially restricted, or become entirely closed?

A completely closed AI ecosystem may limit progress and create monopolies, restricting access to cutting-edge AI technology for researchers, startups, and smaller enterprises. Conversely, fully open AI presents security risks, as malicious actors could exploit advanced AI systems for fraud, cyberattacks, or disinformation campaigns. The most viable solution appears to be a regulated openness, where AI remains accessible but is governed by ethical, legal, and technical safeguards to prevent harm.

---

[43] *Supra* note 153.

[44] European Parliamentary Research Service, "Artificial Intelligence Act: EU Regulatory Sandbox for AI,"*European Parliament*, 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf. (Last visited on January 15 2025).

The EU AI Act provides a framework for this approach by regulating AI based on risk levels. It imposes strict compliance requirements on high-risk and systemic-risk AI models while allowing flexibility for low-risk open-source AI projects. Developers of general-purpose AI (GPAI) models must document their training data, ensure compliance with copyright laws, and implement transparency measures to align with EU regulations. Additionally, AI-generated content, such as deepfakes and synthetic media, must be clearly labelled to prevent misinformation and deception.

Going forward, global AI governance must establish clear legal frameworks that uphold accountability, fairness, and responsible innovation. The future of AI will likely involve a hybrid model, where AI remains partially open, enabling research and development while enforcing strong security, ethical, and regulatory measures. By striking this balance, the AI industry can continue to evolve responsibly, ensuring that AI serves the broader interests of society while mitigating risks associated with unchecked AI development.

[This page was left blank intentionally]

# INTERPLAY BETWEEN DATA PRIVACY REGULATION AND ANTITRUST PRACTICES IN NEW ECONOMY AND AN ANALYSIS OF THE DIGITAL COMPETITION BILL

*[1]

**Abstract**

*The 'new economy' has emerged as a focal point of current discourse, owing to its considerable consequences for economic dynamics and regulatory frameworks. This paradigm change, marked by significant economies of scale and the resulting network externalities, requires careful study by policymakers. Strategic manipulation of data for non-price competition in this setting raises significant privacy and competition concerns, emphasizing the critical need for comprehensive legal and regulatory actions to address these changing market dynamics. This article is centred on these primary concepts and aims to show the negative ramifications of data's potential threats to Indian privacy and competition regulations. The article will first examine the concept of 'Big Data,' with a particular emphasis on its negative consequences, as demonstrated by the Cambridge Analytica case. It will next investigate the implications of Big Data and non-price competition in the antitrust landscape, highlighting the enormous problems they present to existing regulatory frameworks. The article delves deeper into the relationship between the Digital Data Protection Act of 2023 and the Competition Act of 2002, examining their interactions in depth through a series of important cases. It tries to understand how these legal systems connect and what consequences they have for data regulation in the Indian context. To overcome the particular difficulties presented by digital marketplaces, the paper makes the case for regulatory harmony and suggests that the new legislative framework Digital Competition Bill, which combines competition law with data privacy, proves to be ineffective due to an ex-ante approach. Finally, it seeks to test to what degree an ex-ante approach is viable and suggests a way forward for an ex-post approach.*

**Key Words:** Big Data, Digital Data Protection Act, Competition Act, Digital Competition Bill, Antitrust Practices

[1] Mythri Raj, 3rd year, B.A.LL.B, Christ University, mythri.raj@law.christuniversity.in & Solomon Cruz, 3rd year, B.A.LL.B, Christ University, solomon.cruz@law.christuniversity.in

## I. Introduction

The advent of the digital era has led to an exponential increase in the generation and utilization of personal data. This has necessitated robust regulatory frameworks to ensure data security, privacy, and compliance. Globally, people and communities are becoming more dependent on digital platforms for everything from social networking and e-commerce to banking and healthcare. The new economy in India, fuelled by the proliferation of digital platforms, e-commerce, and tech-driven services, has witnessed a surge in market concentration.[2] In the marketplaces of the new economy, large-scale consumer data access is a competitive advantage where data-driven tactics are essential. In the digital age, where data is extremely essential to an economy, the occurrence of data breaches for competitive advantage has become a pressing concern. The privacy of personal data is a major worry raised by modern technologies, despite their unparalleled ease and efficiency. The intersection of antitrust laws and data protection has become a crucial point in the regulatory landscape in the digital era, as the new economy is defining the boundaries of communication and trade.

A paradigm shift in the economic environment brought about by the advent of the digital era has given rise to the so-called "New Economy." Nevertheless, the new economy presents several obstacles to the enforcement of antitrust laws. The conventional antitrust rules designed for traditional markets are difficult to adapt to the dynamic and data-intensive nature of digital marketplaces. This has necessitated robust regulatory frameworks to ensure data security, privacy, and compliance. We must comprehend how data and the new economy interact as we navigate this digital revolution. Because of its enormous worth, personal data is now considered a crucial economic asset that is changing market dynamics and requiring a review of current regulatory frameworks. This change necessitates a more in-depth analysis of data use, protection, and regulation in the context of the new economy.

## II. Literature review

[2]S Srinivasan, V Sinha and S Modi, 'Drafting a pro-antitrust and Data Protection Regulatory Framework' (2023) 4 Indian Public Policy Review 35.

1. **The Interplay between Data Privacy and Competition Law in India, Vishal Rjavash (2022):** The article discusses the debate on whether data protection and privacy should be integrated into competition law. One side argues for proactive antitrust enforcement to protect consumers' data while the others believe existing rules suffice. The Competition Commission of India is increasingly focusing on big data's impact on aspects of competition law.
2. **Drafting a Pro-antitrust and Data Protection Regulatory Framework, S. Srinivasan, V. Sinha, and S. Modi (2023):** The digital era's growth has led to increased personal data generation and utilization, necessitating robust regulatory frameworks on data security, privacy and compliance. The competition authorities around the world have started addressing data privacy in its antitrust framework, highlighting a need for balanced approach.
3. **The Digital Personal Data Protection Act: Yet Another Jurisdictional Overlap? Toshit Shandilya, Deepanshu Poddar (2023)**: Balancing privacy, competition and relevant regulations is necessary as they emphasize the need for user consent and highlight potential anti-competitive effects. However, an ex-ante framework proves to be detrimental. This is due to the fact that CCI takes cognizance of a case once competition concern arises, whereas the Digital Competition Bill taking an ex-ante approach would curb all kinds of technological innovations by making large entities subject to high thresholds.

## III. Data in the new economy

Due to the growing importance of technology in numerous areas of the global market, there has been a considerable shift in the market's characteristics and mechanisms. This new market has been dubbed the "new economy," and Judge Richard Posner is one of the most prominent people who has studied it. Posner emphasized that the old economy is distinguished by heavy capital investment, low investment rates, and infrequent entry and exit. The new economy, on the other hand, has little capital investment, rapid rates of innovation, frequent entry and exit, and economies of scale.[3] The most important characteristic to examine for this topic is the economics of scale or

[3]R A Posner, 'Antitrust in the New Economy' (2000) https://ssrn.com/abstract=249316 (Last visited 12 September 2024).

network externalities. Because of network externalities, the value of the products will either decrease or increase depending on the number of users in the market. In the new economy, the value of a product rises in proportion to its output or the number of users who use it. Instagram, a popular social media app, is a contemporary example. If only one person has an account on the app, they will have no one to show their pictures or messages, but as the number of users grows, so does the interactivity, and the user will find it more valuable. This is the main secret to the success of highly interactive products like the telephone and email. This network externality poses an anti-competition risk to the market because with network externality also comes path dependence. Path dependence happens when the users of a product prefer uniformity over a better, more efficient product. This could potentially create a very high barrier to entry into the market, making it impossible for new entrants with a better product to enter the market because it would be extremely costly for them to essentially force people out of their uniformity and to use their more efficient and better product.[4] Hence, anti-trust law will have to take in the implications and challenges that come with the new economy to ensure competition persists and that consumers get the best product.

### 1. *What is 'Big Data'*

Even though data has been used for products and services in the market for a long time, the new market is unique. The scale at which data is processed differs in the new digital market. Because users cannot comprehend the extent to which their data is being taken away, the absolute scale at which data is processed and collected in the new market creates information asymmetry in the market.[5] This is called the 'Big Data.' The Cambridge Analytica case popularized the drawbacks of big data, and it provided a lot of perspective to the average person, who was initially unaware of the extent to which their data was being used, and is now in a state of panic and shock about how much freedom they actually have in their life choices.

Cambridge Analytica is a data policy consultancy firm founded by Alexander Nix in London in 2013. Their objective is to use "data-based behavioural analysis" to understand individual

[4] *Id.*

[5] Filippo Lancieri and Patricia Morita Sakowski, 'Competition in Digital Markets: A Review of Expert Reports' (2021) 26 Stan JL Bus & Fin 65.

motivation.[6] This company first came to the spotlight in 2015 when a journalist pointed out that their app 'this is your digital life' is used to take a lot of data from users through Facebook without their consent.[7] Subsequently, the firm also came under fire when there was widespread reporting of its involvement in the 2016 US presidential elections.[8] The huge amount of data that the firm had was taken without the consent of the users, and it was further used to manipulate the voters' decisions, all of which is illustrated very aptly in the popular Netflix documentary 'The Great Hack'.[9] Cambridge Analytica is well-known for its suspected influence on the Brexit referendum, which marked Britain's exit from the European Union. Furthermore, the company's role in the Trinidad and Tobago presidential elections has been observed, demonstrating its political power. This opened the public's eyes to the scale at which their minds could be influenced through technology and propelled the world into a stage where everyone started to actually realize the value data holds, not only in privacy but also in the decision-making of the public. Data could be used as a weapon to take away the concept of free thought so subtly that no one would notice until it was too late.

### 2. *Role of Big Data in Antitrust*

Bigger companies that sell a wider variety of goods gather more data and better-quality data, giving them an advantage over competitors when developing new items. Dynamic economies of scale result from this phenomenon, allowing businesses with larger datasets to improve their goods more effectively than their smaller competitors. This makes it very difficult to enter and grow in many digital sectors. To be more precise, these companies gather large-scale population datasets that contain a great deal of information on a lot of people, as well as high-dimensional datasets that contain a lot of information about specific users. Combining these datasets allows for unmatched customization and precise insights into people who aren't yet in the database a data externality. The increasing returns to scale seen in these kinds of businesses are a result of these traits working

[6] Mustafa Eren Akpinar, *A Review on the Relationship of Big Data and Cambridge Analytica* (2022) 2 IBAD 56 10.7456/100201100/006.

[7] Elena L. Boldyreva, Natalia Y. Grishina and Yekaterina Duisembina, *Cambridge Analytica: Ethics And Online Manipulation With Decision-Making Process* (2018) 91 https://www.europeanproceedings.com/article/10.15405/epsbs.2018.12.02.10 (Last visited 20 September 2024).

[8] *Supra* Note 188.

[9] Amita Verma, Karan Jawanda and Arshdeep Kaur, *Data Privacy and Cambridge Analytica: A Case Study* (2021) 24 SUPREMO AMICUS [368].

together in concert.[10] The economics of scale have driven large corporations to amass as much data as possible, raising concerns about privacy and anti-trust practices.

A number of recent cases demonstrate how upstarts have been able to surpass established businesses by utilizing large amounts of data. While well-known examples such as Google replacing Yahoo and Facebook replacing MySpace are well-known, there are many more instances of well-established businesses losing market share to creative newcomers. These examples highlight the revolutionary effect that strong data use may have, resulting in a changing environment where new entrants can quickly surpass their more seasoned competitors.[11] This has also been highlighted by the Facebook case, in which Facebook has been under investigation in Germany by the Bundeskartellamt. They have allegedly infringed on the data privacy of 1.6 people to abuse their market power and maintain dominance.[12] The CCI described "big data" as the "oil" of the twenty-first century in *Matrimony v. Google*[13]. The CCI said in the same judgment that while data-based marketplaces give consumers enormous benefits, they also cause them to lose control over their personal data.[14]

The way that big data is changing market dynamics and data usage interacts with regulatory frameworks is becoming more intricate. Large datasets can be used by businesses to gain a competitive edge, which has brought attention to the need for a balanced strategy that takes consumer protection and innovation into account. Addressing the anti-competitive dangers associated with data-driven business models and making sure that the advantages of data usage do not outweigh the privacy hazards that individuals face are dependent on this dual focus. As a result, in order to properly manage the convergence of data privacy, competitiveness, and the new economic realities brought forth by digital transformation, the regulatory landscape must change. This leads to a crucial analysis of how to strike a balance in the new economy between regulation, competitiveness, and data privacy.

---

[10] Stigler Committee on Digital Platforms: Final report *The University of Chicago Booth School of Business*, https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report (Last visited 12 September 2024).

[11] Tucker, Darren S. and Wellford, Hill, *Big Mistakes Regarding Big Data* (December 1, 2014). Antitrust Source, American Bar Association, https://ssrn.com/abstract=2549044, (Last visited 20 September 2024).

[12] Maria Wasastjerna, *Competitive Law, Big Data and Privacy* (2017) 10 Int'l In-House Counsel J 1.

[13] Matrimony v Google, Case No. 7 and 30 of 2012, paragraph 86.

[14] *Id.*

## IV. Balancing Data Privacy, Competition, and Regulation in the New Economy

In recent years, there has been a significant convergence between competition law and privacy. When this relationship initially gained attention as a legal matter ten years ago, it was highly disputed.[15] There was a growing consensus that privacy ought to be considered a non-price component of competitiveness. In its Telecom Report, CCI defines data usage as "non-price competition," which suggests that an organization may use customer data to get a competitive advantage over rivals in the market.[16] In addition to presenting information security difficulties, data extraction and analysis raise other serious concerns. Organizations possessing access to vast databases and the most recent innovations frequently have a significant advantage over those without these resources, giving them an unfair competitive advantage. As such, it is imperative to underscore that violations of data privacy give rise to antitrust concerns.

However, the question of whether antitrust legislation could handle privacy issues persisted, with some claiming that the antitrust remedy would be worse than the privacy problems themselves. But technological breakthroughs and the development of social media business models have made it abundantly evident how privacy and antitrust are related.

An important piece of law in India, the Digital Personal Data Protection (DPDP) Act, 2023,[17] attempts to control how corporations manage personal data in order to safeguard the privacy of individuals. Drawing heavily from the General Data Protection Regulation[18] of the European Union, the DPDP provides a comprehensive definition of "personal data" with numerous applications.[19] This Act is a significant step towards ensuring the privacy and security of individuals' data in the digital age. The Data Protection Act will cover the processing of personal data in India, including data that is processed online and offline that has been digitalized. It will

[15] Maureen K. Ohlhausen & Alexander P. Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy', (2015) 80 ANTITRUST L.J. 121, 122-23.

[16] Amlegals, *Interplay between Data Protection and Competition Law, Law Firm in Ahmedabad* (Jan. 4, 2023) https://amlegals.com/interplay-between-data-protection-and-competition-law/ (Last visited 21 September 2024).

[17] Digital Personal Data Protection (DPDP) Act, No. 22 OF 2023, Acts of Parliament.

[18] General Data Protection Regulation, (Regulation 2016/679, abbreviated GDPR).

[19] Korff D, 'The Indian Digital Personal Data Protection Act, 2023, viewed from a European Perspective' [2023] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4614984 (Last visited 21 September 2024).

also include the processing of personal data outside of India that is related to the provision of goods or services in India.[20]

Taking into consideration the fact that the Competition Act, 2002[21] was originally designed to regulate traditional markets, it might not completely take into consideration the distinctive features of digital markets. According to reports, the Indian government has formed a Committee on Digital Competition Law (CDCL) to examine whether the current legal framework adequately addresses anti-competitive behavior in digital marketplaces in order to allay these worries[22]. This suggests that the necessity for competition legislation to be changed and adjusted to the needs of the modern economy has been acknowledged.

This has implications for businesses as well as customers, as the marginalized groups are on guard. The dispute between competition law and data privacy in India gained attention mostly because of the WhatsApp data privacy policy change case.[23] This incident highlighted the reliance on large data corporations unilaterally and spurred discussion about the need for competition law authorities to step in and protect consumer rights.

Further, it can be emphasized that the inherent conflict arising from the different objectives of the Competition Act and the DPDP Act, underscores the complex interplay between data privacy and competition law. This conflict highlights the need for regulatory harmony to address both privacy violations and anti-competitive behavior in the digital ecosystem. It is clear that consent is required for the acquisition and processing of user data, particularly by dominant businesses, and that this is covered by both the DPDP and the Competition Act. Their different objectives are what lead to the confrontation between the two. While the Competition Act focuses on stopping dominant businesses from unjustly using permission for the collection of personal data to get a commercial advantage, the DPDP seeks to stop the abuse of personal data.

---

[20] *Id.*

[21] The Competition Act, 2002, No. 12 of 2003, Acts of Parliament, India.

[22] V Dhall, G Desai, S Bhat, A Badoni and J Hirani, '*India: Big-Tech Regulation: Biting Off More Than We Can Chew?'* (26 April 2023) https://www.mondaq.com/india/antitrust-eu-competition-/1304578/big-tech-regulation-biting-off-more-than-we-can-chew (Last visited 21 September 2024).

[23] WhatsApp privacy case: A timeline, IKIGAI LAW (Aug 9, 2018) https://www.ikigailaw.com/article/444/ourstory#:~:text=In%202016%2C%20WhatsApp%20changed%20its%20privacy%20policy%20to,of%20this%20writ%20petition%20in%20the%20same%20year (Last visited 21 September, 2024).

Data-driven strategies are driving market concentration in the digital economy, which raises questions about possible antitrust breaches.[24] In the modern economy, data breaches that result from market competition may give rise to antitrust actions. Consumer data exploitation or breach may enable unfair behaviours including predatory pricing, abuse of dominance, and anti-competitive agreements. Digital platforms have the ability to subtly impact competition through data-driven methods rather than pricing.[25] For instance, Amazon may utilize information about user purchases and seller data from third parties on its online marketplace to advance and develop its own brand at the expense of other companies. These data-driven strategies may have an influence on user data privacy and competition at the same time. In order to maintain healthy competition, avoid monopolistic practices, and safeguard consumers, authorities must modify their approaches as traditional markets merge with digital platforms and data-driven services.

In order to investigate the intersection, let us consider an imaginary situation similar to the WhatsApp instance. Let's say that business 'X' controls the majority of the internet calling services industry and that it conditions its 'free' services on consumers agreeing to divulge personal information. X may stop providing its services to a user who refuses to give consent. Even if this complies with DPDP, the CCI may still find it to be anticompetitive.[26]

Thus, Competition laws and privacy laws are at increasingly at odds in the digital economy. Data privacy is becoming a more common pro-competitive defence used by dominant corporations against claims of exclusionary behaviour. The CCI can form a prima facie view regarding a potential violation of the Competition Act, 2002, upon receiving information or a complaint by an informant, who can be any person, alleging anti-competitive behaviour.[27] Should it prevail, the defendant may use a pro-competitive business defence to shield themselves from legal action. Data privacy is also being used in addition to the traditional defenses of intellectual property rights and consumer protection interests.

---

[24] A Avinash Kotval and I Saraswat, '*Proposed Merger Control Amendments: Questions and Potential Consequences*' (2022)https://indiacorplaw.in/2022/08/proposed-merger-control-amendments-questions-and-potential-consequences.html (Last visited 20 September 2024).

[25] *Supra* note 184.

[26] Toshit Shandilya, Deepanshu Poddar '*The Digital Personal Data Protection Act: Yet Another Jurisdictional Overlap?*' AZB & PARTNERS (Sept. 20, 2023) https://www.azbpartners.com/bank/the-digital-personal-data-protection-act-yet-another-jurisdictional-overlap (Last visited 20 September 2024).

[27] The Competition Act, 2002, §19, No. 12 of 2003, Acts of Parliament, India.

A coherent regulatory framework is necessary to balance the growing concerns about competition and data privacy. The dependence on data-driven tactics emphasizes the necessity of maintaining market competition while safeguarding individual privacy. The Digital Personal Data Protection (DPDP) Act, 2023 in India and the Competition Act, 2002 both emphasize this need. This prompts us to investigate the ways in which these two laws interact and how they affect the digital economy.

## V. The Alignment of DPDP Act and Competition Law in India through the Digital Competition Bill

As mentioned in the preceding paragraph, there is an inherent conflict that arises when balancing data privacy laws with competition laws. Although both sets of laws seek to benefit the public, they do so in fundamentally different ways. Data privacy rules, such as the DPDP, take a more user-specific approach, protecting individual consumers' data and privacy rights.[28] Competition laws, such as the Indian Competition Act, take a sector-wide approach, striving to benefit consumers by encouraging competition and banning anti-competitive practices throughout the market. As a result, while these rules overlap, they cannot be completely harmonized without increasing complexity and misunderstanding when dealing with issues involving both data and competition laws.

The Previous example demonstrates that neither antitrust regulation nor data privacy legislation will be effective in dealing with difficulties of this nature that arise. As a result, it is critical that new legislation is adopted to establish a separate authority to enforce such unusual circumstances. Such law will give enforcers explicit authority to handle complicated situations involving market competitiveness and public welfare relating to data privacy. The Committee on Digital Competition Law [29], established by the Ministry of Corporate Affairs of the Government of India, published its report on February 27, 2024, and proposed an ex-ante approach for Systematically Significant Digital Enterprises offering Core Digital Services.[30]

---

[28] Giuseppe Colangelo, *The Privacy/Antitrust Curse: Insights From GDPR Application in Competition Law Proceedings*, (2023), https://papers.ssrn.com/abstract=4599974 (Last visited on 25 September 2024).

[29] REPORT OF THE COMMITTEE ON DIGITAL COMPETITION LAW – 2024, by Ministry of Corporate Affairs, Government of India

[30] Lokesh Bulchandani, '*Overview of India's Digital Competition Bill*', 2024, https://competitionlab.gwu.edu/overview-indias-digital-competition-bill-2024 (Last visited on September 28, 2024).

This Bill establishes rules that data 'gatekeepers' must follow during their activities. This proactive method increases efficiency by allowing authorities to investigate companies on a preliminary basis, rather than a reactionary one that commences inquiries only after infractions occur. This technique not only conserves resources but also reduces the risk to the public. The ex-ante approach, however, has some drawbacks due to its lack of flexibility, which could cause problems particularly in India's ever-changing market, so we recommend that some ex-post points be included in the bill, even though the bill should be primarily ex-ante based. One of the essential criticisms is that the Bill has the potential to affect the growth of Indian start-ups.

The proposed Digital Competition Bill 2024 in India introduces heavy-handed ex ante regulations for major digital companies, diverging from the objective of the Competition Act which deals with case-by-case ex post analysis.[31] This shift could stifle innovation and technological development by imposing blanket prohibitions on certain practices without thorough investigation. The Competition Act allows for a nuanced approach, assessing each case on its merits and considering the dynamic nature of digital markets. By contrast, the Digital Competition Bill pre-emptively restricts practices, potentially curbing business initiatives and failing to address the specific abuse of dominance issues effectively. Similar ex-ante clauses can be found in the EU's Digital Market Act, which has drawn criticism from OECD Competition Committee chair Frederick Jenny, who claims that rather than promoting competition, it is inhibiting it.[32]

Thus, an ex-ante approach may prove ineffective, especially in a country like India, where the digital markets evolve at a relatively slow pace. This slower evolution can lead to the application of laws without a thorough analysis and understanding of the new economy. Additionally, certain practices may appear anti-competitive at first glance but may actually comply with the Competition Act upon closer investigation. By adopting an ex-ante approach, companies are held accountable for potentially anti-competitive practices at the outset, which may hinder the innovation and growth of certain companies in the emerging economy.

---

[31] Vinod Dhall, '*India's Digital Competition Bill, 2024 – The Need for Caution',* (April 11, 2024) https://touchstonepartners.com/indias-digital-competition-bill-2024-the-need-for-caution/ (Last visited on 30th September 2024).

[32] Frédéric Jenny, *'Competition law enforcement and regulation for digital ecosystems: Understanding the issues, facing the challenges and moving forward'*, (September 2021), https://www.concurrences.com/en/review/issues/no-3-2021/articles/frederic-jenny (Last visited on 30th September 2024).

## VI. Conclusion

In the evolving landscape of India's digital economy, balancing data privacy with competition requires a nuanced regulatory approach. Given the potential conflicts between antitrust and privacy goals, this research advocates for an ex-post regulatory model which intervenes after careful analysis of actual market impacts, rather than imposing broad, ex-ante restrictions on digital firms. An ex-post framework would allow regulators to assess real-world data use and competition effects, tailoring responses to specific anti-competitive or privacy-violating behaviors only as they arise.

CCI in its latest order penalized meta for abusing its dominant position through WhatsApp's 2021 privacy policy update. The policy made data sharing with Meta companies mandatory for all users, removing the option to opt-out. The CCI found that this constituted an unfair condition and violated Section 4 of the Competition Act by forcing users to accept data collection terms, undermining their autonomy. Additionally, Meta was found to be leveraging its dominance in the OTT messaging app market through smartphones to harm competition. The CCI issued cease-and-desist orders and imposed behavioral remedies. However, the CCI also noted the need for a broader view of user data and its impact on competition, indicating that the existing framework might not be sufficient to address all data-related concerns.[33]

While some actions may initially appear to hinder competition, as seen in cases like Prachi Agarwal v. UrbanClap[34] and Harshita Chawla v. WhatsApp,[35] further scrutiny revealed them to be in compliance with the Competition Act. Thus, an ex-post approach acknowledges that not all data-centric business models harm competition or privacy.A careful, evidence-based approach will be crucial to deal with matters concerning data privacy and anti-competitive practices.

[33] In Re: Updated Terms of Service and Privacy Policy for WhatsApp users (Suo Motu Case No. 01 of 2021) and connected matters.
[34] Case No. 30 of 2020, Order dated March 24, 2021.
[35] Case No. 15 of 2020, Order dated August 18, 2020.

[This page was left blank intentionally]

# INTELLECTUAL PROPERTY AND BIOTECHNOLOGY: NAVIGATING THE EVOLVING LANDSCAPE OF MICROORGANISM PATENTING IN INDIA

*[1]

**Abstract**

*Patent protection plays a crucial role in incentivizing novation by granting exclusive rights to inventors for a stipulated period. The patentability of microorganisms has been a subject of legal and ethical debate, particularly in India, where its recognition followed the 2002 amendment to the Patents Act, 1970, in compliance with the TRIPS Agreement. However, a significant challenge remains, i.e., the absence of a precise definition of 'microorganism' in both Indian law and international intellectual property treaties, has lead to ambiguities in determining patent eligibility.*

*This paper examines the legal framework governing the patentability of microorganisms in India, analysing key provisions of the Patents Act and relevant international agreements such as the TRIPS Agreement and the Budapest Treaty. It further explores landmark judicial decisions without which patenting of microorganisms was not permitted. Such decisions have shaped the legal landscape of microorganism patents. Additionally, the study discusses the implications of microorganism deposition under the Budapest Treaty and India's compliance mechanisms. By analysing legislative provisions and judicial decisions, this paper aims to highlight the complexities and challenges associated with microorganism patenting in India and its alignment with global patent regimes. This paper then concludes on the current scenario on patenting of microorganisms in India.*

**Key words**: TRIPS, Budapest Treaty, micro-organism, novelty, invention, discovery, product of nature.

[1] Dr. Fakkiresh S. Sakkarnaikar, Professor of Law, GNLU fsakkarnaikar@gnlu.ac.in & Kunjal Arora Teaching and Research Asssociate, GNLU.

## I. Introduction

Patents are the legal rights from the Government, for a given time period, related to the inventions made by a patentee. Patents are part of Intellectual Property Rights (IPRs). The inventions or creations originating from a human brain are due to human's intellect and if the intellect results into a commercially important product, then it becomes property[2]. Thus, patents are IPRs, the laws governed by the Government to provide rights to a patentee. The patent of any invention is granted for a stipulated time period and once expired is available in public domain for its use by general public[3]. The main objective of a patent is that any new invention out of a human intelligence should be protected as a private property and encourage inventions and development of industries[4]. By patenting a new invention, a patentee can protect the making, using and selling of his own invention and thus a patent helps in protecting the commercial competition of an invention for a limited time period[5]. The patents are territorial rights which means the country in which the patent was filed and granted, the rights given to the patentee are in accordance with the law of that country[6]. The patent laws of a country decide the fate of domestic and foreign investments in a country and thus help in growth and development of that country. In India the Patents law enacted in 1911, the present *Patents Act,* 1970 came into effect from the year 1972 and was amended from time to time for protecting intellectual property rights in the country. For any invention to be patented it should fulfil following criteria:

i) It should be novel not to be recognized anywhere in the world at the time of patent application

ii) It should not be obvious to a person skilled in the field of invention

iii) It should be useful to the society.

[2] Senan, S., Haridas, M. G., & Prajapati, J. B., Patenting of Microorganisms in India: A Point to Ponder, 100 Current Science 159 (2011).
[3] Balachandra Nair, R. & Ramachandranna, P., Patenting of Microorganisms: Systems and Concerns, 16 J. Commer. Biotechnol. 337 (2010).
[4] Braga, P., Sepulveda, C. P., & Noel, M., Intellectual Property Rights and Economic Development, World Bank Discussion Papers (2000).
[5] Besen, S. M. & Raskind, L. J., An Introduction to the Law and Economics of Intellectual Property, 5 J. Econ. Persp. 3 (1991).
[6] Nair, R. & Ramachandra, P., Patenting of Microorganisms: Systems and Concerns, 16 Journal of Commercial Biotechnology 337 (2010).

There are three types of Patents,

i) Utility patents – patents granted for new process, machine, article of manufacture or any new improvement in a process or a matter,
ii) Design patents – granted for a new and ornamental design of an article,
iii) Plant patents – granted for invention or discovery of a new variety of a plant.[7]

Patent laws initially included the inventions in chemical, mechanical and electrical and the later amendments covered the areas of information technology, electronics, pharmacy, and biotech products and processes.[8] The patentability of microorganisms was added in the Indian Patents Act, 1970 after the amendment in 2002, in compliance with the Trade Related aspects of Intellectual Property Rights (TRIPS).[9]

### *1. What is a Microorganism?*

Generally, a microorganism is an organism which is too small and cannot be observed with naked eyes and requires a microscope to do so. Microorganisms include bacteria, fungi, archae, protists, planktons, viruses etc. Microorganisms can exist as a single cell or a cluster of cells[10]. Furthermore, the definition of a microorganism is also found in dictionaries such as in 'The Concise Oxford Dictionary' which defines a microorganism as "Any of various microscopic organisms, including algae, bacteria, fungi, protozoa and viruses".

According to the *Rules For The Manufacture, Use/Import/Export And Storage Of Hazardous Micro Organisms/ Genetically Engineered Organisms Or Cells* Notification of Ministry of Environment and Forest, "*microorganisms*" shall include all the fungi, bacteria, , mycoplasma, viruses, algae, protodoans, cell lines and nematotes mentioned in the schedule and also include

[7] Mikulka, Y., The Rise of Design Patents, 42 Litig. 13 (2016).
[8] *Id.*
[9] Prasad, V., Microorganisms and the Indian Patents Scenario, Khurana and Khurana Associates and IP Attorneys (2020).
[10] Baker, W. P., Leyva, K. J., Lang, M., Goodman, B., & Goodmanis, B., Classifying Microorganisms, 25 Science Scope 40 (2002).

those which have not been presently known to exist in the country or they not have been discovered so far[11].

With the advent of technologies and discoveries in microbiology there are various products which can be produced from microorganisms like ethanol, enzymes, pigments, metabolites, drugs, biofuel, etc. and the demand for these products is constantly rising. Hence, IPRs have become important to explore the microorganisms for commercial purpose.[12]

### *2. Patentability of Microorganisms*

Patentability of a microorganism has been a subject of much discussion however, what constitutes a microorganism has not been defined in patent acts or IP treaties. Thus, there is an ambiguity in the exact meaning of what all includes in 'microorganism' for patentability. Various case laws have discussed patentability of microorganism and thus, that has helped in clearing the understanding of the word.

The first patent based on microorganism was granted in 1873 to Louis Pasteur which involved microbiological process of fermentation of beer.[13] Before the year 1980, patents were given for the inventions based on the microbiological processes but not for the actual living entities *per se* because they have been considered natural products and thus, not patentable. Thus, in all nations across the world, such '*products of nature'* doctrine simply excluded the materials which existed in nature from being patented, including living organisms.

This doctrine specifies that the potentially patentable subject matter must be created by human action. Thus, discovery of a new organism found in nature is not patentable. Using this doctrine, a person could claim patent for the processes using such microorganisms like fermentation processes or purification of compounds but could not claim patent for microorganism because they are living organisms and products of the nature. Microorganisms are considered as a part of Nature and their

[11] Rules for the Manufacture, Use/Import/Export and Storage of Hazardous Micro Organisms/Genetically Engineered Organisms or Cells, Notification of the Ministry of Environment and Forest, Sec. 3(v) (Dec. 5, 1989).
[12] Vitorino, L. C. & Bessa, L. A., Technological Microbiology: Development and Applications, 8 Frontiers in Microbiology 827 (2017).
[13] Pasteur, L., Improvement in the Manufacture of Beer and Yeast (U.S. Patent No. 141,072) (1873).

mere discovery won't be considered as invention. There is a difference between discovery and invention.

This non-patentable status of the micro-organisms was changed with the landmark judgment of the United States Supreme Court in *Diamond v. Chakraborty 1980,*[14] wherein a genetically modified bacterium was patented. In this case, Dr. Anand Chakraborty filed a patent for a genetically engineered bacterium which was able to breakdown the components of crude oil. Though, initially rejected, later it was accepted by the US Supreme Court.

In this case, Dr. Chakraborty made patent claims to the method of producing the bacteria and to the bacteria itself. The US Patent Office denied the patent stating that, the microorganism is a product of the nature and therefore non-patentable. The case went to appeal and finally to the Supreme Court, which discussed the issue in detail and gave the judgment in favour of Dr. Chakraborty. The Court stated that a genetically engineered bacterium having the ability of treating oil spills was an 'invention' because it had the novelty, utility, non-obviousness and industrial applicability which a naturally occurring microorganism could not. Before this decision, patents were granted only on the 'process claims' i.e. the processes in which the microorganisms were used as a medium or part of the invention and this position was changed to the 'product claims' as well.

## II. Patentability of microorganisms in India

India is a signatory of *General Agreement on Trade and Tariff* (GATT) along with 116 countries. The World Trade Organization (WTO) has also imposed a number of rules over member countries under TRIPS agreement, to help protect the patent rights in all the fields of technology The TRIPS agreement has an article on 'Patentable Subject Matter'- Article 27(3) (b) which states that, microorganisms other than plants and animals can be patented, and any non-biological or microbiological process involved in production of plants or animals other than biological processes can only be patented by the member countries. Hence it allows patentability of microorganisms[15]. The TRIPS agreement defines the term 'microorganism' in the broader sense, inclusive of any product out of cellular materials like plasmid, genes. India, being a member country of the TRIPS

[14] Diamond v. Chakraborty, 447 U.S. 303 (1980).

[15] The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) art. 27 (3) (b).

agreement, amended the *Indian Patents Act 1970* in 2005 to comply with it and hence, the Indian patent law also allowed the patentability of microorganisms. As per Section 3(j) of the *Patents Act,* 1970, plants, animals, seeds, and biological processes, excluding microorganisms are not eligible for patents. As a result, this provision permits the patentability of microorganisms under the Indian patent law.[16] Patenting of microorganisms which are already existing in nature is not allowed rather it will be considered as discovery. On the other hand, genetically modified versions of these microbes which impart enhanced properties to them can be patented as it may lead to improved microbial processes, having applications in the industry.[17]

### *1. The Case of Dimminaco A G v. Controller of Patents and Designs &Others*

In the year 2002, the Calcutta High Court took a remarkable decision on the patentability of biotechnological process with living end product in the case of *Dimminaco A.G. v. Controller of Patents and Designs & Others*[18]. In this case, Dimminaco A.G., a Swiss Company, filed patent for the process of preparing a live vaccine for an infection in poultry animals called *Bursitis*.

Initially the Controller of Patents refused to grant a patent of this vaccine which involved the processing of certain micro-organismic substances as it was believed to be, simply a natural process, without involving any manufacturing activities and thus, was not allowed to be patented under Section 2(1) (j).[19] It was a regular practice at that time, to grant patents to only the non-living things and actual inventions that fulfilled the patentability criteria, even though there was no such limitation in the Indian Patent Act.

An appeal was filed in the Calcutta High Court which was looked into by the Court and rejected the pleadings of the Controller which stated that patents are only given in the process which results in a substance, article or manufacture and a vaccine with live microorganism is none of those things. The court then stated in the judgment that, the process of manufacturing a product out of a living organism, is not excluded from the definition of 'manufacture'. Since, the vaccine being the

[16] The Patents Act, 1970, Section 3(j).
[17] *Supra* note 220.
[18] I.P.L.R. 255 (2002).
[19] Sec 2 (1) (j)- invention means a new product or process involving an inventive step and capable of industrial application.

end product of the process was novel, vendible and capable of industrial application and had a proper utility, court allowed the appeal and sent it back for reconsideration.

### *2. The case of Monsanto v. Nuziveedu Seeds*

The judgment of *Monsanto Technology Pvt. Ltd. v. Nuziveedu Seeds*[20] was also about patentability of microorganisms. Monsanto Technology LLC had registered a patent on Nucleotide Acid Sequence (NAS) containing the *Bacillus thuringiensis* gene which was used to produce Bt Cotton. This gene when inserted into DNA of cotton seeds, because of NAS the bollworms feeding on the seed were killed due to NAS and therefore reduced the dependence of farmers on insecticides and pesticides.

This dispute between Monsanto and Nuziveedu Seeds began when Monsanto issued proceedings in the Delhi High Court for patent violation. Nuziveedu filed a counter-claim challenging the validity of the patent. Nuziveedu claimed that, NAS was merely a chemical composition not capable of reproduction and is not a man-made inventive microorganism which can be capable of industrial application. The Supreme Court reverted the matter back to the Delhi High Court to seek expert advice and evidence, and the claims on NAS was rightly entertained by the Indian Patent office. This could have been a golden opportunity for the Supreme Court to explain and decide upon the matter of microorganism patentability in India.

## III. Deposition of microorganisms in India

It is mandatory in the Patent Law that the detailed information of an invention should be submitted in order to file a patent of an invention, referred to as '*sufficiency of disclosure'*.[21] Hence, if a microorganism needs to be patented, then it is necessary to deposit the living sample of that microorganism to an authorized and recognized depository authority for biological inventions. The purpose of the sufficiency of disclosure is to enable a skilled person to reproduce the invention for himself after a specific time period for which patent was granted.

For disclosure and the deposition of microorganisms, the *Budapest Treaty on the International Recognition of the Deposit of Microorganisms for the Purposes of Patent Procedure* was enforced

[20] AIR 2019 SC 559.
[21] *Supra* note 15

in 1980. The Budapest Treaty is administered by World Intellectual Property Organization (WIPO)[22].This Treaty ensures that a patentee need not deposit microorganisms or a biological material in all the countries where he/she applied for the patent. The patentee needs to deposit microorganism or a biological material only once at a recognized institution at his/her own country, known as International Depository Authority (IDA), which also is recognized by all the other countries under Budapest Treaty. Likewise, all the member countries have their own IDAs. Including microorganisms, Budapest Treaty, also allows the deposition of plant and animal cells, hybridoma cell, cell lines, RNA, plasmids etc., in IDA.[23] India being a part of Budapest Treaty has two recognized IDAs namely, Microbial Culture Collection (MCC), Pune and Microbial Type Culture Collection and Gene Bank (MTCC) at Institute of Microbial Technology (IMTECH), Chandigarh respectively.[24] Apart from these two IDAs, India has thirteen more culture collection canters which are used to store various biological resources recognized under National Biodiversity Authority (NBA).[25]

## IV. Conclusion

The patentability of life forms, particularly microorganisms, remains a subject of legal, ethical, and policy debate, especially in India, where intellectual property laws continue to evolve alongside advancements in biotechnology. While the TRIPS Agreement mandates patent protection for microorganisms and certain microbiological processes, ambiguity persists due to the absence of a precise legal definition of "microorganism" in both international treaties and Indian patent law. This lack of clarity creates inconsistencies in determining the scope of patent protection, often leading to legal disputes and varied judicial interpretations.

Landmark judicial decisions, as discussed, have significantly influenced the framework governing microorganism patenting. These cases have established that while naturally occurring microorganisms are considered 'products of nature' and are not patentable, genetically modified

[22] Mishra, V. K., Verma, H., & Singh, G., Recent Development of Patent in Indian Scenario with Special Reference to Microbial Patents, in PGPR Amelioration in Sustainable Agriculture 159 (2019).
[23] Parashar, A., International Depository Authority and Its Role in Microorganism's Deposition, 11 J. Clin. & Diagnostic Res. DE01 (2017).
[24] Kochhar, S., Indian Perspective for Sustainable Development Agenda and Functional IPR and ABS Domains in Agriculture, 21 J. Intell. Prop. Rights 7 (2016).
[25] *Supra* note 22.

microorganisms which exhibit novel characteristic and industrial application may qualify for patent protection. However, the granting of patents for altered microorganisms also raises concerns regarding monopolization, potential restrictions on further research, and ethical considerations in biotechnology.

India's legal framework, while aligned with international obligations under TRIPS agreement, still faces challenges in striking a balance between promoting innovation and ensuring equitable access to biological resources. The requirement of "*sufficiency of disclosure*," as mandated under Indian patent law and the Budapest Treaty, plays a crucial role in facilitating transparency and reproducibility in such scientific advancements. At the same time, the lack of an explicit statutory definition continues to create legal uncertainties that could hinder research and development in biotechnology.

As discoveries in genetic engineering advance at an unprecedented pace, it is important for lawmakers and the judiciary to adapt the patent system to address such emerging challenges. Providing a clear and comprehensive definition of microorganisms within Indian patent law would help resolve the existing ambiguities and foster a more predictable legal framework. Furthermore, it is necessary that the lawmakers must ensure that patent regulations in the country strike an appropriate balance between incentivizing biotechnological innovation, preventing bio-piracy, and maintaining accessibility to genetic resources for future research.

Ultimately, as India positions itself as a global leader in biotechnology and life sciences, the need for a well-defined, transparent, and progressive patent regime becomes increasingly vital. Strengthening the legal framework governing microorganism patents will not only promote scientific and industrial development but also ensure that intellectual property rights serve the broader interests of society.

[This page was left blank intentionally]

# BEYOND NDAs: REIMAGINING TRADE SECRET PROTECTIONS FOR COLLABORATIVE AI RESEARCH IN INDIA

*[1]

**Abstract**

*India's Artificial Intelligence (AI) ambitions are hindered by a legal framework ill-equipped to protect trade secrets in collaborative research. Outdated laws like the Indian Contract Act, 1872, and the Information Technology Act, 2000, fail to address modern challenges such as algorithmic theft or accidental data leaks. Courts, forced to interpret vague statutes, deliver inconsistent rulings, leaving businesses unsure how to safeguard innovations like proprietary algorithms or datasets. This uncertainty stifles partnerships, as startups fear leaks while global firms hesitate to collaborate.*

*This paper proposes reforms to bridge these gaps. A dedicated trade secrets law could clarify terms like "reasonable secrecy efforts" and introduce swift remedies for breaches. Borrowing global insights, India could adopt tiered protections—strict safeguards for core secrets (e.g., AI code) and flexible rules for shared data. Regulatory sandboxes would allow secure testing of AI tools, while whistleblower protections ensure ethical accountability. Judicial training on AI-specific risks and sector-specific guidelines (e.g., strict health data rules, open farm-tech norms) would balance security with innovation. By modernizing its legal framework, India can transform from a bystander to a leader in the AI era, where trust, collaboration, and fairness drive progress.*

**Keywords:** Artificial Intelligence, Trade Secrets, Collaborative Research, Intellectual Property Rights, Legal Reform.

[1] Hemant Singh, 1st year LLM, Rajiv Gandhi National University of Law, hemants4066@gmail.com & Himanshu Singh, 2nd year B.A. LL.B, National Law University Delhi, himanshu.singh23@nludelhi.ac.in

## I. Introduction

AI has evolved over the years; it is not just a testament to human innovation but also a reflection of legal ambiguities. From the early days of rule-based systems like ELIZA in the 1960s to today's generative models like ChatGPT, AI has evolved from a niche academic pursuit to a cornerstone of global innovation.[2] This transformation, however, has surpassed the legal frameworks designed to protect the Intellectual Property (IP) powering it. Unlike traditional inventions such as, a patentable engine design or a copyrighted novel, the value of AI lies in intangible assets: algorithms trained on vast datasets, neural network architectures, and proprietary methodologies. These are not easily wrapped into existing IP categories, creating a paradox where the very tools driving progress are left vulnerable to exploitation.

Historically, IP regimes prioritized tangible creations. The World Trade Organization's (WTO) TRIPS Agreement (1994), for instance, standardized patent and copyright protections globally but said little about algorithms or data.[3] This gap became glaring as AI shifted from theoretical research to commercial applications. Consider IBM's Deep Blue, which defeated Chess Grandmaster Garry Kasparov in 1997. While its hardware was patented, the software's decision-making logic, a precursor to modern machine learning, remained unprotected, raising questions about how to safeguard iterative, self-improving systems.[4] Today, AI startups in Bengaluru and Hyderabad face similar dilemmas. Their innovations such as predictive healthcare models or crop-yield algorithms, are often shielded only by secrecy, as patents require disclosing methodologies that competitors could replicate.

The rise of collaborative AI research further complicates this landscape. India's National Strategy on Artificial Intelligence (2018) emphasizes public-private partnerships to tackle challenges in agriculture, healthcare, and education.[5] While these collaborations accelerate innovation, they also blur ownership lines. For example, when a government lab partners with a startup to develop an AI-driven diagnostic tool, who owns the algorithm, the lab funding the research, the startup

[2] Joseph Weizenbaum, *ELIZA—A Computer Program for the Study of Natural Language Communication Between Man and Machine*, 9 COMM. ACM 36 (1966).
[3] Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.
[4] Feng-Hsiung Hsu, *Behind Deep Blue: Building the Computer That Defeated the World Chess Champion* (2002).
[5] NITI Aayog, *National Strategy for Artificial Intelligence* (2018).

providing the data, or the clinicians refining the model? Unlike the U.S., where the *Bayh-Dole Act* (1980) clarifies IP ownership in federal projects, India lacks analogous legislation, leaving stakeholders reliant on ad-hoc contracts.[6]

### 1. *Importance of Trade Secret Protection in AI Innovation*

If patents are the sturdy locks on innovation's doors, trade secrets are the hidden keys. Nowhere is this truer than in AI, where breakthroughs often hinge on proprietary datasets and undisclosed training techniques. Take OpenAI's GPT-4: while its capabilities are public, the model's architecture and training data remain closely guarded secrets. This secrecy isn't mere corporate paranoia—it's a survival strategy. The *Indian Contract Act,* 1872, a law drafted when telegrams were cutting-edge, governs confidentiality through Section 27, which voids contracts imposing "restraint of trade."[7] Courts have interpreted this narrowly, often siding with employees who leave firms with proprietary knowledge, arguing that overly broad NDAs stifle career mobility.[8]

Trade secrets serve as the invisible scaffolding of AI innovation, shielding the proprietary algorithms, datasets, and methodologies that power breakthroughs. Unlike patents, which demand public disclosure, trade secrets thrive on confidentiality, thereby making them uniquely suited to protect innovations that evolve rapidly or lose value once exposed. In AI development, where models like neural networks or recommendation systems are refined iteratively, secrecy often determines a firm's competitive edge. For instance, the precise architecture of a machine learning model or the curated dataset it trains on can be worth millions, yet these assets rarely fit neatly into traditional IP categories.[9]

## II. Understanding Trade Secrets in AI Research

### *1. Definition and Legal Characteristics of Trade Secrets*

Trade secrets are the silent guardians of innovation, akin to a family's cherished recipe passed down through generations—valuable precisely because it remains hidden. Unlike patents or copyrights, which demand public disclosure, trade secrets thrive on confidentiality. Legally, a trade secret encompasses any information that is not generally known, provides economic value

[6] Bayh-Dole Act, 35 U.S.C. §§ 200–212 (1980).
[7] Indian Contract Act, 1872, No. 9, Acts of Parliament, § 27 (India).
[8] Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber, (1996) 61 DLT 6.
[9] Carys J. Craig & Ian R. Kerr, *The Death of the AI Author*, 52(1) Ottawa L. Rev. 31 (2021).

because of its secrecy, and is subject to reasonable efforts to maintain its confidentiality.[10] Take for e.g., Coca-Cola's formula, guarded for over a century, or Google's search algorithms. These are quintessential examples of trade secrets that have shaped industries.

Globally, frameworks like the U.S. *Uniform Trade Secrets Act* (UTSA) formalize these elements, emphasizing secrecy, economic benefit, and protective measures.[11] Similarly, the WTO TRIPS Agreement obligates member nations, including India, to protect undisclosed information.[12] Yet, India lacks a dedicated trade secrets law, relying instead on the *Indian Contract Act,* 1872, and judicial precedents to enforce confidentiality. For instance, in *Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber*, the Delhi High Court upheld Non-Disclosure Agreements (NDAs) but warned against overly broad terms that hinder employee mobility.[13]

Three pillars underpin trade secret law:

1. **Secrecy**: The information must not be publicly accessible. A startup's proprietary AI training data, for example, loses its value if leaked on platforms like GitHub.
2. **Economic Value**: The secret must offer a competitive edge. Consider the algorithms behind Netflix's recommendation engine or Tesla's autonomous driving systems, both derive worth from exclusivity.[14]
3. **Reasonable Efforts**: Businesses must demonstrate proactive steps to protect secrecy, such as NDAs, restricted data access, or encryption. Courts often scrutinize these measures.

Unlike patents, which expire after 20 years, trade secrets can endure indefinitely, provided they remain confidential. However, this longevity is a double-edged sword. Once exposed, protection evaporates, as seen when Waymo sued Uber over stolen self-driving car secrets.[15]

[10] Uniform Trade Secrets Act § 1(4) (1985).
[11] *Id.*
[12] Agreement on Trade-Related Aspects of Intellectual Property Rights, art. 39, Apr. 15, 1994, 1869 U.N.T.S. 299.
[13] Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber, (1996) 61 DLT 6.
[14] World Intell. Prop. Org., *Trade Secrets and Innovation* (2022).
[15] Waymo LLC v. Uber Techs., Inc., 256 F. Supp. 3d 1059 (N.D. Cal. 2017).

### 2. *Types of AI Trade Secrets: Algorithms, Data, Models, and Frameworks*

In the world of AI, trade secrets are not monolithic, rather they are a mosaic of interconnected elements, each requiring distinct protection strategies. From the mathematical blueprints guiding AI decisions to the curated datasets fuelling them, these secrets form the backbone of innovation. Let's unpack the four pillars of AI trade secrets:

#### *a. Algorithms: The Invisible Architects*

Algorithms are the DNA of AI systems, the coded instructions that transform raw data into actionable insights. Consider OpenAI's GPT-4: while its outputs dazzle users, its transformer architecture remains shrouded in secrecy.[16] This deliberate opacity is strategic. Reverse-engineering such algorithms could take years, but leaks through platforms like GitHub are alarmingly common.

The legal challenge lies in defining algorithmic secrecy. Unlike patents, which protect functional inventions, algorithms thrive on their obscurity. For instance, in *Diljeet Titus v. Alfred A. Adebare*, the Delhi High Court recognized proprietary methodologies as trade secrets but stressed the need for "reasonable precautions" to safeguard them.[17] Without watertight NDAs and access controls, algorithms risk exposure.

#### *b. Data: The Fuel of AI*

Data is the lifeblood of AI, but its value hinges on exclusivity. Imagine an Indian health-tech startup training its diagnostic model on a dataset of 10 million anonymized patient records. Once leaked, competitors could replicate the model, rendering the data worthless. This vulnerability is amplified in India, where the *Digital Personal Data Protection Act,* 2023 mandates strict data handling but offers limited recourse for trade secret breaches.[18]

The stakes are higher with sensitive datasets. Courts have yet to clarify whether such datasets qualify as trade secrets or constitute mere "business information" under the *Indian Contract Act*.

#### *c. Models: The Crown Jewels*

[16] OpenAI, *GPT-4 Technical Report* 5 (2023).
[17] Diljeet Titus v. Alfred A. Adebare, (2006) 130 DLT 330.
[18] Digital Personal Data Protection Act, No. 22 of 2023, § 9(2) (India).

Trained AI models, like ChatGPT or Tesla's Autopilot, are the end products of algorithmic labour. While their outputs are public, their internal "weights"[19] (parameters dictating behaviour) are guarded fiercely.[20] These weights, often refined over millions of iterations, are vulnerable during collaborations.

India's lack of a trade secrets statute complicates enforcement. While the EU's *Trade Secrets Directive* explicitly protects "the composition of a product," Indian courts rely on contractual interpretations, as seen in *Burlington Home Shopping v. Rajnish Chibber*.[21]

*d. Frameworks: The Unsung Architects*

Frameworks like Google's TensorFlow or Meta's PyTorch, are the unsung architects of AI development. While these tools are often open-source, their proprietary optimizations, such as techniques to accelerate model training or reduce computational costs—remain fiercely guarded.[22] Scholars argue that the line between open-source collaboration and trade secret protection in AI frameworks is increasingly blurred. For instance, Google's TensorFlow, while publicly accessible, incorporates undocumented optimizations that streamline large-scale training, feature competitors like Microsoft's CNTK have struggled to replicate.

The legal ambiguity around such optimizations is stark. A study done by Sonia K. Katyal delves into the complex relationship between trade secret protections and open-source software development. It investigates how companies manage the conflicting priorities of sharing code within collaborative public platforms while safeguarding proprietary modifications to maintain a competitive edge.[23]

[19] Yann LeCun, Yoshua Bengio & Geoffrey Hinton, Deep Learning, 521 *Nature* 436 (2015).
[20] Ian Kerr, *The Death of the AI Author*, 22 Minn. J.L. Sci. & Tech. 1, 14 (2021).
[21] Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber, (1996) 61 DLT 6.
[22] Martín Abadi et al., *TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems*, arXiv preprint arXiv:1603.04467 (2016).
[23] Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 Cornell L. Rev. 1184 (2019).

## III. Global Lessons for India

### *1. The U.S. Approach – Defend Trade Secrets Act (DTSA) and AI Protection*

The United States' *Defend Trade Secrets Act* (DTSA), enacted in 2016, has become a cornerstone for safeguarding AI innovations.[24] Its most striking feature is the provision for *ex parte seizures*, which allow courts to swiftly confiscate stolen trade secrets without prior notice to the accused—akin to a "legal emergency response" for high-stakes cases. The 2017 legal dispute *Waymo v. Uber* highlights the complexities of safeguarding trade secrets in AI. Waymo accused a former employee of misappropriating proprietary autonomous vehicle technology for Uber's benefit. Though no preliminary injunction was granted during litigation, the case ultimately led to a settlement requiring Uber to refrain from utilizing Waymo's confidential data. This outcome underscores the urgency of robust legal safeguards in AI innovation, where proprietary algorithms can be disseminated worldwide almost instantaneously, amplifying risks to IP.[25] This legal agility is critical in AI, where a leaked algorithm can be replicated globally within hours.

Yet the DTSA isn't just about brute force. It balances enforcement with whistleblower protections, ensuring employees can report misconduct, like unethical AI practices, without retaliation.[26] For India, this duality offers a blueprint. While the *Draft Digital India Act,* 2023 acknowledges AI governance, it lacks mechanisms to expedite trade secret disputes or protect whistleblowers in tech collaborations.[27] Integrating DTSA-inspired safeguards could bridge this gap, ensuring innovation thrives on trust, not secrecy.

### *2. The EU Model – Trade Secrets Directive and Open Innovation Balance*

The European Union's (EU) approach to trade secrets is a masterclass in balancing secrecy with collaboration. At its core, the *EU Trade Secrets Directive (2016)* seeks to harmonize protection across member states while safeguarding the open innovation ethos that drives Europe's tech ecosystem.[28] Unlike rigid frameworks that prioritize corporate control, the Directive acknowledges

[24] Defend Trade Secrets Act, 18 U.S.C. § 1836 (2016).
[25] Waymo LLC v. Uber Techs., Inc., 256 F. Supp. 3d 1059 (N.D. Cal. 2017).
[26] 18 U.S.C. § 1836 (2016).
[27] Ministry of Electronics & Info. Tech., Draft Digital India Act (2023), https://www.meity.gov.in (last visited Jan. 25, 2025).
[28] 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.

that not all knowledge can, or should, be locked away. Instead, it carves out space for healthy competition and collective progress, making it uniquely suited to the collaborative nature of AI development.

Central to the Directive is the principle of **proportionality**. Trade secrets are protected only if acquired through "breach of confidence" or "dishonest means," explicitly exempting reverse-engineering of publicly available products.[29] This distinction is vital. In AI, where tools like open-source frameworks (e.g., TensorFlow) are widely shared, the Directive ensures that studying and improving existing code isn't penalized. By contrast, India's reliance on vague contractual terms often leaves startups uncertain about what constitutes "legitimate" experimentation versus theft.

Another cornerstone is the requirement for "**reasonable steps**" to protect secrecy.[30] This flexible standard avoids a one-size-fits-all mandate, recognizing that a fledgling AI firm in Lisbon might lack the resources of a tech giant like SAP. For instance, a small team could secure its algorithms through encrypted access and NDAs, while larger firms might deploy advanced digital rights management. The EU's emphasis on practicality here is instructive for India, where startups often struggle with overly rigid or ambiguous confidentiality norms.

For India, the EU's model offers a roadmap to reconcile secrecy with openness. By adopting proportionality and reasonable safeguards, India could empower its startups to collaborate without fear while ensuring core innovations remain protected. The alternative, a patchwork of vague laws and erratic enforcement, risks stifling the very partnerships that drive AI progress.

### *3. China's Strict IP Laws – State-Controlled AI Innovation*

China's approach to IP and AI innovation is a cautionary tale of state power overshadowing private enterprise. At its core, China's legal framework prioritizes national interests over individual ownership, blurring the lines between trade secret protection and state control. Laws like the *Cybersecurity Law* and *Data Security Law* mandate strict data localization, requiring firms to store sensitive information domestically and share it with authorities.[31] While framed as safeguards

[29] *Id.* art. 3(1)(b).
[30] *Id.* art. 2(1)(c).
[31] Cybersecurity Law of the People's Republic of China (effective June 1, 2017), art. 37.

against foreign exploitation, these rules often serve dual purposes, bolstering state-backed AI initiatives while stifling independent innovation.

This state-centric model creates a paradox. On one hand, China has emerged as a global AI powerhouse, leveraging vast datasets from its population to train cutting-edge models.[32] On the other, foreign firms face daunting risks. Ambiguous statutes allow authorities to classify almost any data as "core" or "important," subjecting it to state scrutiny.[33] For startups, this uncertainty discourages transparency; collaborations with international partners dwindle under fears of forced technology transfers or data expropriation.

The broader lesson for India lies in the tension between control and creativity. China's model demonstrates how overreach can transform trade secret protection into a tool for centralized dominance, chilling the collaborative spirit vital for AI advancement.[34] India's *Digital India Act* must navigate this tightrope, securing critical data without replicating China's heavy-handedness. The challenge is not just legal but philosophical: fostering innovation demands trust, not just surveillance.

### *4. Lessons for India – Bridging Gaps with Global Insights*

India's AI ambitions hinge on learning from global experiments—adopting what works and sidestepping pitfalls. The U.S., EU, and China offer contrasting playbooks, but their collective wisdom points to three actionable lessons for India:

#### *a. Tiered Protections: Balancing Secrecy and Openness*

The U.S. DTSA demonstrates the value of urgency in protecting core innovations. For instance, *ex parte* injunctions could shield Indian startups from algorithmic theft during critical R&D phases.[35] Conversely, the EU's *Trade Secrets Directive* teaches proportionality—not all secrets deserve ironclad protection. Collaborative datasets, like anonymized health records shared with

[32] Data Security Law of the People's Republic of China (effective Sept. 1, 2021), art. 21.

[33] Rogier Creemers, China's Conception of Cyber Sovereignty: Rhetoric and Realization, in Governing Cyberspace: Behavior, Power, and Diplomacy 107 (Dennis Broeders & Bibi van den Berg eds., Rowman & Littlefield 2020).

[34] Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L.J. 687 (2015).

[35] Defend Trade Secrets Act, 18 U.S.C. § 1836 (2016).

researchers, should follow the EU's "reasonable steps" standard, fostering trust without stifling innovation.[36]

India's *Draft Digital India Act,* 2023 could formalize this tiered approach:

- **Core Secrets**: Algorithms, source code, and proprietary models safeguarded via expedited judicial remedies.
- **Collaborative Secrets**: Shared datasets governed by flexible confidentiality norms, encouraging public-private partnerships.[37]

*b. Ethical Safeguards: Whistleblowers and Accountability*

The DTSA's *whistleblower immunity clause* (18 U.S.C. 1833(b)) offers a blueprint for ethical AI governance.[38] In India, where biases in facial recognition tools or agricultural algorithms can harm marginalized communities, protecting insiders who expose flaws is critical. Embedding DTSA-style protections in the *Digital India Act,* 2023 could empower ethical dissent, aligning secrecy with social responsibility.

*c. Regulatory Sandboxes: Safe Spaces for Experimentation*

The EU's embrace of platforms like 'Hugging Face', where firms collaborate on AI tools in controlled environments, highlights the value of **regulated openness**.[39] India's proposed 'AI regulatory sandboxes' could replicate this, allowing startups to test models with shared data while protecting core IP.

*d. Avoiding China's Path: Nuance Over Control*

China's *Cybersecurity Law* and *Data Security Law*[40] illustrate the perils of conflating trade secrets with state control. India's approach must prioritize **sector-specific nuance** over blanket mandates. Stricter safeguards for health data under the *Digital Personal Data Protection Act, 2023* could

[36] 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, art. 2(1)(c).
[37] Ministry of Electronics & Info. Tech., Draft Digital India Act (2023), https://www.meity.gov.in (last visited Jan. 25, 2025).
[38] Defend Trade Secrets Act, 18 U.S.C. § 1833(b) (2016).
[39] Hugging Face, https://huggingface.co/ (last visited Jan. 26, 2025).
[40] Cybersecurity Law of the People's Republic of China (effective June 1, 2017), art. 37.

coexist with relaxed norms for agricultural AI, where open-source collaboration boosts rural innovation.[41]

## *IV.* India's Legal Gaps and Judicial Trends

India's legal framework, particularly in the technology and data sectors, presents several challenges. This chapter explores some of these issues by discussing statutory and contractual limitations, the difficulties of enforcing legal rights in multi-party collaborations, and a review of recent judicial trends on confidentiality in Indian courts.

### *1. Statutory and Contractual Limitations*

India's legal framework for protecting trade secrets resembles a puzzle missing critical pieces. Unlike jurisdictions such as the U.S. or EU, which have dedicated statutes, India relies on a patchwork of century-old laws and judicial interpretations. The *Indian Contract Act,* 1872, forms the backbone of trade secret protection, but its provisions are ill-suited for the complexities of AI and the broad language of the act may leave parties uncertain about obligations related to confidentiality and proprietary information in digital contexts. Section 27, for instance, prohibits agreements that impose "restraint of trade," creating confusion about how far businesses can go to safeguard secrets through NDAs or non-compete clauses.[42]

The *Information Technology Act,* 2000, adds another layer of ambiguity. While it penalizes unauthorized access to computer systems, it says nothing about algorithmic theft or accidental leaks during collaborations.[43] This gap leaves AI firms vulnerable, imagine a scenario where a disgruntled employee leaks a proprietary dataset through a misconfigured cloud server. Without specific provisions, victims must stretch existing laws to fit digital realities, a risky and often futile effort. Furthermore, statutory provisions in areas such as IP or data protection may be ambiguous or outdated. This legislative gap means that certain issues, like whether a trade secret can be easily reclassified or the extent to which digital data is protected under current law, remain open to interpretation.

[41] Digital Personal Data Protection Act, No. 22 of 2023, § 9(2) (India).
[42] Indian Contract Act, 1872, No. 9, Acts of Parliament, § 27 (India).
[43] Information Technology Act, 2000, No. 21, Acts of Parliament, § 43 (India).

The *Draft Digital India Act,* 2023, promised modernization but sidestepped trade secrets entirely.[44] This legislative silence forces businesses to rely on contractual "Band-Aids," like NDAs, which courts may later invalidate. The result? A culture of secrecy over collaboration, where startups hoard innovations rather than share them, stifling India's AI potential.

### *2. Enforceability Challenges in Multi-Party Collaborations*

Collaboration is the lifeblood of AI innovation, but India's legal system struggles to manage the intricacies of multi-party partnerships. Suppose an AI firm teams up with a research institute and a foreign tech giant, the web of responsibilities and liabilities becomes tangled. Contracts often fail to address third-party risks, like subcontractors or cloud providers, leading to disputes when leaks occur.

Jurisdictional hurdles compound these challenges. If a data breach involves servers in Singapore or collaborators in Germany, Indian courts may defer to international arbitration, dragging out resolutions for years. The lack of clear guidelines for cross-border disputes contrasts sharply with the EU's *General Data Protection Regulation (GDPR)*, 2016 which provides a roadmap for handling transnational data issues.[45] India's *Digital Personal Data Protection Act,* 2023, however, remains silent on trade secrets, leaving businesses navigating a legal fog.[46]

When disputes occur in a multi-party setting, it is not always clear which party bears the burden of proving that confidentiality was breached or that damages are warranted. The complexities multiply when foreign parties are involved, and the Indian legal system must consider principles of comity and international arbitration. All these factors contribute to an environment where parties may be reluctant to form partnerships that are crucial for technological progress.

### *3. Case Law Analysis: Confidentiality in Indian Courts*

Indian courts have addressed trade secret issues in several notable decisions, yet the outcomes often vary and legal clarity remains elusive.

#### *a. Diljeet Titus v. Alfred A. Adebare (2006)*

[44] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[45] General Data Protection Regulation (GDPR) 2016 O.J. (L 119) 1.
[46] Digital Personal Data Protection Act, No. 22 of 2023 (India).

In this case, the court discussed regarding the legal advice, opinion given by advocate to client which must be considered as a confidential and privileged information and the taking away of these by the defendants constituted a breach of confidentiality.[47]

*b. Burlington Home Shopping v. Rajnish Chibber (1996)*

In this case, the court held that the customer database, which was compiled over years with significant effort and investment of time and money, qualifies as a trade secret and a literary work under copyright law. According to the court, though the information might be common, but the unique selection, arrangement of data makes it protectable. The use of database by the defendant was deemed as an infringement of trade secret.[48]

*c. Dr. Sudipta Banarjee v. L.S. Davar & Company & Ors. (2022)*

The court held that the data shared by a professional body to its employees during their tenure falls under the head of confidential information, and is protected by law. Any unauthorised disclosure or use could lead to the breach and could cause irreparable harm to plaintiff's interests. Reinforcing the need to maintain strict confidentiality, the court emphasized that such protection is rooted in both equitable principles and common law.[49]

## V. Bridging Law and Innovation: Policy Interventions for AI-Centric Trade Secrets

### *1. Enact a Dedicated Trade Secrets Law*

India urgently needs a standalone trade secrets law tailored to address AI's unique challenges. Current laws, like the *Indian Contract Act*, 1872, are outdated and ambiguous, leaving businesses to navigate a maze of contractual clauses and judicial interpretations. A dedicated law should clearly define terms such as "algorithmic theft," "reasonable secrecy measures," and "trade secrets" to eliminate guesswork. For instance, borrowing from the U.S. DTSA, India could introduce *ex parte* injunctions to freeze stolen AI models swiftly while ensuring whistleblower protections. This law must balance corporate interests with public accountability, protecting innovations without stifling ethical transparency.

[47] Diljeet Titus v. Alfred A. Adebare, (2006) 130 DLT 330.
[48] Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber, (1996) 61 DLT 6.
[49] Sudipta Banerjee v. L.S. Davar & Company & Ors., (2022) 3 ICC 19.

### *2. Create Tiered Protections for Different Secrets*

Not all secrets are created equal. A *tiered framework* would distinguish between **core secrets** (e.g., proprietary algorithms, source code) and **collaborative secrets** (e.g., shared datasets, joint research). Core secrets could mirror the EU's strict protections, requiring robust safeguards like encryption and restricted access, while collaborative secrets might follow lighter rules, such as basic NDAs, to encourage partnerships. For example, a health-tech startup's diagnostic algorithm would qualify as a "core secret," warranting urgent legal remedies if leaked, while anonymized patient data shared with researchers could fall under "collaborative secrets" with simplified compliance. This approach fosters innovation without overburdening smaller players.

### *3. Protect Whistleblowers to Promote Ethical AI*

India's legal framework must shield employees who expose unethical AI practices, such as biased algorithms or privacy violations. Drawing from the *DTSA's whistleblower immunity clause*, Indian law should guarantee legal protection and anonymity for those reporting misconduct.

### *4. Establish AI Regulatory Sandboxes*

Regulatory sandboxes, safe environments for testing AI tools, can bridge the gap between secrecy and collaboration. Inspired by the EU's Hugging Face platform, India could create sector-specific sandboxes.

### *5. Train Judges on AI-Specific Legal Nuances*

Courts often struggle to apply outdated laws to AI disputes, as seen in *Wipro v. Beckman Coulter*, where non-compete laws were misapplied to algorithmic theft. Regular workshops led by tech experts and legal scholars could help judges understand AI's unique risks, such as algorithmic contamination or rapid replication of digital assets. Collaborations with institutions like the NALSAR or NLU Delhi could develop specialized modules on AI ethics, data privacy, and trade secrets, ensuring rulings reflect technological realities.

### *6. Clarify Cross-Border Collaboration Rules*

Global partnerships are vital for AI growth, but jurisdictional ambiguities deter Indian startups. Clear guidelines should define how NDAs and trade secret protections apply in cross-border disputes.

## VI. Conclusion

The revolution of AI in India lies on a delicate balance: protecting the secrets that drive innovation while fostering the collaboration that moves it forward. Today, this balance is skewed. Outdated laws like the *Indian Contract Act,* 1872 and the IT Act, 2000, leave businesses in uncertainty, where trade secrets are protected more by luck than law. Courts, burdened with interpreting vague statutes, deliver inconsistent rulings what qualifies as "reasonable efforts" in one case may be dismissed in another. This unpredictability stifles startups and deters global partnerships, leaving India's AI potential untapped. The solution lies in learning from global models while tailoring them to India's needs. A dedicated trade secrets law could replace guesswork with clarity, defining terms like "algorithmic theft" and setting clear standards for protecting innovations. Borrowing from the U.S. DTSA, India could introduce swift remedies like *ex parte* injunctions for urgent cases while safeguarding whistleblowers who expose unethical practices. For instance, a developer revealing biasness in a healthcare AI Technology should be protected, not penalized. Tiered protections are equally important because they differentiate core secrets (e.g., proprietary code) from collaborative data (e.g., anonymized datasets). Core secrets demand strict safeguards, while shared data thrives under flexible rules that encourage partnerships. Judges too need support. Training programs on AI Technology like how algorithms differ from traditional IP can ensure rulings reflect modern and up to date realities. Meanwhile, India must avoid China's trap of state-controlled data, opting instead for sector-specific rules: strict privacy for health tech, openness for agriculture. Trust is the foundation of progress. Patients sharing health data, startups collaborating with global firms all rely on faith in the system. By modernizing laws, India can transform itself from a spectator to a leader in the AI era, where innovation thrives not in secrecy but in secure and ethical collaboration. The time to act is now before the next breakthrough slips away.

[This page was left blank intentionally]

# COUNTERFEIT GOODS IN THE DIGITAL ERA: A LEGAL ANALYSIS OF TRADEMARK ENFORCEMENT AND ECOMMERCE PLATFORM LIABILITY IN INDIA

*[1]

**Abstract**

*Counterfeit goods have become a significant global challenge, threatening the brand reputation of the trademark owners and consumers trust in the brand. The rise of e-commerce has further facilitated the distribution of counterfeit goods. According to the OECD, the counterfeit and pirated goods market accounted for $464 billion in global trade in 2019, equating to 2.5% of world trade. Counterfeit products can be observed to be sold online mainly in two forms, that is, by way of creating standalone websites or by selling their products using large e-commerce platforms like Amazon, Flipkart, etc. Trademark Proprietors face a dilemma in the form of being unable to take action against the infringers due to the anonymity offered by the internet. Further, the effectiveness of an injunction is diluted, as infringers have the ability to open another avenue online to continue the sale of counterfeit goods by simply creating a new domain. This has led to owners taking action against the e-commerce platforms, using the concept of secondary liability. This paper explores the enforcement of trademark protection in the online world, against independent infringers and e-commerce platforms. The paper further explores the extent of liability of the e-commerce platforms in India compared to their foreign counterparts. Finally, the paper recommends various ways to curb the problem of counterfeit goods in the rise of e-commerce.*

**Key Words:** E-commerce, Infringement, Intermediary, Secondary Liability, Trademark

[1] Aditi Prabhu, 4th year B.A.LL.B, School of Christ, aditiprabhu11@gmail.com & Navya Joshi, 4th year B.A.LL.B, School of Christ, navyajoshiandrew@gmail.com

## I. Introduction

The supply of counterfeit products in the market has increased worldwide in the last decade. The sale of counterfeit products in the market is not only limited to luxury products but also extends to daily household items, which could, in most situations, result in fatal consequences for consumers. While some consumers purchase these counterfeit products unknowingly, others intentionally do so. Certain consumers are drawn by the reduced prices while being able to enjoy the presumed brand reputation, with an inferior quality of goods. For these reasons, the counterfeit market in the world continues to thrive. India is known for being ranked fifth amongst countries for having the largest counterfeit market.[2]

While counterfeit products were limited to being sold on the streets and in small retail shops, with the rise of the digital movement and the ease of selling goods online in the last two decades, counterfeiters have found a safe haven to sell their goods with ease. The low cost of setting up and maintaining e-commerce websites to sell counterfeit goods and the ease of re-establishing another website when it is taken down, along with the lesser amount of technical skills and staff required to maintain the stores,[3] further enables counterfeiting in the online world.

Counterfeit goods, when bought unknowingly by a consumer on an online platform, under the belief of buying the original product, may result in distrust of the brand and the e-commerce platform. Due to the anonymity offered to the platform and the sellers, the consumers are most often left remediless, and thereby suffer with a sub-par quality product. Although, counterfeit products in the online world have a negative impact on Trademark proprietors, they have the following positive impacts–

1. They raise brand awareness;
2. Driving consumers to directly purchase the product from the brand rather than from the platform (where there exists a possibility of receiving a counterfeit good); and

[2] PTI, India on 5th place in fake goods trade; China on top, The Economic Times (May 1, 2016, 4:26 PM) https://economictimes.indiatimes.com/news/economy/foreign-trade/india-on-5th-place-in-fake-goods-trade-china-on-top/articleshow/52064171.cms?from=mdr.

[3] Gina Boone, Designing Dupes: A Legislative Proposal for Holding Online Marketplaces Contributorily Liable for Counterfeit Goods, 31 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1310-1311 (Summer 2021).

3. The wealthy consumers of the brand pride themselves in being able to distinguish between a genuine and counterfeit product, and also by virtue of possessing the genuine product.[4]

The enforcement of Trademark protection in the physical realm is relatively easier due to the ease of gaining access to the name, location, phone number, etc., of the infringer. However, enforcement sets hurdles when most of the sellers or the platforms in the online world are anonymous. This paper aims to ascertain the liability of e-commerce platforms in the digital world for the sale of counterfeit goods and the extent to which secondary liability cab be imposed on an intermediary platform can be held secondarily liable for contributory trademark infringement along with the requirement for "knowledge" to determine liability.

Further, the paper analyses the current framework for trademark protection, especially with reference to protection in the online world. The authors trace the history of trademark protection when a trademark has been infringed on an online platform by a third party, as well as the secondary liability of e-commerce platforms for contributory infringement in foreign jurisdictions and in the Indian jurisdiction with the help of landmark precedents. Finally, the paper provides recommendations that can be adopted to safeguard the rights of the Trademark holders.

## II. Egalitarian Theory

The theoretical aspect associated with why consumers purchase counterfeit goods can be understood through the egalitarian theory. As inequality increases, consumers prefer counterfeit goods for their egalitarian value. This can be understood as the belief that counterfeit goods can restore equality in society.[5] Purchasing counterfeit goods is considered to bring about equality by levelling the unequal playing field of luxury markets as it makes such goods less exclusive. This is understood as the "*egalitarian value of counterfeit goods"*. This *value* is the reason behind the increase in the purchase of counterfeit goods. Consumers purchase such goods when they have

[4] C. Awele Nwajei, *Combating Counterfeit Couture: an Argument for the Application of Third Party Liability to E-Commerce Websites in the Fight against Counterfeit Luxury Goods*, 11 OHIO ST. BUS. L.J. 23, 28 (2017).

[5] Jingshi (Joyce) Liu, S. Wiley Wakeman & Michael I. Norton, The Egalitarian Value of Counterfeit Goods: Purchasing Counterfeit Luxury Goods to Address Income Inequality, 35 J. CONSUMER PSYCHOL. 269, 269–280 (2025).

ideologies which desire social equality and possessing the counterfeits of luxury goods provides them with this sense of social equality.[6]

## III. Evolution of Trademark Law in Digital Space

The rise in the use of e-commerce platforms has led to challenges for brands to protect their trademarks. This can be attributed to the growth in digital technology and access to the internet, which allows individuals to violate intellectual property rights.[7] When there is a violation of intellectual property rights, infringers make use of anonymizing technology to continue such violations. Moreover, the expenses associated with litigation make it difficult for owners to seek legal remedy for such violations.[8] The internet has brought in new challenges to brand owners related to trademark infringement which includes taking advantage of the brand's value. This type of trademark infringement happens through cybersquatting and typo squatting.[9]

As individuals have become more dependent on online marketplaces, it has led to an increase in counterfeit products in the digital age.[10] Trademark owners face tremendous challenges in monitoring large amounts of counterfeit products on e-commerce platforms and reporting and taking necessary legal actions against the sellers of such products.[11] Due to the sales of counterfeit goods happening through online marketplaces, sellers can evade the methods used to identify counterfeit goods.[12] This is because consumers usually identify counterfeit products through location and price, which becomes irrelevant in e-commerce platforms, and consumers eventually purchase the goods.[13]

Luxury brands contend that e-commerce platforms, like eBay, should be held liable for the sale of counterfeit goods on such platforms by the users. When such cases arise, Courts are required to analyse the level of knowledge that must be present to impose contributory infringement on the

---

[6] *Id.*

[7] Mark Bartholomew & John Tehranian, *The Secret Life of Legal Doctrine: The Divergent Evolution of Secondary Liability in Trademark and Copyright Law*, 21 Berkeley Tech. L.J. 1363, 1419 (2006).

[8] *Id.*

[9] Yafit Lev-Aretz, *Combating Trademark Infringement Online: Secondary Liability v. Partnering Facility*, 37 Colum. J.L. & Arts 639 (2014)

[10] Boone, *supra* note 294.

[11] Bartholomew and Tehranian, *supra* note 298.

[12] Daniel C.K. Chow*, Strategies to Combat Internet Sales of Counterfeit Goods,* 52 Seton Hall L. Rev. 1053 (2022)

[13] *Id.*

intermediary platforms where counterfeit products are sold.[14] To understand counterfeiting from an economic perspective, it is necessary to see how the infringers free ride on the trademark of a reputed brand. This affects the trade routes as they become polluted with counterfeit goods, which subsequently has far-reaching impacts on the global economy.[15] As counterfeited goods look like the original goods to a large extent, it becomes difficult for an ordinary customer to differentiate between them. Moreover, counterfeit goods are made with low-quality materials, which affects the brand's reputation in the market.[16]

Trademarks play a vital role in reducing the search costs of consumers.[17] Consumers are usually able to inspect the goods before purchasing them, which helps them to gather all the necessary information about a particular product.[18] This is not possible while purchasing goods through e-commerce platforms. Moreover, when counterfeit goods are sold through these online platforms, in many instances consumers are not aware that they may be purchasing counterfeit goods. This is because counterfeit goods freeride on the goodwill of a well-established brand in the market. Trademarks play a vital role in making the products identifiable to consumers and reduce the incentive which manufacturers have to cheat consumers by offering low-quality products[19] but when counterfeit products are sold on e-commerce platforms, they free-ride on the goodwill of an already established trademark and can take advantage of the fact that consumers may not be able to differentiate between the original product and the counterfeit product.

## IV. Current Legal Framework in India

The statute which primarily protects the interest of the registered or unregistered trademark holders is the Trademarks Act of 1999. The statute provides for various reliefs and protection in case of infringement, dilution, passing off, and other violations against a mark. However, with the change in technological status and the growing digital economy in India, the Information Technology Act,

[14] Kurt M Saunders' & Gerlinde Berger- Walliser, *The Liability of Online Markets for Counterfeit Goods: A Comparative Analysis of Secondary Trademark Infringement in the United States and Europe*, INT. LAW, 38 (2011).
[15] Prachi Tyagi, *Counterfeiting and Its Impact on Trademark in the Fashion Industry through the Lens of Indian Law*, 29 J. INTELLECT. PROP. RIGHTS 181 (2024).
[16] *Id.*
[17] *Id.*
[18] Mathias Strasser, *The Rational Basis of Trademark Protection Revisited: Putting the Dilution Doctrine into Context*, 10 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 375, 384 (2011).
[19] *Id.*

2000comes into the picture, governing the legal framework to be followed by online platforms. In addition, as the transactions ultimately affect the consumers, the Consumer Protection (E-commerce) Rules, 2020, ensures a framework to be followed by the marketplace and inventory entities in the marketing, sale, and purchase of goods and services online.[20]

### *1. The Trademarks Act, 1999*

The Trademarks Act, 1999 ("TM Act") provides various rights to trademark owners of registered and unregistered trademarks. Section 28 of the Act confers various rights after registration of a trademark. The registered proprietor has exclusive rights over the trademark, which has been registered for a specific class of goods and services, and can obtain relief when there is an infringement of the said trademark.[21] The Act also provides rights to protect the interests of unregistered trademark holders. The rights of the prior user of a trademark who is unregistered shall be protected over the rights of the proprietor who obtained registration for an *"identical or nearly resembling"* mark for an "*identical or nearly resembling"* goods or services.[22]

### *2. Information Technology Act, 2000*

In India, Section 79 of the Information IT Act is the law regarding intermediary liability.[23] The law is also known as the *"safe harbour"* provision, as it exempts intermediaries from liability if its function is limited to providing access to communication systems through which third parties make information available. The information is either transmitted through the intermediary or temporarily stored or hosted by the intermediary.[24] If the intermediary did not initiate, select the receiver, select or modify the transmission[25], the intermediary will not be held liable for the third-party information hosted on the platform.[26]

---

[20] Trilegal, *Consumer Protection (E-Commerce) Rules, 2020* (Aug. 5, 2020), https://trilegal.com/wp-content/uploads/2021/11/Consumer-Protection-E-Commerce-Rules-2020-1.pdf (last visited Feb. 1, 2025)

[21] Trademarks Act, § 28(1) (1999).

[22] Trademarks Act,§ 34 (1999).

[23] Information Technology Act, § 79(2000).

[24] Information Technology Act, §79(2)(a) (2000).

[25] Information Technology Act, § 79(2)(b) (2000).

[26] Information Technology Act,§79(1) (2000).

It is the intermediary's responsibility to perform duties under the Act and abide by the guidelines issued by the Central Government.[27] This provision is called the *"safe harbour"* provision because intermediaries are exempted from liability subject to the fulfilment of certain conditions as per Section 79. Furthermore, intermediaries have the responsibility to remove or disable access to any material from a computer resource, which has been used to commit unlawful activity. This must be done without affecting the evidence in any manner.[28] As per Section 2(w) of the IT Act, *online marketplaces* come under the ambit of an *intermediary* as defined under the Act. Along with the Act, the Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules"), which superseded the previous Information Technology (Intermediaries Guidelines) Rules, 2011, ensures that intermediaries by itself and by its users make reasonable efforts to ensure that information shall not *infringe any patent, trademark, copyright or other proprietary rights*.[29]

### *3. The E-commerce Rules, 2020*

The Consumer Protection (E-commerce) Rules, 2020 ("E-commerce Rules") falls under the Consumer Protection Act, 2019. The Rules aim to regulate the transactions that happen with the purchase of goods and services through e-commerce platforms and safeguard the interests of consumers.[30] The Rules are applicable to *"all goods and services bought or sold over digital or electronic network including digital products."*[31] Furthermore, it is applicable to all models of e-commerce,[32] all e-commerce retail[33] and any form of unfair trade practices which happen through e-commerce platforms.[34]

As per Rule 3(b) of the E-commerce Rules, 2020, an *e-commerce entity "is any person who owns, operates or manages digital or electronic facility or platform for electronic commerce, but does not include a seller offering his goods or services for sale on a marketplace e-commerce entity."*[35]

[27] Information Technology Act,§ 79 (2)(c) (2000).
[28] Information Technology Act, § 79(3)(b) (2000)
[29] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3 (1)(b).
[30] The Consumer Protection (E-commerce) Rules, 2020.
[31] The Consumer Protection (E-commerce) Rules, Rule 2(a) (2020).
[32] The Consumer Protection (E-commerce) Rules, Rule 2(b) (2020).
[33] The Consumer Protection (E-commerce) Rules, Rule 2(c) (2020).
[34] The Consumer Protection (E-commerce) Rules, Rule 2(d) (2020).
[35] The Consumer Protection (E-commerce) Rules, Rule 3(b) (2020).

It is important to note that when sellers sell counterfeit products to consumers through e-commerce platforms advertising it as the original, it becomes an unfair trade practice that involves deceiving the consumers. The Consumer Protection Act, 2019 also punishes such false or misleading advertisements.[36]

## V. The Fight Against Counterfeit Goods in the E-Commerce World

With the popularity of E-commerce platforms, it is easier for sellers to distribute fake or counterfeit goods on the platform, as consumers are more likely to be confused between genuine and counterfeit listings, providing them with a low risk of detection. Further, the ease of setting up e-commerce websites and the ease of re-establishing the website using new domain names remains a pertinent problem.[37] Some owners of Trademarks have started to take proactive action against the infringers by way of filing suits for injunctions and damages before the courts.

One of the most common ways of distributing counterfeit goods by the seller is through independent websites, attempting to imitate the owners and deceive the consumers into being perceived as a genuine brand. Usually, independent websites are notoriously known for providing anonymity to the sellers - rendering the consumers as well as the owners helpless and without any relief. The Owners, in an attempt to gain relief, file an '*Ashok Kumar*' order, also known as *John Doe* order, against the infringers. The inception of John Doe orders in India was in 2003, when the Delhi High Court expanded on the concept of 'Anton Pillar' orders to include unnamed defendants or 'John Doe's',[38] in the case of *Taj Television v. Rajan Mandal.*[39]

In the *Taj television* case, the court granted an injunction against six known defendants, 14 unknown defendants, and any other cable operator who may violate the broadcasting rights of the Plaintiffs. The Courts, in most cases, have granted relief by way of an injunction and damages against the Unknown defendant where the infringer has deliberately attempted to infringe the trademark or adopt a deceptively similar mark where there may be a likelihood of confusion

[36] The Consumer Protection Act, § 79 (2019).

[37] OECD, E-Commerce Challenges in Illicit Trade in Fakes: Governance Frameworks and Best Practices (2021), https://www.oecd.org/en/publications/e-commerce-challenges-in-illicit-trade-in-fakes_40522de9-en.html (last visited Jan 14, 2025).

[38] Prashant Reddy, *A Critical Analysis of the Delhi High Court's Approach to Ex-Parte Orders in Copyright and Trade Mark Cases*, 3 MANUPATRA INTELL. PROP. REPORTS 171 (2011).

[39] *Taj Television v. Rajan Mandal 2003 FSR 22.*

amongst the consumers, as per the provisions of Section 29 of the Trademark Act. Nike filed a suit against an Ashok Kumar defendant and obtained an ex-parte decree in their favour, where a permanent injunction was granted to them and pecuniary damages to the tune of Rs. 1 Lakh for the infringement of their trademark.[40] The court, in this case, relied on the Delhi High Court ruling in *the Heels v. Mr. V. K. Abrol and Anr*.,[41] while stating that purely because the defendant is staying away from proceedings, making it impossible to conduct an enquiry into the extent of damages caused by the defendant, the "plaintiff cannot be deprived of the claim for damages",[42] and by virtue of the same, the defendant cannot go scot-free.In one of the recent cases of *Rahul Mishra v John Doe*,[43] the defendant operated the website "www.rahudress.com",[44] which sold counterfeit dresses at significantly lower prices, while also displaying the exact dresses and apparel sold by the Plaintiff, a well-known fashion designer Rahul Mishra, and thereby attempting to deceive the public into believing they are the genuine website. The court granted an injunction in favour of the Plaintiffs, restraining the defendant from using the domain name and dealing, advertising, selling, or manufacturing the Trademark 'RAHUL MISHRA' in any manner on the internet and e-commerce platform, as well as restraining them from using the device and work mark of the Trademark owner. The court, in the case of *New Balance Athletics v Ashok Kumar,* granted relief by the way of an ad-interim injunction in favour of the Plaintiffs, whose counterfeit goods were being sold on the defendants' website "https://www.myshoeshop.in" openly as "first copies" of the original brand, along with other well-known brands like Adidas, Louis Vuitton, Nike, etc. at highly discounted prices.[45]

Ultimately, a John Doe order is a temporary relief given to the proprietors of the trademark, to prevent further infringement of their mark by way of blocking the website, among other reliefs. When there is a standalone website attempting to deceive the public into believing they are selling

[40] *Nike Innovate C.V Vs. Ashok Kumar*, TM No 23/17 (2017).

[41] *The Heels v. Mr. V. K. Abrol and Anr*, CS (OS) No. 1385 of 2005 decided on 29.03.2006.

[42] *Id.*

[43] *Rahul Mishra v. John Doe,* 2024 SCC OnLine Del 9433.

[44] Delhi High Court Issues Dynamic Injunction Against John Doe to Safeguard Fashion Designer Rahul Mishra's Copyright and Trademark - European Commission, https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/delhi-high-court-issues-dynamic-injunction-against-john-doe-safeguard-fashion-designer-rahul-mishras-2025-01-10_en (last visited Jan 25, 2025).

[45] *New Balance Athletics v Ashok Kumar* 2022 SCC OnLine Del 2578.

genuine products, like in the case of *Rahul Mishra*[46] and *Nike*[47,] the court directs the takedown of the whole website, instead of blocking the URL. The main aim of issuing a John Doe order is to identify the defendant and thus, is an ad-interim injunction when the defendants remain unidentified; thereby, it is a temporary order in nature.[48]

## VI. Secondary Liability of E-commerce Platforms

E-commerce marketplaces have provided a platform for counterfeiters to imitate legitimate businesses and prey on innocent consumers.[49] While usual businesses sell their products on these online platforms as first-party vendors, counterfeiters prefer to sell as third-party sellers, which allows them to sell products directly to the consumers. The third-party seller model has exponentially driven up the selection of goods on the e-commerce platforms since their inception.[50] Due to the anonymity of the third-party vendors, it is hard for the Trademark holders to take action against them directly, they choose to take action against the e-commerce platform instead.

### *1. Concept of Secondary liability*

Secondary liability is a matter of concern for various online intermediaries who offer varied services.[51] Secondary liability is the liability of the defendant when the plaintiff's mark is used by a third party.[52] Contributory infringement is when the defendant has played an active role in causing the third party to infringe the plaintiff's trademark or when supplying products to the third party to infringe the plaintiff's trademark.[53] In contributory infringement, the owners of the mark bring a claim on the defendant and not on the infringing third party who is actually responsible for

[46] *supra* note 32.
[47] *supra* note 31.
[48] Lokesh Vyas & Anuj Bajaj, *John Doe Order: A Cogent Jurisprudential Account of Judicial Endeavours*, 3.1 J. Indian L. Stud. 29 (2020).
[49] Ani Khachatryan, *The Digital Dilemma: Counterfeit Culture And Brand Protection Reform In The E-Commerce Era*, 43 Loy. L.A. Ent. L. Rev. 247 (2023).
[50] *Id.*
[51] Graeme B. Dinwoodie, *Secondary Liability for Online Trademark Infringement: The International Landscape*, 37 Colum. J.L. & Arts (2014).
[52] Saunders' and Walliser, *supra* note 305 at 42.
[53] *Inwood Labs. v. Ives Labs.,* 456 U.S. 844, 854–55 (1982).

violating the plaintiff's rights.[54] Vicarious infringement occurs when the relationship between the defendant and the infringing third party is a relationship of agency. Vicarious infringement also occurs when the infringing third party and the defendant exercise control over the means of infringement together.[55]

### *2. Inception of Secondary Liability suits in Trademark*

The first third-party liability suit can be traced back to *Inwood Labs Inc. v. Ives Labs, Inc.,*[56] where the Supreme Court of the United States of America ("SCOTUS") held a pharmaceutical distributor, Inwood Laboratories, contributorily liable for trademark infringement[57] by manufacturing look-alike capsules and for *intentionally inducing* another to infringe a trademark and *knowingly* supplying generic medication to pharmacies mislabelled as 'Cyclospasmol', the patented drug manufactured by Ives Laboratories. The SCOTUS extended the liability of trademark infringement beyond those who directly infringe upon others' trademarks.[58] This judgement set a precedent in providing a favourable ruling in favour of the Luxury brand LVMH, in 2006.[59] In this case LVMH, a luxury goods conglomerate known for manufacturing luxury handbags 'Louis Vuitton', filed a suit and obtained a permanent injunction in their favour against the landlords who permitted the sale of counterfeit goods on their premises, instead of taking action directly against the vendors, thereby tackling the problem of counterfeit goods by implementing the 'deep pockets' theory.[60] The theoretical explanation behind employing the deep pockets theory is that, unlike the tenants, the landlords cannot abandon their property and flee prosecution.[61]

[54] Dinwoodie, *supra* note 42 at 463.
[55] David Berg & Co. v. Gatto Int'l Trading Co., 884 F.2d 306, 311 (7th Cir. 1989).
[56] Khachatryan, *supra* note 340.
[57] Nwajei, *supra* note 295 at 55.
[58] Esther A. Zuccaro, *Gucci v. Alibaba: A Balanced Approach to Secondary Liability for E-Commerce Platforms*, 17 N.C. J.L. & Tech. On. 144 (2016).
[59] Nwajei, *supra* note 295 at 55.
[60] *Id.*
[61] *Id.*

### *3. Position of Secondary Liability of E-commerce Platforms in Foreign jurisdictions*

The first case to ascertain the secondary liability of e-commerce platforms for trademark infringement in the United States is the case of *Tiffany v eBay*[62]. Tiffany is a well-known Luxury Jewellery Company, which found that up to 73% of the sterling jewellery, which was fake, sold on the platform carries the trademark of 'Tiffany & Co.' and filed a suit against eBay for contributory trademark infringement,[63] direct trademark infringement, direct trademark dilution, among other causes of action.[64] Tiffany argued that eBay should be held liable under the second prong of the Inwood test, i.e. by permitting the sale of goods on their platforms *while knowing or having reason to know* that such sellers were infringing Tiffany's Trademark.[65] However, the court, while ruling in favour of eBay, held that although, possessed *general knowledge*, it was insufficient to hold them liable under the Inwood test. The court further stated that a platform must have "*more than a general knowledge or reason to know that its service is being used to sell counterfeit good*s."[66] The court expanded on the Inwood test while stating that eBay must have "*specific knowledge*" of such infringement being undertaken on their platform, however, stated that if platforms are "*wilfully blind*" to the sellers selling counterfeit items, the second prong of the Inwood test would be satisfied, thereby, holding the platform liable for contributory trademark infringement. [67]

In another case in 2011 before the 9th Circuit in the United States, the District Court held a third party liable for contributory Trademark infringement in the case of *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc*.,[68] which solidified the "*specific knowledge*" requirement. Akanoc, in this case, was a web-hosting platform, which leases packages of servers leased to them by "Managed Solutions Group, Inc. (MSG).[69] Louis Vuitton, a luxury conglomerate, noticed multiple websites selling counterfeit goods bearing their trademark which sold the products not directly through the

---

[62] Tiffany Inc. v. eBay Inc., 600 F.3d 93 (2d Cir. 2010).

[63] Nwajei, *supra* note 25 at 37.

[64] Virginia Welch, *Contributory Trademark Infringement: Who Bears the Burden of Policing Online Counterfeit Activity?,* 13 SMU SCI. & TECH. L. REV. 361, 364 (2010).

[65] Zuccaro, *supra* note 349.

[66] Andrew Lehrer, *Tiffany v. eBay: Its Impact and Implications on the Doctrines of Secondary Trademark and Copyright Infringement*, 18 B.U.J. SCI. & TECH. L. 373 (2012).

[67] *Id.* at 31.

[68] Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 591 F. Supp. 2d 1098, 110708 (N.D. Cal. 2008).

[69] Michael Pantalony, *Contributing to Infringement: Intermediary Liability After Tiffany v. Ebay and Louis Vuitton v. Akanoc*, 105 TRADEMARK REP. 709, 713 (2015).

websites, but the transaction could be initiated through email address. Louis Vuitton, upon noticing that these infringing websites are using IP addresses belonging to Akanoc and MSG, the defendants, filed around eighteen Notices of Infringements ("NOIs"), bringing the same to their notice. Even after sending the NOIs, there was a failure of action on the part of the defendants. The District court in this case held that the defendant's web servers had received "*actual knowledge*" that infringing websites were using their services in light of the NOIs served by Louis Vuitton.[70] Further, the court stated that the defendants possessed "*direct control and monitoring of the instrumentality used by the third party to infringe*" [71] and using an analogy similar to the deep pockets theory in the *LVMH case*, stating that websites exist in cyberspace and would not be able to exist without physical roots in the servers and internet services,[72] thereby holding the landlord (web host defendants) liable for the actions of the infringing websites on whose IP addresses the counterfeit goods are sold.

Apart from the principle of secondary liability in the above cases, the court also laid down the Red flag test in the case of *Viacom v. YouTube* under the Digital Millennium Copyright Act to determine whether the defendant has specific and identifiable knowledge or just a general awareness of the infringing activity on its website. The court stated that if an Internet Service Provider (ISP) has the knowledge, by way of notice or "red flag", of the cases of infringement, they must endeavour to remove the infringing material, which reiterates the "actual knowledge" requirement to claim immunity under safe harbour provisions. Failure on the part of the ISP to remove such infringing content places a burden of proof on the copyright owners to establish and identify the infringement.[73] This case demonstrates general knowledge or awareness is not sufficient to place liability on the platforms.

In the United Kingdom, the court in *L'Oréal v eBay*, while deciding whether eBay was entitled to the benefit of Article 14 of the E-commerce directive, held that an intermediary depends on the "active role" they played in the alleged illegal activity, and would lose immunity if it was aware

[70] *Id.*
[71] *Id.* at 714.
[72] *Id.*
[73] *Viacom International v. YouTube Inc.* No. 07 Civ. 2103 (LLS).

of facts or circumstances based on which a diligent economic operator should have realised the unlawful sale on its platform and, in the event of it being so aware, failed to act expeditiously.[74]

The European courts are comparatively stricter with respect to holding e-commerce platforms liable for contributory trademark infringement. In a 2008 ruling, the French court held eBay liable for *knowingly allowing* the sale and auction of counterfeit products listed as "replica Louis Vuitton" and the failure of eBay to take action against repeated complaints regarding the infringers.[75] The court further agreed with Louis Vuitton while stating that the consumers would be confused between genuine and replica goods and that the non-approved distribution channel hurt their business, thereby ordering eBay to pay damages of 38.5 million Euros.[76] Under the EU law, failing to comply with notice and takedown does not automatically amount to liability. However, it results in no immunity provided under the Safe Harbour provision to the intermediary. This highlights a stark contrast with the US jurisdiction, as in the *Tiffany* case continuing to supply services after notice will trigger liability. On the other hand, liability in Europe will only arise if the standard for secondary liability is also met under the applicable national law. [77]

### *4. Indian Position of Secondary Liability of E-commerce Platforms*

The Indian Courts adopt a middle ground, incorporating principles from both jurisdictions while holding e-commerce platforms liable for contributory trademark infringement. One of the first cases which discussed the liability of an internet platform for intellectual property violation is *Myspace Inc v Supercassetes.*[78] Myspace is an intermediary web platform where users can access music works, entertainment videos, images, cinematograph works, etc., for free. It also acts as a platform where users can upload content without registration, but adhering to their Terms of Use Agreement and Privacy Policy. The business model employed by Myspace is that they can obtain a limited license from the users to use, modify, delete from, add to, publicly perform, publicly display, reproduce and display the User Generated Content (UGC). Supercassetes is one of India's

[74] Dinwoodie, *supra* note 32 at 488.

[75] Mikouya Sargizian, *Counterfeit Chic: Society's Friend or Foe?,* 17 INTELL.PROP. L. BULL. 111, 123 (2013).

[76] Reuters, LVMH and eBay settle litigation over fake goods Reuters (2014), https://www.reuters.com/article/technology/lvmh-and-ebay-settle-litigation-over-fake-goods-idUSKBN0FM15G/ (last visited Jan 30, 2025).

[77] Dinwoodie, *supra* note 32 at 489.

[78] *Myspace Inc. v. Super Cassettes Industries Ltd*. 2016 SCC OnLine Del 6382.

largest music companies, holding copyright and having business of producing and acquiring a large number of musical works, films, songs, etc. Supercassetes alleged that Myspace facilitated and encouraged the uploading of infringing content on their platform and that, further, the advertisements alongside the infringed content benefitted the platform at their cost and caused significant financial and reputational harm. The court, in this case, held that Myspace cannot be held liable for secondary infringement when infringing videos do end up on their platform, despite the safeguards in place and notice and takedown regime, while making a reference to the "*red flag"* test in the *Viacom case*. However, one of the first cases that dealt with the liability of an e-commerce platform for contributory trademark infringement is the case of *Cartier International A.G. v. Gaurav Bhatia,*[79] decided by the Delhi High Court in January 2016. Cartier, along with other luxury brands, filed a suit against the defendants who operated the e-commerce platform www.digaaz.com, which sold luxury counterfeit products bearing the trademark of the plaintiffs at highly discounted rates. The court held the defendants liable for trademark infringement while stating that the defendant had sourced and directly sold counterfeit products to the consumers, had a direct role in selling the counterfeit products and a deliberate and wilful infringement of the plaintiff's brands, thereby making them liable for passing off under Section 135 of the Trademarks Act,[80] apart from their criminal liability under Section 420 of IPC and Section 66A of the IT Act, and thereby granted a permanent injunction and demanded the defendants to pay punitive damages amounting to Rs. 1 crore.

However, it is difficult to determine the liability of big e-commerce platforms, like Amazon, Flipkart, etc., which act as an intermediary platform for the sellers to sell goods to the consumers, thereby raising the contention as to the level of "knowledge" these intermediaries need to possess to be held liable.

### *5. Requirement of "Knowledge"*

The extent of what constitutes knowledge to claim immunity under the safe harbour provision of Section 79 of the IT Act was first laid out in the case of *Shreya Singhal v. Union of India.*[81] The

[79] *Cartier International A.G. v. Gaurav Bhatia* 2016 SCC OnLine Del 8.
[80] *supra* note 22, § 135.
[81] *Shreya Singhal v. Union of India* (2015) 5 SCC 1.

court, while deciding the constitutional validity of Section 66A and 69A of the IT Act and the liability of intermediaries to monitor UGC published on its website, held that "*Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails.*"[82] However, the judgement was in the context of intermediary liabilities like Facebook, Google, etc., and the subject matter of the dispute was not an infringement of intellectual property.

Post the landmark judgement in *Shreya Singhal*, the division bench of the High Court in the *Myspace* case affirmed the ratio of the former stating that while Myspace, albeit, cannot be held liable for secondary infringement, stated an intermediary could only be held liable upon receiving knowledge from the content owner and only then would constitute "*actual knowledge*" under Section 79(3) of the IT Act. The court, while distinguishing between actual and constructive knowledge, stated that to constitute actual knowledge, Myspace must have information of actual knowledge of the users uploading songs on the platform, and to constitute constructive knowledge analysed the international position on the safe harbour provision as well as the Indian stance under Section 79 of the IT Act, which applies when –

(i) the intermediary establishes, publicizes and implements a "Notice and Take Down" regime for removing content once a copyright owner sends a notice to the intermediary;
(ii) there exists a system for identifying repeat offenders and removing them from the system and
(iii) to make provisions for technical protection measures.[83]

The court, in the case of *Kent Systems Ltd. v. Amit Kotak,*[84] held that an intermediary is required to satisfy that any posting, or activity in general, would not result in an infringement of intellectual property, and any person aggrieved by way of infringed intellectual property is required to inform the intermediary. Thereby, general awareness is insufficient to hold an intermediary liable for

[82] *Id* at 122.
[83] *supra* note 29.
[84] *Kent Systems Ltd. v. Amit Kotak* (2017) 69 PTC 551 (Del).

infringement. In the case of *Christian Louboutin SAS v Nakul Bajaj,*[85] where the court determined the liability of an e-commerce platform, defendant *Darveys.com*, for the sale of counterfeit goods and infringing of marks by use of meta-tags, stated that in light of the platform being a members-only platform, had a direct role in identifying and enabling the sellers to sell counterfeit goods and thereby cannot claim immunity under Section 79 of the IT Act. Further, the court stated that the IT Rules, 2011 are *mere guidelines*[86] and cannot substitute the requirements laid down under Section 79 of the IT Act or any other relevant law. The court held that mere compliance with the guidelines "*would not offer protection to any 'intermediary' that have 'conspired', 'abetted' or 'aided' or 'induced the commission' of an unlawful act.*"[87] The court stated that Section 81 of the IT Act has an overriding effect over Section 79 in case of inconsistency with any act in force, which implies that the IT Act will not grant immunity to any intermediary responsible for a violation under the Trademark Act.

Further, in the *Christian Louboutin* case, the court, while relying on the precedent of *Kapil Wadhwa v. Samsung Electronics Co. Ltd.,*[88] held that the use of meta-tags[89] by the platforms is illegal, as it allows the platform to free-ride off the goodwill of the plaintiff proprietor, and the unauthorised use of the Plaintiffs mark amounts to falsification of mark.

In another case before the High Court of Delhi, Puma filed a suit for contributory trademark infringement against the e-commerce platform Indiamart Intermesh Ltd.(IIL), claiming that the drop-down option provided to the sellers to choose a brand, without prior verification, they represent amounts to aiding, abetting and facilitating such infringement and passing off.[90] The court, in this case, while relying on and analysing the judgement of *Google LLC v DRS Logistics*, held that IIL can be held liable on the principle that an intermediary can be held liable for the infringing content if such infringing work would "be detrimental to the distinctive character and

[85] *Christian Louboutin SAS v Nakul Bajaj* 2018 SCC OnLine Del 12215.
[86] *Id* at 33.
[87] *Id.*
[88] *Kapil Wadhwa v. Samsung Electronics Co. Ltd* (2012) 194 DLT 23.
[89] Meta tags are HTML tags used to provide additional information about a page to search engines and other clients. See, Meta Tags and Attributes that Google Supports | Google Search Central | Documentation | Google for Developers, https://developers.google.com/search/docs/crawling-indexing/special-tags (last visited Jan 31, 2025).
[90] *Puma SE v. Indiamart Intermesh Ltd.*, 2024 SCC OnLine Del 17.

repute of the registered trade mark",[91] and thereby action for infringement would lie under Section 29 of the Trademark Act. In this case, IIL was held liable in light of Section 79 and Rule 3(1)(b)(iv) of the IT Rules, while reiterating that an intermediary should strive to make efforts to ensure the removal of any infringing content from their platform. Further, IIL is not a mere spectator and has an active role in controlling the website, especially in light of pocketing a certain sum of proceeds from sales on the platform.

The court in the case of *Akash Aggarwal v. Flipkart Internet Private Limited and Ors*.[92] Held an intermediary platform of promoting and enabling 'latching on' of third-party sellers to sell counterfeit goods is in while stating that allowing sellers to list products to compete with the original proprietor and offer counterfeit goods at competitive prices while displaying caption "Grow your business by 3x" allows the third party to latch on and ride off the Plaintiffs mark amounts to traditional passing off, and thereby ordered the Defendant to disable the option permitting latching off.

The courts ensured that sanitary hygiene products were not counterfeited as they could have severe repercussions on the health of the female population in the country, in the case of *Sirona Hygiene Private Limited v. Parulben Navnath Chothani Trading As Shiv Enterprise & Ors*.[93] The court stated due to rise in e-commerce, knock-off and counterfeit products of the plaintiff's product under the mark "SIRONA" being sold on e-commerce platforms like Amazon, Meesho, Snapdeal, etc., under a deceptively similar mark "SIROMA" could cause irreparable injury and likelihood of confusion amongst the public, and thereby granted an injunction in favour of the plaintiff, restricting the use, distribution, sale of their products as well as directing the platforms to immediately takedown such infringing content on their platforms within 36 hours of the order.

It can be deduced that the liability of an e-commerce platform depends on its role in taking down infringing sale listings and the level of knowledge and awareness it possesses. For instance, in the *Kent RO* and the *Sirona Hygiene* case, the court established that it is the duty of the owners to inform the platform of such infringing content and that general awareness is not adequate to hold

[91] *Google LLC v DRS Logistics* (2023) 4 HCC (Del) 515.
[92] *Akash Aggarwal v. Flipkart Internet Private Limited and Ors,* CS (COMM) 492/2022.
[93] *Sirona Hygiene Private Limited v. Parulben Navnath Chothani Trading As Shiv Enterprise & Ors.* CS(COMM) 260/2022.

such an intermediary liable while adopting a similar principle laid down in the *red flag test*. On the other hand, in the Puma and Akash Aggrwal case, by the sole reason of their business model, i.e. the "drop-down" and the "latching off" options offered to sellers without verification requirements, respectively, imposed liability on the platforms by virtue of the models enabling counterfeit sellers to deceive consumers.

## VII. Recommendations

In recent times with the rise in Artificial Intelligence (AI) technologies, there are various benefits and challenges associated with intellectual property violations through e-commerce platforms.[94] AI can definitely play a vital role in detecting potential counterfeit goods through machine learning and advanced algorithms, but the challenges would be accuracy in capturing subtle infringements and the possibility of false positives or hallucinations.[95] Due to the development of technology like Virtual Reality (VR) and Augmented Reality (AR), there is a possibility for counterfeiting of goods through such technologies. Therefore, it is necessary to address the challenges that may arise through these technologies by allowing registration of physical trademark registrations to also protect the virtual trademarks of a particular brand. This would grant protection to all brands and not merely luxury brands, as luxury brands would be able to seek protection in these new technologies easily due to their well-known status.

The problem of counterfeit goods can be combated using blockchain technology. Some of the key features of this technology are *"improved traceability and end-to-end tracking."* This technology consists of an immutable ledger, which records the transaction and has the ability to track the movement of a product. [96] Blockchain technology is secure and can help identify the *"proof of origin"* of products. Due to this reason, it is specifically useful in understanding the origin of counterfeit products.[97] Another important benefit of blockchain technology is that it is easily traceable and transparent, which helps in promoting authenticity. It also has unmodifiable

[94] Anna Pokrovskaya, *Protection of Trademark Rights on E-Commerce Platforms: An Updated Outlook*, 1 J. COMPR. BUS. ADM. RES. 65 (2024).
[95] *Id.*
[96] Use of blockchain to protect against counterfeiting - European Commission, https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/use-blockchain-protect-against-counterfeiting-2022-09-16_en (last visited Jan 14, 2025).
[97] *Id.*

properties and can help in recording transactions efficiently.[98] The tracking available through blockchain technology can be useful for both businesses and consumers as it can be easily integrated into businesses that operate through e-commerce platforms.[99]

## VIII. Conclusion

The rise of counterfeit goods online has posed significant challenges to the trademark proprietors. The only remedy left for the owners to prevent further damage to their rights is to indulge in expensive and time-consuming litigation. There has been a massive change in the scientific and technological developments to the trademark, whereas the Trademark Act, 1999, remains unchanged. A key development concerning secondary liability leaves a legal vacuum in the statute, forcing the courts to resort to other statutes to hold these online intermediaries liable. Platforms are being held liable for contributory trademark infringement, it is in light of the provisions under the E-commerce guidelines and the IT Act. The court, in the *Myspace case*, highlighted the importance, with the rise in technology and the rise of the internet, to harmoniously interpret the provisions of Intellectual Property laws, in this case, the TM Act, with the provisions of the IT Act. The Indian Courts embrace a middle-ground position, adopting their European counterpart's strict enforcement of Trademark owners' rights, imposing penalties, and holding the infringers liable for trademark Infringement by deceiving the public into believing their websites are genuine brands, and adopting the American counter-parts stance of the requirement of "*actual"* knowledge and not *general knowledge* or *awareness* to hold an intermediary liable. If a platform qualifies as an intermediary under Section 79 of the IT Act, it can only claim immunity under the safe harbour principle under the Act if it complies with all the necessary requirements under the Intermediary guidelines and the E-commerce rules. The new IT rules of 2021, which supersedes the previous 2011 rules places an obligation on the intermediary to make reasonable efforts to ensure by itself and cause users to ensure no intellectual property is infringed by the sale of any goods or services.

The Indian courts are concerned with the rights of the brand owners and ensure that their rights are enforced; however, if the doctrine of secondary liability is stretched, it may result in dire

[98] Anthony et al., *Developing an Anti-Counterfeit System Using Blockchain Technology*, 216 Procedia Comput. Sci. 86, 87 (2023),
[99] Use of blockchain to protect against counterfeiting - European Commission, *supra* note 299.

consequences for the e-commerce platforms. To hold a platform liable for secondary or contributory infringement, a platform must play an active role in c*onspiring, abetting, aiding or inducing trademark infringement*, and must receive *actual knowledge* of infringement, as laid down in the *Shreya Singhal* case.

There is no strait-jacket formula to protect the rights of trademark holders in the digital realm, as the internet makes it easy for infringers to carry on their business in a different domain name. While holding an e-commerce platform liable is another means to claim relief by way of imposing secondary liability, it is impractical to hold an intermediary liable for any and every infringing content taking place on their platform, as in the case of large platforms with millions of sellers, it is hard to keep check of every product being sold on their platform. It is important that the intermediaries, upon receiving knowledge of the infringing content, take down the same within 36 hours in light of the IT rules to claim immunity under Section 79. While the rights of the owners in some cases are rejected in light of the safe harbour provision, the court ensures that the proprietor's rights are enforced by ensuring any infringing content is taken down from the intermediary' platform, and failure to do the same can result in secondary liability of the e-commerce platform. Another way to protect the rights of trademark holders in the digital era is to employ blockchain technology, which can help in the identification of the source of products and is known for its traceability and transparency, which can help counter the problems faced with counterfeit goods sold on the internet and making it easy for the e-commerce platforms to incorporate it in their businesses.

In conclusion, the role of e-commerce in facilitating counterfeit goods has presented a plethora of legal issues. While the Indian courts have, by relying on surrounding legislations such as the IT Act and the Consumer Protection Act, aimed to protect the rights of the Brand owners effectively, the vacuum in the TM Act fails to protect and enforce the rights of the proprietors. The incorporation of such technological tools and the creation of a uniform guideline for e-commerce platforms to adhere to remove counterfeit goods can address the vacuum in the TM Act while also balancing the needs of the Trademark holders, thereby safeguarding brand reputation while also fostering innovation in online marketplaces.

[This page was left blank intentionally]

# THE UNSUNG COGNIZANCE: NAVIGATING THE INDIAN LEGAL LANDSCAPE AND PROCEDURAL CONUNDRUMS OF NON – CONVENTIONAL TRADEMARKS

*[1]

**Abstract**

*The registration of a non – conventional trademark essentially originates as a critical domain of interest within the entire regime of regulatory frameworks concerning the intellectual property rights (IPR), categorically focussed on Trademarks. Non – conventional trademarks, as a basic consideration, includes a set of certain categories of marks including the gustatory(taste), olfactory (scent) and sound marks, essentially extending elaborative considerations to further examine interpret the intricate registration procedures inclusive of this class of marks which essentially forms the main objective context of the current research paper.. This research paper begins the discussion by facilitating a meticulous background and outlook of the significance carried by non – conventional trademarks in the contemporary legal prospect and the potential possessed by each category of such marks to foster adequate brand differentiation to emerge as unique identifier in this regard. Moving further, the paper attempts to examine the current position of Trade Marks Act, 1999 from the standpoint of the trademarks being discussed in the present context and highlighting the key challenges such as the requirements of distinctive character, graphical representation, etc., thereby creating potential research gaps in realising the effective process of registering these non – conventional trademarks. Moving further, the paper aims to address these challenges from the lens of the existing legal provisions, by suggesting a structured set of actionable recommendations aimed at adopting certain initiatives on the global scale to foster a diverse view of combating the procedural conundrums and as well, appropriate directions for reforms to be made in the trademark legislations is also duly mentioned in the paper.*

**KEYWORDS** – Non – conventional trademarks, Taste marks, Olfactory marks, Trademarks Act, Registration.

[1] Amuktha Malyada Gudla, 4th year BB.A.LL.B, School of Law, GITAM & Lammata Ashish Kumar, Assistant Professor of Law, School of Law, GITAM.

## I. Introduction

The developments traversing the much evolving pathway of the intellectual property regime has resulted in the rising importance of trademarks in India and possessing a global relevance thereof. In simple terms, a trademark can be understood as any such unique parameter or 'mark'[2] that identifies and distinguishes the source of goods or services from those of others in terms of trade related prospects to fulfil the requirements of distinctive branding and the consumer recognition in the increasingly competitive market conditions. Over the past few decades, there has been a growing preference for Non – Conventional Trademarks which essentially encompass a range of identifiers including smell marks, sound marks, taste marks, colour marks and the moving images/ holograms/ gestures and three – dimensional trademarks. Despite the increasing significance, the registration procedures of non – conventional trademarks often revolves around innumerable complexities on account of the rigid rules of its implementation, specifically in the Indian legal landscape.

Considering the historical perspectives, the conception of trademarks can be traced back to the era of industrial revolution thereby enabling large scale production of goods and the considerable shift in the approach of manufacturers towards protecting their brand identity and tilting the focus to achieve the aimed consumer recognition for their brands. This has eventually directed to the emergence of notable legal developments, with respect to, trademarks thereby subjected to various amendments and repeals. The current legal framework governing trademarks in India is the Trade Marks Act, 1999 that was adopted by the Nation after joining as a party to the Agreement on Trade- Related Aspects of Intellectual Property Rights (TRIPS) with an aim to formulate procedures in accordance with the concerned agreement on a global scale to be executed in tandem with the Indian Trade Marks Rules of 2017.

The legal definition of 'Trademark'[3] under the Act of 1999, specifically mentions three essentials of trademarks, namely, existence of a 'mark', the very mark capable of graphical representation and the distinguishing factor of goods or services with those of others. In this regard, the stringent statutory requirements, particularly concerning 'graphical representation' and 'distinctiveness' pose certain serious barriers for facilitating a smooth registration process of Non – Conventional

[2] The Trademarks Act, 1999 (Act 47 of 1999), s. 2 (1) (m).
[3]The Trademarks Act, 1999 (Act 47 of 1999), s. 2 (1) (zb).

trademarks in the Indian context, especially those marks that do not easily conform to conventional representations. As stated supra, these marks span across various categories, the renowned examples of the same on a global note would be the Dutch company's *Tennis balls with the scent of newly mown grass* for **smell marks**, Netflix's *'Tadum'* sound for the **sound marks** category, the colour *'Light blue'* trademarked by Tiffany for their jewellery packaging as part of **colour trademark,** the 3D registration of *Coco-Cola bottle* in Japan is a popular example for the **three-dimensional trademarks,** further marks includes **motion marks,** for which *Nokia's 'CONNECTING HANDS' is the first motion mark in India* (initially registered as a device mark – until *Toshiba Corporation* secured a registration for motion mark in 2019)and finally, **shape marks,** which operate on the criterion that the shape of the product should not result from the nature of the product itself, on this note the familiar examples would be that of *Manolo Blahnik shoe,* and *the shape of Toblerone chocolate*, are few relevant instances of marks in the non – conventional category.[4] However certain categories like that of taste marks, due to its inflexible hindrances with graphical representation doesn't record any successful registrations in this respect. But, an application that was made to register the *orange flavour by* ***N.V. Organon, In re****,* for its anti- depressant drug, remained due on the aspect of functionality parameter that is discussed in detail in the further sections of the paper. In this case, it was argued on the aspect as to how can a consumer associate an orange flavour with a medical drug. Most importantly, in this process, a crucial observation, with respect to taste or gustatory marks was made on the question that *How can taste function as a trademark if the consumers have to purchase the product before accessing the flavour?* This condition would pose several reasons for making it as a poor indicator to the source product.

By formulating a comparative analysis of the global cases from the previously mentioned examples, it becomes clear that a number of jurisdictions, including the United States and the European Union, have opted more flexible stance to non- conventional trademarks and thus experience easier registration processes. Unfortunately, in India because of the previously stated circumstances that essentially causes the issues raised above, the limited scope of protection afforded to brand owners in India frequently steers the brand image and consumer confidence down the road of deterrence.

[4] V.K Ahuja, *Law Relating to Intellectual Property Rights* (Lexis Nexis, 3rd Student edn, Reprint 2022).

Thus, the special focus of this paper is on examining the specific challenges that non-conventional trademarks in India are facing with regard to the procedural conundrums associated to the registration procedures and the related components thereof. In order to highlight the need for an inclusive trademark framework that complies with the evolving global standards, the effectiveness of the current Indian legal provisions regarding registration will be analysed in terms of the objective of offering some reasonable suggestions for reform in this area towards the conclusion of the paper.

## II. Understanding the Legal Framework of Non – Conventional Trademarks

The legislations on trademarks and the statutory equivalents thereof, as stated earlier primarily aim to streamline and regulate the national as well the global procedures with respect to the procedure entailed to the registration aspects so far as trademarks are concerned. However, this is not the case in India, though, where the procedural complexity of trademark registration differs from that of other major jurisdictions worldwide.

This section of the paper addresses the legal framework related to the topic from three distinct angles, providing a thorough overview. Initially, the historical context and development of trademark laws generally; followed by the viewpoints from other countries; and lastly, the actual focus of the entire study, which is the Indian legal perspective on trademark registration.

This section of the paper essentially steers the route for further analysis of the concept as the objective is set forth to cover the intricate details of non- conventional trademarks and the procedural aspects of its registration.

### *1. Evolution of Trademarks Laws –*

#### *a. Trade Marks – Historical Context:*

The historical context of 'trademarks', in the first instance, traces back to the barbarian times where illiteracy among the people gave rise to logical method of communication. It was believed that the early marks of identification were made with respect to animals to prevent any sort of confusion and to act as a distinguishing factor. Further developments in trade and commerce has refined and expanded the scope of these very identification marks from the lens of trade related aspects, the best examples in this regard would be *Roman Times* appeared on the vessels to indicate upon the origin and unique identification of the actual owner thereto. Around the 10$^{th}$ century, in the course

of developments in merchant trade, these very marks were referred to as 'Proprietary mark' or 'Merchant mark' and have become the ground to prove 'ownership rights' of goods. The Industrial Revolution, specifically, has enhanced the use and vitality associated with the concept of trademarks as the disintegration of guild system of trade occurred leading to growing participation in free business, thereby laying the foundational stone for the touch of rules and procedures as emphasis was laid on the establishment of civil protection against those who replicated the mark of another.

## *2. Understanding the Evolution:*

### *a. International Perspective – The Foundational Stone:*

History has always honoured the case ***Southern* v. *How, 1617***[5]*,* for being the first reported trademark casein the Anglo – American Law, however it is important to understand that this case doesn't specifically relate to trademark laws but dealt with the aspect of counterfeit of jewels . This case, also emphasizes upon the importance of judicial decision and the revolutions created as a result of their implementation, the reason being, the connection of this case with that of trademark laws is established on the basis of the dictum of Judge Dodderidge, wherein the Honourable Judge has made a brief yet an intellectually relevant reference to an earlier, unnamed and unreported case that involves a suit brought against a cloth maker who used the mark of another cloth maker. This very lawsuit quoted in the case of 1618 as stated above is published as the *'Sandforth Case'*[6]. This casehas established the idea that 'nobody' has any right to neither represent/ pass-off their goods as the goods of 'somebody' else.

In this regard, it is absolutely crucial to note that, the most hostile treatment of the case belongs from Frank Schechter's book "*The Historical Foundations of the Law Relating to Trade-Marks"*[7], this commentary remains as the most reliable source on the subject for the firm stance and stand opted by the author throughout the process of justifying his disagreement with the aspect of

[5] Popham's Reports 143 (1618), 79 Eng. Rep. 1243 (K.B. 1907); J. Bridgeman's Reports 125 (1659), 123 Eng. Rep. 1248 (K.B. 1912); Cro. Jac. 468 (1659), 79 Eng. Rep. 400 (K.B. 1907); 2 Rolle's Reports 5 (1676), 81 Eng. Rep. 621 (K.B. 1908); 2 Rolle's Reports 26 (1676), 81 Eng. Rep. 635 (K.B. 1908).**[Sic]**

[6] 79 Eng. Rep. at 1244.

[7] Frank I. Schechter, *The Historical Foundations Of The Law Relating To Trade-Marks* 123 (1925).

relevancy of the suit with the trademark law. Schechter, in this book devoted seven crucial pages to discredit the factor of calling ***Southern v. How***, as the most reliable foundation in Anglo – American Trademark Law[8]. The author places his entire focus on highlighting that the '**irrelevant dictum**' by a reminiscent judge is the sole contribution for the by far expressed denial of claim. [9] The case study discussed above is, however opined by certain clan of trademark scholars as the most significant value in establishing the earliest common law of trademarks and the unfair competition. [10]

On the footprints of this foundational instance, firstly considering the international perspective of legislative evolution in this regard, the need for a statutory resource or law for the registration of trademark and the protection against infringement if any was recognised with the aim of giving an expansive scope for the very first statutory enactment in Britain the year 1875. This statute provided for a formal registration of trademark based on the criterion whether a trademark acted as a distinguishing parameter for the goods of the trader or not, as a result of which, 'Registration' was considered the *prima facie evidence*[11] of ownership of trademark. In due course, the Trademark Act was repealed and replaced by the Patents, Designs and Trademark Act, 1883, wherein emphasis was extended even to the aspects pertaining to patents and designs with the facility to register certain 'fancy words not in common use' and 'brand names and dynamics' as new marks for the first time. However, eventually this Act too underwent certain repeals which lead to its substitution by the Trademarks Act, 1905 having its next re – enactment as The Trademarks Act, 1938.[12]

---

[8] *Id*. at 9-12, 123-26. Other commentators have agreed with this analysis. See DUNCAN MACKENZIE KERLY, *KERLY'S LAW OF TRADE MARKS AND TRADE NAMES* 2 (7th ed. 1951); Benjamin G. Paster, *Trademark's—Their Early History*, 59 TRADEMARK REP. 551, 562-63 (1969) (closely following Schechter's analysis of the case); Edward S. Rogers, *Some Historical Matter Concerning Trade-Marks*, 9 MICH. L.R. 29 (1910), re printed in 62 TRADEMARK REP. 239, 251 n.30 (1972).**[Sic]**.

[9] Keith M. Stolte, *How Early Did Anglo-American Trademark Law Begin? An Answer to Schechter's Conundrum VIII Book II* Fordham Intellectual Property, Media and Entertainment Law Fordham Intellectual Property, Media and Entertainment Law Journal (Article 6) 18 (1997).

[10] *Id*. at 9.

[11] *History and Evolution of the Trademark System (2011)*, https://www.bananaip.com/history-and-evolution-of-trademark/#:~:text=Evolution%20Of%20Trademark%20Law&text=Before%20the%20enactment%20of%20a,Britain%20in%20the%20year%201875.

[12] *Id*. at 11.

Considering the prospects of Non – Conventional Trademarks, the International influence and the TRIPS Compliance could be a major source of reference in this regard as the TRIPS agreement, essentially encourages the member countries to protect non – traditional trademarks and is one of the initial binding sources that acknowledges the importance of such marks and has laid an open platform for its signatories and countries worldwide to adopt such measures applicable in their legal framework for facilitating the registration. Subsequent to this, certain jurisdictions like the European Union (EU) and the United States (US) formulated a more liberal approach to registration while India yet remains to lag behind in terms of updating its jurisdictions, which is discussed in the section vide infra.

b. *Indian Perspective – The Offshoot Implementation:*

In view of the origin of trademarks in the international perspective discussed above, the wide scope of trademark law and regulation poses clarity of thought in this regard. However, as a known fact, Non – Conventional Trademarks have witnessed a considerable spike in importance in terms of the complexities of representation entailed therewith. The changing market dynamics influenced by potential international agreements marks the era of evolution of non – conventional trademarks in India reflecting a broader trend in the Intellectual Property law regime.

In this regard, it is significant to note the historical roots of the trademark concept in the Indian pretext with the vibrant cultural evidence of artisans making their goods as far back as three thousand years ago. Despite the prevalence of the interweaving connect with the rooting parameters, the contemporary state of the significant legislation yet ponders upon a secured position for the procedural footprints of the non-conventional trademark registrations. The first statutory source being The Trademarks Act, 1940 followed by the Trade and Merchandise Marks Act of 1958 which though provided for a structured approach to trademark registration, but doesn't clearly delve into the procedural implications with that of Non-conventional trademarks. Furthermore, the current legislation, namely, the Trademarks Act of 1999 has modernized the existing framework for a much effective procedural experience but does not explicitly address the nuance of the Non – conventional version of trademarks.

Thus, it is clear that the existing research gap in this criterion of non – conventional trademarks is the lack ofan appropriate procedure for representation accompanied with the complex structure of its implications. These gaps are further explored in the following segments of the paper.[13]

## III. Registration of Non – Conventional Trademarks: Challenges and Potential Concerns in India:

The registration of non – conventional trademarks especially in the pretext of the Indian Legal framework poses several procedural complications imposing a critical influence on both legal and implicative challenges. In the era of increased business potential across multiple fields with proactive innovation at each step, it becomes absolutely vital to understand the challenges confronted by concerned sector and the need for a structure procedure to facilitate effective intellectual property protection. This section of the paper discusses about the registration conundrums of non – conventional trademarks aligning with the identified gaps of research. [14]

### *1. Graphical Representation : Sine qua non of Trademark Registration –*

The requirement to graphically represent the trademark is indeed the first and a foremost challenge in the registration of non – conventional trademarks in India remains to be a stringent challenge in the registration process concerned further complicated with the statutory mandate imposed by the Trademarks Act, 1999. Though this ensures meticulous filtration of productive trademarks, it poses hurdles for marks such as sounds, scents and tastes.

The complexity extends to two divergent paths of understanding, namely, Digital Representations and Complexity of Representation, while the former emphasises upon the ambiguity in terms of the implementation and the latter parameter holds paramount hindrance for it necessitates the depiction of the mark through traditional visual means which is quite cumbersome so far as the non – conventional trademarks are concerned.[15]

---

[13]Rachna R. Kurup & Nimita Aksa Pradeep, *NON-CONVENTIONAL TRADEMARKS IN INDIA: THE WHAT, THE WHY AND THE HOW*, E- Journal of Academic Innovation and Research in Intellectual Property Assets (E-JAIRIPA) Vol. 1 (01), Dec 2020, pp. 131-148 2.

[14] Dr. Reetika, *Issues and Challenges Relating To Non-Conventional Trademarks*, International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471, Volume 7 Issue 2, February-2018, Impact Factor: 3.578.

[15]Rumpi Ghosh Alam & Dr. Shampa I Dev, Exploring Non-Conventional Trademarks: Challenges, Registrability, and Legal Implication, ISSN: 2582-8878, PIF: 6.60.

***2. Distinctive Criteria –***

'Distinctiveness' continues to be a critical hurdle in its position as a mandatory requirement so far as the non – conventional trademark is concerned as they cannot serves a functional purpose herein concerned.

This factor is often understood under two broad parameters namely the 'Acquired Distinctiveness' and 'Consumer Perception' which leads the way to inconsistent outcomes during the registration process. The most cumbersome aspect associated with this factor is the complexities in demonstrating the recognition, where the onus lies on the applicant to prove that their non – conventional trademark carries a distinctive nature. Various external, yet relevant factors aid this process, including consumer surveys, sustainable evidence of use and market research.

***3. The Functionality Doctrine – On the Verge of Clarity –***

This doctrine necessarily creates a critical burden for those marks possessing a 'functional' purpose with the aim of preventing the monopolization of any critical product features with that of the concerned statutory objective. Further reliance is steered towards the legal precedents in terms of the uncertainty faced by the applicant at the registration of the non – conventional trademarks.

In view of the potential challenges stated supra the root cause for the continuous increase of the intensity if these hurdles remains in the 'LACK OF COMPREHENSIVE GUIDELINES' and the vague regulations further complicates the scenario by not only inadequate address of various trademark types but imposes great deal of confusion among the concerned parties involved in the aspects thereof.

## IV. Comparative Analysis: Approaches and Procedures of Registration in other major jurisdictions globally with that of the Indian Legal Scenario

This segment of the paper essentially deals with the procedures adopted and followed by the major jurisdictions globally to formulate a comparative analysis that is depicted in the following tabular

form based on the success rates in each country on this aspect to determine the stand of India in terms of Non – Conventional trademarks. [16]

| **Type of Non – Conventional Trademark** | **European Union (EU) Success Rate (percentage %)** | **United States (US) Success Rate (percentage %)** | **India Success Rate (percentage %)[17]** |
|---|---|---|---|
| SOUNDS MARKS | 35% | 30% | 15 % |
| COLOUR MARKS | 45% | 40% | 20% |
| OLFACTORY MARKS | 30% | 25% | 25% |

## V. Recent Trends and Case Study Analysis

This segment of the research paper, essentially deals with certain existing case studies and the analysis of recent trends with due regard to the non – conventional category of trademarks from the context of the associated registration process.

### *1. Case Study Analysis -*

The case of ***Yahoo! Inc & Ors. vs. Akash Arora & Anr. (1999),*** although doesn't relate to non – conventional trademarks directly, yet sets the base for the recognition of the "well – known" trademarks in India which lays the essential foundation for further analyses and interpretation with respect to the protection of non – conventional trademark and their registration process which in way would contribute to soothe the intricacies implied thereof.[18] The facts of this case revolves

[16]Bisman Kaur, *India: A statistical analysis of trends in IP rights*, https://www.managingip.com/article/2bsn506g6k74w5g8askcg/expert-analysis/local-insights/india-a-statistical-analysis-of-trends-in-ip-rights.

[17] Trademark Office Reports and Legal Analyses.

[18]Khurana and Khurana, *The Rise of Non – Conventional Trademarks in India: Legal Framework, Challenges, And Future Prospects,* (August 19, 2024), https://www.mondaq.com/india/trademark/1507624/the-rise-of-non-conventional-trademarks-in-india-legal-framework-challenges-and-future-prospects.

around the background where, the plaintiff, Yahoo Inc., had established a significant outline presence with its domain name "yahoo.com", in this regard the plaintiff claimed that the defendant, in this case, Akash Arora, had registered a similar domain name, "yahooindia.com" to provide internet services, which evidently and in all aspects imitates the Yahoo brand.

This case, receives a significant standpoint from the outlook of the defences put forward by the defendant to the case, who crucially argue that, there was no intention to infringe on Yahoo's trademark and argued that the alleged similarities were not substantial enough to constitute an infringement of trademark. Further the defendants claimed that the word "Yahoo" is a common dictionary word and thus lacked a distinctive character of its own.

However, the Honourable High Court of Delhi, in this case, ruled in favour of Yahoo Inc, thereby issuing an interim injunction against Akash Arora, by basing the rationale on certain important grounds that include, cybersquatting, protection of domain names primarily on the basis that adequate protection shall be provided for well – known trademarks, in the current context, Yahoo Inc, and thus the Court ordered Akash Arora to cease using the domain name "yahooindia.com" permanently, laying emphasis on the word that 'Yahoo' has necessarily acquired significant goodwill and reputation.[19]

The case of ***Zippo vs. Anil Moolchandani &Ors.(2013)***[20], portrays the level of protection extended to shape marks within the Indian legal framework, governing the trademark law. The reason being, the first protection to a 'shape mark' as a trademark was provided by the High Court of Delhi to the *Zippo Manufacturing Company*(plaintiff), based out of USA for its iconic lighter against imitation by the Moolchandani products.The facts of this case are, the plaintiffs came across counterfeit lighters being sold with the Zippo mark in the shape for which the plaintiffs claims to be a well – known trademark in the category concerned. In view of this instance, the plaintiffs sent a notice to the defendants who immediately agreed to stop selling and manufacture the similar

[19] Preyansi Anand Desai, *Yahoo!, Inc vs. Akash Arora & Anr,* https://thelegalquorum.com/yahoo-inc-vs-akash-arora-anr/.
[20] Zippo vs. Anil Moolchandani& Ors. (unreported, CS (OS). 1355/2006) [DEL HC – pronounced 31st October, 2011].

lighters.[21] The cause of action arose, when in June 2006, the plaintiffs were familiar of the fact that the defendants didn't stop their business and thus sought an injunction for the same.

In this case, it was duly observed by the Honourable Court that –

*"Like other trademarks it would be sufficient for a shape mark to enable the public concerned to distinguish the product from others which have another commercial origin, and to conclude that all the goods bearing it have originated under the control of the proprietor of the shape mark to whom responsibility for their quality can be attributed."*

This case effectively recognises the distinctiveness of the shape and granted the application which paved the way for shape marks, with respect to the Indian origin.[22]

The case of ***Christian Louboutin SAS vs. Abubaker & Others (2018)*** [23]**,** essentially deals with the trade dress claim of Louboutin, who sought to protect its red sole as a trademark on the claim that it had acquired distinctiveness through extensive and long – term use in fashion.[24] The background of this case, crucially signifies the cause of action thereby concerned, when the defendants Abubaker, a competitor to the plaintiffs (here, Christain Louboutin SAS), began selling shoes with a similar red sole thereby prompting Louboutin to file for trademark infringement.

This case is significant in the current context, as it serves as an essential precedent on eh global scale of legal interpretation for any cases to be filed in the future that involves non – conventional trademarks in eh Europe, specifically and for other States an international case study, thereby encouraging brands to explore unique identifiers beyond the traditional logos and names.

The Judgement of this case, was ruled in favour of the plaintiffs, i.e., Christian Louboutin, where the CJEU allowed the red sole to be registered as a trademark under certain conditions including the distinctive character and non – functional nature and as well the ability to be represented graphically, thereby possessed by the plaintiff brand.

---

[21] Mridula Bhatt, *The Case of Unconventional Trade Marks – Does the Trade Marks Act, 1999 Need Reform,* (March 19, 2023), https://www.scconline.com/blog/post/2023/03/18/the-case-of-unconventional-trade-marks-does-the-trade-marks-act-1999-need-reform/.

[22] *Id*, at 18.

[23] Christian Louboutin SAS vs. Abubaker & Ors (2018 SCC Online Del 12069).

[24] *Id, at 18, 22.*

This case, from the perspective of non – conventional trademarks covers two major considerations –

- ⇒ *Effective Recognition for Colour Marks* – this case lays a focussed platform for non – conventional trademarks as it emphasises on the possibility of registering colour marks, especially when the distinctiveness for such marks has been acquired through extensive use. [25]
- ⇒ *Registration Challenges*– the ruling delivered in this case, underscores the on-going challenges in registering non – conventional trademarks particularly on the grounds of distinctive character and functionality. For pursing effective registration, businesses shall provide some substantial evidence of consumer recognition in order to ensure that their marks do not effectively serve the functional purposes and as well is of a distinctive nature.

### *2. Recent Trends:*

***Crayola*** obtains an olfactory trademark for the scent of its crayons. This is a successful instance of registration for a non – conventional trademark where Crayola was issued a registration for its "crayon - scent" in 2024, after a six – year long battle with the United States Patent and Trademark Office **(**USPTO**)**by facing innumerable procedural complexities dating back to the time when Crayola filed its application on the 10th of September, 2018.[26] It is important to note here that, the trademark was issued to Crayola under the category of Non – Visual, Non – Speciality Crayola Crayon Scent Mark, which could be evidently deduced from the description given the applicants as –

*"The mark consists of a scent reminiscent of a slightly earthy soap with pungent, leather – like clay undertones."*

This latest instance only marks the foundation for the successful registration of an olfactory mark but also highlights the various reasons behind the intricacies and complexities associated with the registration process for such marks being unusual in terms of the challenges a layperson faces in

[25] Sumedha Sainath, *A Critical Comparative Analysis of The Contemporary Challenges Revolving Non –Conventional Trademark*, IJLLR, ISSN: 2582-8878, PIF: 6.605.

[26] *Crayola trademarks the 'slightly earthy' smell of its crayons,* (August 23, 2024), https://financialpost.com/news/crayola-trademarks-smell-crayons.

clearly describing the mark in a way that meets the necessary distinctiveness criteria.[27]In this present case, long delay in the trademark registration is initially due to the refusal of the Crayola's application 4 separate times by the USPTO on the ground that the "crayon scent" essentially came from the ingredients used to make the crayons thereby indicating the functional nature of the claimed scent and thus registration was refused.[28]Further, the refusal highlighted the reasoning revolves around the aspect that the scent of their crayons are a natural by-product of the manufacturing process for the goods and is a fragrance which the competitors should use for their products and that the application made was for the wax mix with the colouring compounds thereby forming the common crayon.

As a strong reaction to the refusal, Crayola argued that, the scent of their crayons was unique irrespective of the fact that same ingredients as other crayons was used and essentially mentions about a 'special step' in its manufacturing process that results in the fragrance of the crayons. Thus, it was argued that as this special step is the main reason for the obtained scent, this cannot be considered as a functional factor and it is not a result of the manufacturing process involved in making the crayons. After this argument by the Crayola Properties, Inc., the USPTO has successfully accepted the application for their trademark registration.

## VI. Actionable Suggestions and the Way Forward

By analysing the various aspects concerning the non – conventional trademarks and the procedural conundrums faced by this very category of marks, lays a broad scope for certain set of actionable suggestions and the future prospects concerning the very registration criteria, which has been lucidly specified in the present segment of the research paper –

### *1. Actionable Suggestions:*

*a. Relevant amendments to the existing Trademarks–*

[27]Michael Buck IP,*'Scent Trade Marks: The Sweet Scent of IP Protection',*(November 17, 2024)https://www.lexology.com/library/detail.aspx?g=e91c4f0e-7374-4894-88b3-ba1fddaf43c3&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2024-11-19&utm_term=

[28]*Crayola trademarks the smell of its crayons, a 'slightly earthy soap with pungent, leather – like clay undertones',* (August 22, 2024), https://www.hindustantimes.com/business/crayola-trademarks-the-smell-of-its-crayons-a-slightly-earthy-soap-with-pungent-leather-like-clay-undertones-101724324748967.html.

It is necessary to bring about certain relevant changes in the Trademarks Act, 1999, to explicitly include detailed provisions regarding the non – conventional trademarks with clear definitions and structured guidelines to promote its registration procedures.

**b.** *Extensive Consumer Surveys and Market Research* **–**

This aspect categorically forms the basis for consideration as a crucial suggestion in order to foster a thought in the applicants, thereby encouraging surveys and market research in order to assemble the necessary evidence of the acquired distinctiveness in order to lessen the registration complexities to at least a basic extent. This collected data, may aid the applicant to substantiate their claims during the entire registration process.

## *2. The Future Prospects – The Way Forward:*

This section of the paper, enlists the future prospects to enhance the position of non – conventional trademarks from the vantage point of the registration conundrums, specifically, within the Indian legal framework, which are mentioned as follows –

***a.*** *Collaborative Initiatives***–**

The scope and awareness of the procedural complexities of the non – conventional trademarks can be effectively addressed and necessary steps can be taken to overcome the hindrances arising thereof, if considerable level of engagement with the stakeholders, is made, including that of the businesses, consumer groups and specifically with legal experts in order to formulate and constitute a collaborative framework to address the cropping concerns while fostering the brand promotion and innovation.

***b.*** *Pilot Programmes***–**

The concept of pilot programmes, in the long – run associates a great relevancy to foster a bright future prospect for the non – conventional trademark by launching certain pilot programmes in order to allow the businesses to test the registration process for the non – conventional trademarks under an administered environment thereby gathering all the necessary feedbacks to refine the procedures before proceeding further to pursue with an application to be made for the concerned non – conventional trademark.

## VII. Conclusion

Taking all the said and discussed aspects into consideration, it can thus be concluded that an extensive navigation into the governing legal landscape with respect to the non – conventional trademarks and the registration process thereof, essentially constitutes a scope that is both broad and challenging. In the era of globalisation, as the businesses set forth to indulge more into differentiating their stand in the competitive market in terms of their products by add ending a unique identifier that improves their market position considerable notches higher in terms of their product value and the associated factor of reputation. As clearly elaborated in the previous section of the paper, the unique parameters in the form of scents, sounds, tastes, colours, etc., need to be accommodated with a robust legal framework on the notes of these very innovative trademarks that are growing to own a paramount importance, essentially in the entire regime of intellectual property rights. However, the procedural conundrums that are identified as potential research gaps, thereby posing as a stumbling block in the pursuance of a registration journey free from any version of hurdles are clearly understood, primarily from the provision of the statute governing Trademarks and most importantly, The Trade Mark Rules, 2017, where Section – 5 of the Form TM-A, vitally deals with the Application form for Trademark read with Rule No. 26 of the said Rules that emphasise upon the Non – conventional trademarks and the form of application to be made to serve the intended purpose. However, further clarity is required about the same so far as the procedural modalities are concerned. In terms of the identified gaps in procedural compliance, the category of 'smell marks' should be given the necessary importance in the ambit of the application forms such that more recognition for the Non – Conventional Trademarks could be realised. Thus, in this regard, the actionable suggestions and future prospects specified in the research paper as promised in the abstracts, essentially mandates an ample understanding of the existing and prospective technicalities entailed with the entire concept of non – conventional trademarks to enact certain targeted reforms and strategic initiatives to tune in with the *lex loci* legal requirements, thereby laying a path forward to place the innovative shade of trademark as a dynamic commercial landscape to realise the full potential of the concerned trademarks from the new normal lens of intellectual property rights.

[This page was left blank intentionally]

# AUTHORSHIP DILEMMA IN AI-GENERATED WORKS: AN ANALYSIS OF THE CONCERNS RELATED TO COPYRIGHTS AND CREATIVITY AS POSED BY GENERATIVE AI

*[1]

**Abstract**

*The symbiosis of AI and content creation has revolutionized creative landscapes. However, this synergy also raises intricate copyright challenges. This article explores collaborative solutions to navigate the complexities of AI-generated content and copyright, emphasizing the importance of interdisciplinary cooperation, ethical considerations, transparency, and adaptive legal frameworks. Recently there has been an influx of applications and software for content creation. This has been thoroughly utilized by Gen Z. The task of creating content whether a piece of writing, poem, or research paper, which was the domain of human intellect, can be delegated to an algorithm/large language model. This poses pertinent risks to human capabilities and raises questions concerning the content's ownership and further IPR issues. The article explains the brief history of generative AI, the workings of generative AI, and ethical considerations, specifically of the ChatGPT, and endeavours to seek a resolution. While discussing the issues, the prime concern is kept in mind: Will such software applications be able to impact the originality of the content creation? If yes, what are the major issues relating to intellectual property that would be expected as an outcome?*

**Key Words:** Authorship, Copyrights, IPR, AI, Generative AI

[1] Dr. Alamdeep Kaur, Assistant Professor of law, Army Institute of law, Mohali, alamdeep.k@gmail.com

## I. Introduction

The idea of generative AI has generated interest and anxiety in the field of artificial intelligence (AI). Systems capable of producing original content are referred to as generative AI. Although generative AI's capabilities have produced creative applications in several industries, they have also brought up difficult legal issues, especially about copyright law. In contrast to traditional creative works where humans are acknowledged as the authors, artificial intelligence (AI)-)-generated works have blurred the lines of authorship due to questions regarding who should be credited as the creator and who owns the rights to these creations.

While trying to differentiate the traditional process of creation of text from the AI-based generation, one must mention Ernest *Hemingway*[2] who is very rightly referred to as "an economist of words" and is applauded for his writing style. This relation can be understood only when writing or reading is associated with the enjoyment of the task. As also, stated by the former Honorable Chief Justice D.Y. Chandrachud about the texts as 'pages read like poetry'. Creative work here is writing such a text that is digestible, comprehensible, and meaningful. The meaningfulness is a trait of the text, which is imperative to any writing. There is subjectivity in the task of writing and reading, as well. In writing, it is the style of every writer, whereas in reading, it is the interpretation of the text. However, 'contextual connotation' is the foremost element in both processes.

While one ponders upon the comprehensibility and contextuality of writings, the world has entered into an era of automated 'content creation'. Now, here the creation is not the text in the form of poetic writing but still, there is the creation of a 'content'. The algorithms are continuously generating responses. One looks forward to the quick output and not the joy of writing. The content is created out of a large corpus of text data and not out of the vortex of wisdom and ideas of the author.

OpenAI has created one such generative AI[3] called ChatGPT. It has also led to debates on the infringement of Intellectual Property rights. Other applications work like Chat GPT, such as Perplexity, Chatbot AI, Jasper AI, etc., however, Chat GPT is formative. With 175 billion parameters and the capacity to process billions of words in a single second, it is the biggest and most potent language model yet developed.[4] The evolution of technology has facilitated every

[2] Ernest Hemingway, an American writer and journalist, is a Nobel laureate in Literature.

[3] *Accelerating Your Growth from R&D to Roi*, Informa TechTarget, (June 12, 2023) http://www.techtarget.com/.

[4] *The Technology Behind Chat GPT-3 - ClearCOGS*, ClearCOGS (March 4 2023), https://www.clearcogs.com/post/the-technology-behind-chat-gpt-3, ( last visited March 25, 2023).

aspect of life. Existence has become trouble-free and numerous things are just one click away. AI is also used in a variety of applications, including product recommendation systems like Amazon's where AI can measure the room to suggest beat furniture and image recognition software like Google Lens. Additionally, platforms like Myntra, Nykaa, and Tira use AI to analyse beauty products, and Lenskart has been using AI for a while to implement 3D try-on features to suggest best possible glasses according the face shape, among other things. This has led to a transformation, whether positive or negative, in lifestyle, creativity and production.

## II. Computer tools and Automation

Usage of computers had increased considerably by the 70's. Till date the applications that are most used have been MS Word[5] and MS Excel[6] and others of like sort. However, this did not pose much of concerns about the copyrights and ownership of the works created by using them. This is because computer programmes were used as mere tools for writing with the sole purpose of assisting in the creation of the work at hand. Creativity was majorly the human domain. Artificial Intelligence has transformed the use of computer programmes, as they are autonomous and can make independent creative decisions.As a result, the question of copyright ownership for works produced by AI systems and humans becomes relevant, especially as the similarities between these two types of work increase.

## III. Generative AI and its implications?

Generative AI is a path-breaking technology that uses chatbots[7] with never before like generation and understanding of linguistic content which is similar to natural language used by humans.[8] The GPT-3 model is similar in working to AI based models but it is a language processing model.[9] It is from large language models that Generative AI is derived[10]. Large language models are a form of

[5] *The history and timeline of Microsoft Word*, Microsoft (July 17, 2024), https://www.microsoft.com/en-us/microsoft-365-life-hacks/writing/history-of-microsoft-word, ( last visited April 4, 2025).

[6] *The History of Microsoft Excel*, Excelhelp.com, https://www.excelhelp.com/the-history-of-microsoft-excel/, ( last visited April 4, 2025).

[7] Oxford Language Dictionary, A computer program designed to simulate conversation with human users, especially over the internet.

[8] *Supra* note 2.

[9] Rahib Imamguluyev, *The rise of GPT-3: Implications for natural language processing and beyond*, 4 International Journal of Research Publication and Reviews 4893–4903 (2023).

[10] Shreya Sampathkumar, *ChatGPT and Copyright Issues*, IP Matters (April 20, 2023), https://www.theipmatters.com/post/chatgpt-and-copyright-issues (last visited April 25. 2024).

machine learning called the Natural language processing model and it processes huge amounts of data along with processing the connections between the words picked up from texts.[11] While it generates human-like text, it is also used for translation and summarisation. GPT, Generative Pre-training Transformer, is from the neural networks family[12] that use the transformer architecture[13]. GPT is breakthrough in the field of AI which powers the generative AI applications[14]. GPT provides the applications with the ability to generate language responses that are coherent and relevant. The responses of the application are human-like and seem to be like a conversation, however, are generated as per the input provided to the application. GPT and chat-based applications together automate and generate responses to do tasks like translation, summarisation to writing blogs, creation of websites, visual designs, animation, coding, in-depth research, and writing poems.[15] The GPT models are used in various applications such as chatbots and virtual assistants.[16] For example, a chatbot using GPT can generate replies to customer inquiries and also give personalised recommendations to customers dependent on the earlier interactions between the chatbot and the customer.

The extent of success of such technology lies in the speed and scale at which it operates. The labour of hours altogether in research can be saved within seconds. Such AI based models have enhanced the research into the fields of increasing productivity in organisations along with better services for the customers by reinventing new applications.[17]

## IV. Generative AI and its Working

[11] *Id.*

[12]Neural networks are simple models of the way the nervous system operates. A **neural network** is a simplified model of the way the human brain processes information. It works by simulating a large number of interconnected processing units that resemble abstract versions of neurons. *available at:SPSS Modeler 18.0.0*, IBM - United States (May 25, 2023), https://www.ibm.com/docs/en/spss-modeler/18.0.0?topic=networks-neural-model, (last visited April 25. 2024).

[13]Transformer is a deep learning (DL) model, based on a self-attention mechanism that weights the importance of each part of the input data differently. *available at:*www.datagen.tech, (last visited on May 25, 2023).

[14]Generative AI can learn from existing artifacts to generate new, realistic artifacts (at scale) that reflect the characteristics of the training data but don't repeat it. *available at:*https://www.gartner.com/en/topics/generative-ai (last visited May 30, 2023).

[15]*What is GPT AI? - Generative Pre-Trained Transformers Explained - AWS*, Amazon Web Services, Inc., https://aws.amazon.com/what-is/gpt/ (last visited May 29, 2023).

[16] Hafsa Rizvi, *Applications and Benefits of GPT Models in Natural Language Processing*, LinkedIn: Log In or Sign Up (Apr. 12, 2023), https://www.linkedin.com/pulse/applications-benefits-gpt-models-natural-language-processing-rizvi, (last visited April 25, 2024) .

[17]*Supra* note 12.

It is important to comprehend the complex process of content generation by the AI, which is significant for deciphering the possible infringements and other issues. Arthur McCarthy coined the term "artificial intelligence" in 1956. Artificial intelligence (AI) is the ability of a digital computer or computer-controlled robot to do tasks routinely performed by intelligent beings.[18] AI is intangible form of technology and is further of many kinds such as verbal, learning, problem-solving etc. There is a large pool of data that consists of billions of human conversations. Based on this pool of huge data these models are trained. As they are trained, they use it to learn the patterns. The structures of human conversations are learned and then comes the output part. When they receive input, based on the patterns and structures the text is generated. This text is the 'content' which is created. Now, this is to be understood that this generated text is going to be similar in style to the data they were trained on. Generative AI trains on a massive amount of data which is processed and learned from.

## V. Affirmative utilisation of Generative AI

Generative AI can be utilised to the fullest by academicians. The humongous task of going through the lengthiest of judgments can be minimalised by generative AI. Reading the authorities like *Keshwananda Bharti vs. Union of India*[19] can be a time-consuming task, however, generative AI's summarisation could help if time is scarce. The crux of the case or the ratio decidendi could be highlighted to assist the researcher. It comes with a great deal of help to academic writers when they are searching for list-specific journals. It comes in handy for the students when they have to research on various topics and also while making their project reports. If the researcher is struggling with a specific footnoting style generative AI can be of help.

## VI. Concerns posed by Generative AI

What is groundbreaking here is that the content that is created is an intelligible piece of text. These are paragraphs altogether and not merely standalone sentences. This is done by processing the data and not by understanding it. It can be very rightly compared to a parrot.

[18] *Artificial Intelligence*, Science Direct, https://www.sciencedirect.com/topics/social-sciences/artificial-intelligence#:~:text=Artificial%20Intelligence%20is%20defined%20as,decision%20making%2C%20and%20language%20translation, (last visited April 25. 2024) .

[19] (1973) 4 SCC 225; AIR 1973 SC 1461.

Elon Musk's group cited a paper in their letter that calls ChatGPT a "stochastic parrot".[20] As it is being said, it works like a parrot. A parrot has no understanding but can change the order of words and still comes out with meaningful sentences without knowing what it is saying. A parrot can change the sequence of words and still end up speaking something meaningful but it doesn't know the meaning of the sentence. It is like a highly advanced auto-complete mechanism, that can't comprehend the content it is creating. The responses that are given by generative AI seem to make some sense but are merely an articulate copy of the massive amounts of data available to it. It is compared to a parrot because a parrot merely mimics the sounds that humans make and while doing so it never comprehends nor can put some meaning to the sounds that it is making. However, the confusion begins when the sounds which are made by the parrot end up making some sense to them. This needs to be understood here that while copying the sounds parrot never comprehended the meaning of the human sounds and while repeating them also it never understood the meaning or context of the sounds. The meaning or sense of the speech of a parrot is put in by the listener who can comprehend and interpret the language. A parrot cannot even differentiate between two different languages because its capabilities are restricted to only copying the sounds it hears, which can be in Chinese, English, or even gibberish.

Children adore playing with applications such as 'Talking Tom' or 'Talking Angela'. These applications also repeat the sounds they hear and the kids' amusement has no bounds when they hear what they had fed 'Talking Tom' or 'Talking Angela', to be repeated in a comical sound. But, can we say that 'Talking Tom' or 'Talking Angela' understand the meaning of the kids' conversations with it, the answer would be 'No'. This is very simple to understand here that 'Talking Tom' or 'Talking Angela' have no understanding of the language and neither can they differentiate between two languages nor could they comprehend the meaning.

Similarly, generative AI is a mechanism that is trained like a parrot and mimics precision, like 'Talking Tom' or 'Talking Angela'.[21] It works on continuous guesswork and resetting of the data available to it. There is no memory and no understanding of the input given to it and also the output

[20] *AI experts disown Musk-backed campaign citing their research*, The Economic Times, https://economictimes.indiatimes.com/tech/technology/ai-experts-disown-musk-backed-campaign-citing-their-research/articleshow/99150759.cms (last visited July 14, 2023).

[21] Although a Parrot and the toys like 'Talking Tom' or 'Talking Angela' can be differentiated as a parrot can still be trained but toys like 'Talking Tom' or 'Talking Angela' are pure mechanics, but 'Talking Tom' or 'Talking Angela' application for smart phones might not be just pure mechanics.

provided by it. All the relevance and meaning are put in the output by the user and the eventual result is the creation of 'content'.

### 1. *Issue concerning authorship and copyrights*[22]:

*a. Authorship and AI:*

The algorithms are trained on data sets that many times include material that is already copyrighted, this results in copyright infringement, unknowingly.[23]It is important to know the author of the work, whether it is created by an individual or generative AI. It is the ownership/authorship of the content that connects it to the copyrights of the content. Here, with generative AI, the concern is manyfold. Two main issues have attracted attention towards the creative work of AI and has led legislative discussions around copyright and artificial intelligence (AI): First, can the content generated by AI be copyrighted, and Can the Training of AI lead to infringement of copyrighted content? The content generated via AI could lead to infringement in two-fold manner, first, direct and second is indirect. The direct infringement means when the AI produces content which is word by word copy of another copyrighted material. Indirect is when the content reproduced is can be used for further infringements. These roles of generative AI require a fresh outlook with regard to the decide the liability.

First, it is undeniable that through this technology massive amount of content can be produced, the question that arises is whether the generative AI would be the owner or the user would be the owner of the content. The term 'content' consists of two things, 'input' and 'output'. 'Input' is the text prompt or query put up by the user to generative AI, based on which it will generate a response. E.g. as per the terms of service of ChatGPT, such 'input' i.e. the question that is put forth to ChatGPT would belong to the user. In such cases, the 'output' also would belong to the user, because, the response was generated dependent on the 'input'. However, this would be so to the extent the user is abiding by the company's policy and does not infringe any other law. Beyond this, the user is free to use the content in the manner he/she wants. Whereas, this is not the case with the 'output'. Output is also owned by the user, but generative AI companies claim that the

[22] Copyrights Act, 1957, §. 14.

[23] Malcolm, Jeremy (2018). Artificial Intelligence: Governance and Intellectual Property. Electronic Frontier Foundation.

same or similar output can be generated resultant of another user's 'input'.[24] This can happen because of the nature of machine learning. The responses generated might not be unique.

*b. The idea of originality:*

The question of Copyright over the content created via generative AI is an unavoidable one. However, if, we understand the most basic concept of 'copyrights', as mentioned in Section 13 of the Copyrights Act, 1957, which pertains to the instances where the copyright would subsist and the ingredient which comes to light is originality. So, first, the work[25] must be original, second, the person claiming the copyright as per Section 2(d) (i)[26] must be the author of the work. Also, when the work is created through a computer, as per Section 2 (d) (iv)[27], the author is the person who is causing the work[28] to be created. So, if the input is generated into the generative AI by the user, he/she is causing the work, output, in this case, to be created. However, the role of the user further than generating the input is doubtful. As per Section 2 (d) (iv)[29] the use of a computer is a tool to create the work[30] whereas with generative AI this is not the case. It is generative AI which is further creating the work on its own without any role played by the user. So, one is faced with two distinct works that are copyrightable i.e. the input or the text prompt and the output. In the European Union, the concept of originality is related to the expression of the author's creation. If this is the standard then the shortest of the prompts also will qualify the test of originality if they are created out of the author's intellect.[31] Also in the United Kingdom the text prompts into an AI can be original if they are a demonstration of the author's effort inclusive of the decision making involved in the creation

[24] Samantha Fink Hedrick, *I think, therefore I create: Claiming copyright in the outputs of algorithms*, 8 New York University Journal of Intellectual Property & Entertainment Law, 324-381 (2019).
[25] Copyrights Act, 1957.
[26] Copyrights Act, 1957, §. 2(d) (i).
[27] Copyrights Act, 1957, §. 2 (d) (iv).
[28] Copyrights Act, 1957, §. 2(y).
[29] Copyrights Act, 1957, §. 2 (d) (iv).
[30] Pamela Samuelson, Symposium: The Future of Software Protection: Allocating Ownership Rights in Computer Generated Works, 47 University of Pittsburgh Law Review, 1205-09 (1986).
[31] Francesca Mazzi, *Authorship in AI-Generated Works: Exploring Originality in Text Prompts and AI Outputs Through Philosophical Foundations of Copyright and Collage Protection*, https://atrip.org/wp-content/uploads/2024/05/3rd-place-revised.pdf. (last visited Jan 05, 2025).

process.[32] Whereas in the US a certain level of creativity has to be visible in the same to attract copyrightability. [33]

Getting back to the initial argument of originality, further two ingredients become significant, which are the independence of the work and the protection of the expression of the idea and not merely the idea. According to the approach of "skill and judgment with a flavour of creativity," As laid down in *Eastern Book Company v. D.B. Modak,*[34] creativity is apparent in the expression of a work, not the idea on which the work is based. Both the ingredients can be realized when the work is fixed in some tangible form. This means that the originator of the idea might not be the author under the Copyrights Act, 1957. This difference becomes clearer in the cinematographic films, photography, and music as well. Certainly, the generative AI output is a tangible medium but the output which is in front of us is a result of an idea expressed by the user i.e. in the form of a query and the output is dependent upon this query. Had there been no query there would have been no output.

So, the output created is itself not independent. This means that just because an author has copyright protection over the text prompt will not mean that the author will also get protection over the output generated by the AI. The copyrights protection extends only to the expression of the ideas and not the ideas themselves. So, the text prompt can be seen as a creative work which results in the protection of output as a distinct work. So, the author of the input i.e. the text prompt might have copyright protection over the same but might not have any protection over the response generated by the AI. The copyright over the text prompt leads to further rights in favour of author such as reproduction, distribution of the material. But all such rights will not be extended to the response generated by the AI. So, the author will not have any right over the generated content with respect to acknowledgment, license, and infringement.

*c. The Idea and Expression dichotomy:*

This leads to the second argument of authorship that to be the author, one must be the creator of the work. This further emphasises the significance of the resolution of the idea and expression

[32] *Id.*
[33] *Id.*
[34] (2008) 1 SCC 1.

dichotomy. In *Eastern Book Company vs. D.B. Modak,*[35] the Supreme Court has emphasised that to be able to claim a copyright the author must validate it based on skill and judgement and a mere newness of the idea would not be able to establish the same. The copyright is not based on the original idea rather it pertains to the expression of the idea. The test of "sweat of the brow", which venerates the efforts and expense put in by the author, becomes redundant here as the labour and time are not at all invested by the user of the generative AI.

As per this doctrine, reliance is put more on labour and time invested in creating the work instead of the level of creativity it holds. Moreso, generative AI cannot imbibe expression into the content as it is not basic to machine learning language. It can create a particular language dependent upon its training but will not be able to exert any meaning into it. Etymologically, generative AI lacks expression which is reflected in the form of output. Second, is the question of authorship, where generative AI's status is doubtful once again. Its 'terms of use' clearly talk about the output to be under the ownership of both i.e. users as well as the AI. As earlier stated, the output created is not the sole work of generative AI, it is the fruit of the seed put forth by the user.

Also, if we stretch this argument to its farthest length, it can be contended that the user whether a free-rider or subscriber used the services of the platform. So, it becomes morally obligatory for the user to share the ownership of the content with the platform. However, in both scenarios both i.e. the user and generative AI will not be able to claim sole authorship over the content, especially the output.

On further deliberations, it becomes clear that there are two scenarios: the user being the author or the AI being the author.[36] If the author is considered to be the user the argument would be based on the fact that it was the user who undertook all the necessary arrangements for the generation of the artistic work generated by the AI. Whereas in the scenario of AI or the developer of the said AI being the author, it plays the role of an autonomous agent. The role of the user is limited to the initiation of the process.[37] Even if the user is put in the role of a programmer, then also the situation doesn't change much as the main responsibility of the production of the content based on training of the algorithm or creativity is on the shoulders of the AI algorithm. This is also so because the developer of the said AI has programmed the algorithm such that it would be able to create the

[35] *Id.*

[36] Arjun Padmanabhan & Tanner Wordsworth, *A Common Law Theory of Ownership for AI-Created Properties*, 104 Jornal of Patent and Trademark Office Society 155, Apr. 2023, at 155, 176.

[37] *Id.*

outcome as it was laden with specific skills by the developer.[38]This can be compared to the use of other programmes but without AI qualities such as Microsoft Word. Microsoft Word also allows users to create original works. However, the status of an authorship is very clear when any work is created using Microsoft word, the copyright of such work would be with the user of the software. The user has used the application which had word processing tool so, the application was also used as an assisting tool. The Microsoft will not be able to claim a copyright on the work so created. But with the AI generated work the scenario is different. When a computer acts as an autonomous agent and produces works through algorithmic, sequential, or non-deterministic processes, there seems to be a noticeable difference between the input that humans provide and the output produced by computers using AI.

Delhi High Court in *Camlin Pvt. Ltd. Vs. National Pencil Industries*[39], stated that "copyright is conferred only upon authors or those who are natural person from whom the work has originated and expounded the meaning of the term "author" by affirming that "mechanically reproduced printed carton" was not a subject matter of copyright for the reason that it was not possible to determine who the author of such carton was. In the circumstances, the plaintiff cannot claim any copyright in any carton that has been mechanically reproduced by a printing process, as the work cannot be said to have originated from the author. A machine cannot be an author of an artistic work, nor can it have a copyright therein".[40] The painting created by using Raghav AI art work was initially granted the copyright under co-authorship however, was denied the same subsequently owing to lack of lack of IPR regime to be able to accommodate such cases.[41]

***c.*** *Considering Joint authorship:*

The argument of Joint Authorship[42] may be considered, however, two issues emerge if the doctrine of joint authorship is applied here. However, the joint authors must share the responsibility of expressing their ideas. Because there is involvement of more than one author in the generation of

[38] Pamela Samuelson, Symposium: The Future of Software Protection: Allocating Ownership Rights in Computer Generated Works, 47 University of Pittsburgh Law Review, 1205-09 (1986).
[39] AIR 1986 Delhi 444.
[40] *Id*. at para.54-55.
[41] Kumkum Mishra, AI-Generated Content & Copyright Law in India: Navigating the Legal Maze, IP LINK (April 5, 2025), https://www.iplink-asia.com/article-detail.php?id=1286, (last visited on April 7, 2025).
[42] Copyrights Act, 1957, §. 2(z).

the work the test to weigh it becomes collaboration, contribution, authorship, and non-distinctness.[43]

First, where there is a joint authorship, the issue resolves itself if the work can be segregated to determine separate authorships. However, the problem is when the author's contribution cannot be segregated. In such cases, the following relation between the authors comes into play: first, if both of them are employees the copyright will vest in the author.[44] Second, if they are independent, then the ownership will depend on the agreement. If there is no agreement then it is generally joint and shared.[45]

Consequently, this would not qualify as works of joint authorship as defined under Indian Copyrights Act, 1957 for the simple reason that the contribution of one author is not distinct from the work of the other. Moreso, in generative AI there is no requirement of oversight by the user beyond the input prompt in order to generate the content. So, that would be the end of the role of the user in the generation of the content.

Secondly, many a times joint authorship means that the authors would be able to exploit the work, whereas, at many other places it means that in order to be able to exploit the work jointly they need the other's consent.[46] In India, on the same lines, Allahabad High court has held a similar view in *Nav Sahitya Prakash and others vs. Anand Kumar and others*[47], where it was observed that the joint owners of copyrights need the consent of the other to be able to grant a license or interest in the copyright.[48] In the English case *Powel and Head*,[49] in the instances of one of the joint owners granting the license with the consent of the other would not bind the other author and he would be able to sue for infringement of copyright.[50] So, if the authorship is joint between the user and generative AI, first, there is no segregation of the contribution of the creativity into the work. Only

[43] Tehila Rozencwaig Feldman, *The Author and the Other: Reexamining the Doctrine of Joint Authorship in Copyright Law*, 32 The Fordham Intellectual Property, Media and Entertainment Law Journal (2021).

[44] Joint Authorship, Joint Work | Technology and IP Law Glossary, Technology and IP Law Glossary, http://www.ipglossary.com/glossary/joint-authorship-joint-work/ (last visited Oct. 5, 2023).

[45] *Id.*

[46] *Id*.

[47] AIR 1981 All 200.

[48] *Joint authorship and copyright*, Asia IP, https://www.asiaiplaw.com/article/joint-authorship-and-copyright#:~:text=Meanwhile,%20in%20Nav%20Sahitya%20Prakash,or%20interest%20in%20the%20copyright." ( last visited Oct. 6, 2023).

[49] 1879 12 Ch.D 686.

[50] *What Do You Need To Know About Joint Authorship in India? Academike Explainer - Academike*, Academike, https://www.lawctopus.com/academike/joint-authorship-in-india/ (last visited Oct. 5, 2023).

Input being the contribution of the user makes the Output dependent on itself. Second, as mentioned previously the responses generated might not be unique. The same or similar output can be generated resultant of another user's 'input'. So, here the first user being a joint author with generative AI must be given a right to be consulted when the work would be shared with another user. If consulted and the consent to do so is decline by the first user generative AI will not be able to share or generate it for any other user. Moreso, copyright is a right to protect the author or original work from duplicity or copying. Generative AI itself claims the similarity of the output, which makes the other user also the equal owner of the content. So, to conclude the discussion, all three entities claim right over the content i.e. the users and AI. Here another question surfaces, will the other user, be able to claim to be the 'owner of the content'? Also, will he/she be able to put forth a claim to be the 'owner of copyright' to the said similar content?

Leaving whole of this argument aside, in countries like India, a machine cannot claim the protection of copyrights, it can only be claimed by humans. Whereas, countries like UK do talk about the machines and claim to copyrights.

***d.*** *Ethical dilemmas:*

As explained, AI works on lines of large language models based on algorithms. In conventional copyrights the creator if using someone else's creation would seek permission to utilise the work for his purpose. Section 52(1)(j) of the Copyrights Act, 1957 deals with this. The AI developer does not do so. This is specific to the data fed to the AI algorithm and also the data that AI generates and then utilises the data itself. This raises pertinent questions related to the use of previously copyrighted materials, such as can a generative AI use the content, which is created, for its training purpose? E.g. the terms of use of ChatGPT say that the API Content won't be used for training purposes whereas the non-API content can be used if the user doesn't opt out.

Many generative AI models are available in the free version and also in the form of a paid subscription. It is also available to the companies through the generative AI platforms. In this way, companies can install generative AI into their systems such as to answer the queries of the customers etc. The content which is created by such companies while using generative AI is the API content and when the user is using generative AI itself, such content is non-API content. As the Indian copyrights law still does not include the AI in the definition of 'author' but that is not

just the problem. There is the issue with respect its working as well. These algorithms work on data sets and imitate patterns. For example, if an AI generated image is to resemble the work of Japanese artist Yokoyama, the AI would be trained on the original work of the artist.[51] Similar is the instance when the AI is to generate content similar to the work by J.K. Rowling, so it will train on the original work of the author.[52]

Data, for whichever purpose it may be used, has become the precious metal for 21st century. "Web scaring" is the term coined for the unauthorised user of data available in the web space. That is why the AI developers have been criticised as they use users data without their consent.[53] More than 300 billion words "articles, websites, books, posts, including personal information obtained without users' consent," are purportedly taken from the internet by OpenAI.[54] for training of its algorithms. Since data is now regarded by US courts as "property," such scarping gives rise to claims of data theft and misappropriation.[55]

A user still has a legitimate expectation that his data will be safe and private, even if posted an image or any other type of data online for public viewing, as on our blog or social media profiles.[56] In *KS Puttaswamy vs. Union of India*,[57] the Supreme court held that right to privacy is a component of Article 21 of the Constitution. A negligent conduct that violates our privacy and betrays our confidence occurs when our data is utilized to train AI software without our express agreement.[58]

### *2. Role of Intention in copyright infringement by AI*

The conventional idea of copyrights emphasises on the intent and deliberate knowledge of the wrong. That is why; to overcome this, the concept of fair use underlines the purpose of the

[51] IndiaAI, https://indiaai.gov.in/article/the-legal-implications-of-ai-generated-content-in-copyright-law (last visited Jan 9, 2025).

[52] *Id*.

[53] It is alleged that AI companies have violated Article 5(1)(a), 12, 15, 16 and 25(1), 36 of GDPR. Such as failure to take prior consultation as required under Article 36 of GDPR. Available at <ChatGPT-maker OpenAI accused of string of data protection breaches in GDPR complaint filed by privacy researcher | TechCrunch>.

[54] Uri Gal, "ChatGPT is a Data Privacy Nightmare. If you've ever posted online, you ought to be concerned"; The Conversation (Feb 7, 2023) available at ChatGPT is a data privacy nightmare. If you've ever posted online, you ought to be concerned (theconversation.com).

[55] Calhoun v. Google, 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021).

[56] https://corporate.cyrilamarchandblogs.com/2023/10/guardians-of-genius-securing-tomorrows-generative-ai-via-copyright-protection/

[57] (2017) 10 SCC 1.

[58] Californian Torts Law recognizes intrusion into the solitude or seclusion of person or his private affairs as highly offensive to a reasonable person.

unauthorised usage of the content. If the purpose is to use it for criticism, research, and teaching etc., the unauthorised usage may be allowed. What is to be noted here is that the emphasis on the purpose is to further unveil the conscious intent behind the usage. Whereas, generative-AI, as explained above, lacks knowledge, consciousness and intent. As there is no malicious intent that would raise the question of treating the AI-generated content differently.[59]The liability of copyright infringement is shared between the developer of the AI and the user prompting the algorithm. It is significant to comprehend both the roles as the user provides the context by feeding the prompt into the AI algorithm, which eventually results in the output generated by the AI. The conventional notion based on intent, which could be related to the natural beings, cannot be connected to an artificial being which is autonomous.The concept of copyright infringement must evolve to cover this concept of liability. There are safe harbour provisions related to social media platforms, which protect them from the liability that could be incurred due to actions of the users while using such platform. Generative AI is autonomous so the applicability of safe harbour provisions requires fresh outlook. As with AI-generated content, new issues are brought forth in the legal framework and technological innovations could themselves come to the rescue with solutions. Due to the increase in the content created by the AI there have been new challenges relating to copyright infringement.

## VII. A Comparative Analysis of National and International Laws

In the Berne Convention of 1886, there have been no discussions on "non-human authorship' and similar has been carried forward in the TRIPS agreement. Moreover, a less similar view has been put forth in the WIPO internet treaties WIPO Performances and Phonograms treaty, and the WIPO copyrights treaty. However, there has been no restriction against it as well. So, if the states wish they could include specific laws in their municipal law.

As explained above, according to Indian copyright law the work to be copyrightable must have enough content input from the author. As the AI-generated content lacks this so, it has been time and again established by courts that AI algorithms cannot be held owner of such content. This has been reinstated In *Tech Plus Media Private Ltd v. Jyoti Janda*,[60] by Delhi High Court. It was held

[59] Sobel, Ben (2017). *Artificial Intelligence's Fair Use Crisis*. Columbia Journal of Law & the Arts, 41, 45-73.
[60] 2014 (60) PTC 121 (Del).

that AI is a juristic person and so, as per Indian copyright law, it is incapable of holding a copyright. The Court further stated that the plaintiff, however, could become the owner of the copyright in the work under a contract with its author.[61]

The Indian view has been reinstated by the U.S. Court in *Naruto v. Slater*[62], popularly known as the "Monkey Selfie" case, the court in the United States held that the monkey could not be taken as the author of the selfies it clicked. Copyright in a work can only be conferred on a human author and not on animals and machines in the U.S.[63] Also as declared by the U.S. Copyrights Office the works created by any non-human entity is not copyrightable.[64]. Moreover, in *Express Newspapers plc v. Liverpool Daily Post & Echo*[65], the U.S. courts have regarded the computer as a tool for human assistance. The U.S. district court of Columbia in 2023, while delving on the same issue reinstated its previous stance in *Stephen Thaler v. Shira Perlmutter*[66] *that the U. S. copyrights office was proper in rejecting the application for grant of copyrights for a work created by an AI.*[67]They emphasised on lack of human involvement in the process.

Whereas, The UK Copyright, Designs and Patents Act, 1988 presents a different view. It defines computer-generated work to be work as if it has not been created resultant of any kind of human intervention.[68] This clause was added, "to create an exception to the requirement of human authorship to provide due recognition and protection for the work that goes into creating a program capable of independently generating works."[69] If that is the case then as established in the United States also, the author of a work that is created with the help of AI may have a copyright if he/she establish that the AI program was used as a tool/medium in the creation of the work.[70]

---

[61] *Id*., at para 20.

[62] 2016 U.S.Dist.Lexis 11041 (N. D.Cal. Jan, 2016).

[63] *Id*. at 449.

[64] U.S, Copyright Office, The Compendium of U.S Copyright Office Practices, Chapter 300, 313.2 (revised on Sept.29, 2017).

[65] (1985) FSR 306.

[66] Civil Action No. 22-1564 (BAH) Decided: August 18, 2023.

[67] Rajiv Sharma, Ninad Mittal, Artificial Intelligence lacks personhood to become the author of an Intellectual Property, LiveLaw (Sept. 22, 2023), https://www.livelaw.in/law-firms/law-firm-articles-/artificial-intelligence-intellectual-property-indian-copyright-act-singhania-co-llp-238401?fromIpLogin=73619.53008038545, ( last visited on April 7, 2025).

[68] The Copyright, Design and Patents Act, 1988, §. 178.

[69] Nina Fitzgerald & Eoin Martyn, *An In-depth Analysis of Copyright and the Challenges presented by Artificial Intelligence.* Ashurst's Website, https://www.ashurst.com/en/news-andinsights/insights/an-indepth-analysis-of-copyright-and-the-challenges-presented-by-artificial-intelligence (last visited Mar 11, 2020).

[70] Kalin Hristov, "*Artificial Intelligence and the Copyright Dilemma*", 57 (3) IDEA 435 (2017).

## VIII. Other concerns posed by Generative AI:

There are several legal and ethical issues ancillary to AI-generated content, along with the prime issue of authorship. AI many times can generate objectionable or indecent content. The content so generated might insinuate racism, violence, defamation, etc. However, the legal framework misses out on civil or criminal liability. Moreover, the possibility of the elimination of the incriminating material will make the adverse effects irreversible. Consequently, the prospective measures would become ineffective because of the irreversibility of the effects.

### 1. *Risk of replacing human creativity:*

There is a pertinent risk of replacement of human creativity by AI tools. The human-generated ideas are now competing with machine-generated ideas. The intuitive feel of fresh and original thought is facing the risk of being replaced by mechanical algorithms based on auto-generated ideas. As mentioned above, generative AI will be able to write poems, as well. William Wordsworth while closing "Daffodils"[71] beautifully explains remembering daffodils and the pleasure of the same through his heart dancing with the daffodils. The task, if we can say, here in front of Wordsworth was not, merely, to jot down a few rhyming lines, rather it was an emotions-based healing i.e., by staying close to nature and the lesson to appreciate the beauty of nature. The task, we can now certainly say, here in front of generative AI is to come up with something that seems to be a poem. Certainly, the option to use or not to use AI tools for one's work is open to every creative thinker. It is similar to the instances of creating something on one's own or getting it outsourced. However, the only difference is that earlier the entity to whom the task was to be outsourced used to be another human, whereas now, it is an algorithm. But the creative thinker is in a fix just like Prince Hamlet[72] and as he says," to be or not to be is the question".

[71] William Wordsworth, *Daffodils*, *Poems in Two Volumes*, (Longman, Hurst, Rees, and Orme, 1807).

[72] *Prince Hamlet* is the title character and protagonist of William Shakespeare's tragedy 'Hamlet' (1599–1601).

### *2. Incorrect factual information:*

Generative AI has made the courts of law to be face to face with an "unprecedented circumstance".[73] This refers to the instance that came to light in front of a court in New York where a lawyer used ChatGPT for research and referred to cases that never existed. Although embarrassing for the lawyer who happened to have 30yrs of experience but the consequences could be far-reaching as the fact was brought to light by the opposing counsel stating that they could not find the cases their opponents were referring to. The senior vice-president of Google, Prabhakar Raghavan has stated that AI can many a times 'hallucinate' and come up with 'answers which are convincing but completely made-up'.[74] The incorrect factual information can be given with such precision that it sounds reliable. The issues which arise due to such instances is that this might lead to spreading of misinformation, which can be a deliberate act as well. Emphasising the role of AI in the dissemination of wrong information, OpenAI's CEO Sam Altman, has shown concern.[75] This can tarnish the repute of a person by creating such content and further quoting such article which never existed. One such instance comes from a law professor of and American university that he was wrongly accused of sexually harassing a female student in the AI-generated content which referred to an article that was never written.

ChatGPT not only came up with a piece of false information but also relied upon the false content. Now, here the problem becomes two-fold. This can be understood when we see that generative AI is creating content out of the pool of data which consists of numerous human conversations. If the content it is being fed with is incorrect would result in further false information. This answers the question of it coming out with wrong answers or content and also clarifies the point that the spreading of the misinformation can be deliberate. As discussed above, generative AI is unable to understand the meaning or context, it will produce whatever is being fed to it. This might lead to a vicious circle of misinformation, which cannot be relied upon. Also, the rights mentioned under Section 57 of the Copyrights Act, 1957 provide authors with integrity, and paternity rights also get infringed. The AI cannot claim royalties for its works as per the present laws. Similar is the

---

[73] *Lawyer faces trouble after using ChatGPT for research, AI tool comes up with fake cases that never existed*, India Today, https://www.indiatoday.in/technology/news/story/lawyer-faces-trouble-after-using-chatgpt-for-research-ai-tool-comes-up-with-fake-cases-that-never-existed-2385542-2023-05-28 (last visited June 12, 2023).

[74] *Id.*

[75] *ChatGPT falsely accuses US law professor of sexually harassing a student, invents a news article*, India Today, https://www.indiatoday.in/technology/news/story/chatgpt-falsely-accuses-us-law-professor-of-sexually-harassing-a-student-2357597-2023-04-09 (last visited Oct. 12, 2023).

scenario when objectionable or defamatory content is generated. It becomes difficult to determine the AI's liability as AI cannot discern its actions based on moral judgment.

### *3. Generation of wrong responses:*

These models generate wrong, erroneous, or inappropriate responses. This can be understood from the fact that it takes different paragraphs or sentences from various sources and merges them. As we have understood how it works, the seemingly sensible responses have no understanding of the language or context. So, the random texts put together can create content that is meaningless, contradictory, or factually distorted. It seems similar to the ginormous amount of data available on the internet, out of which many texts, comments, or conversations contradict one another. However, it is not quite similar also as the content posted on the internet is mostly generated by humans, whereas generative AI doesn't even know the meaning of whatever it says. It must be remembered that generative AI is a model that creates text responses in a conversational format. So, a similar exercise of fact-checking after browsing would need to be followed after the content creation via generative AI.

## IX. Addressing the concerns

Answering the question of the impact of AI on human creativity, this would always stand as an argument that generative AI is merely a tool and must be used. One must be cautious while using them and check the results generated. These tools if utilized optimally can augment human creativity. For example, a writer might use generative AI to generate ideas for a story or to suggest alternative ways to phrase a sentence.[76] An artist might use generative AI to generate ideas for a painting or to suggest color palettes or composition ideas.[77]

Generative AI trains on a massive amount of data but it is limited, however, the human ability to perceive and create is not restricted. Humans have a gift to think out of the box, which any algorithm will not be able to do as they are trained merely to replicate and re-create out of what is made available to it. It is important to remember that AI models are limited by the data they have been trained on and the algorithms that power them.

---

[76] Mahendra Palecha, *ChatGPT explaining why you should not use ChatGPT for creativity*, LinkedIn: Log In or Sign Up (Feb. 23, 2023), https://www.linkedin.com/pulse/chatgpt-explaining-why-you-should-use-creativity-mahendra-palecha.

[77] *Id.*

A 'content creator' might be confused due to the massive overflow of content and the speed of the same but a 'creative thinker' would not be, because, he is empowered by the capability to contemplate a particular thought or an idea.

When this is argued, that generative AI generates wrong, erroneous, or inappropriate responses, which shows that such models are not perfect. It becomes significant that it is used with caution and its output is duly verified. However, the future versions of generative AI are likely to be more advanced. Such as they are expected to have better Language Understanding and comprehend the intent of the user resulting in a more natural response. Also, if this technology becomes more industry-specific, such as medical, legal, finance, hospitality customer service etc., then specialized and more accurate responses can be expected. This would happen because the domain-specific application will train on the domain-specific data. Also, as mentioned at the beginning of this paper, there must be a writing style followed by an author, the future versions of generative AI could be customized to the extent of personalized user-based conversations. Such responses could pertain to the individual needs of a particular user including the style of writing he might follow.

## X. Suggesting an integrated approach

The NITI Ayog report 2018 has specifically centered around AI in various sectors across India. While carving out a national strategy for Artificial Intelligence, it has been realized that there are unclear security, privacy, and ethical regulations.[78] This is so because the IPR regime is in its infancy, and security, privacy, and ethical regulations appear as arenas to be dealt with. To address the issue at hand, a collaborative approach is required involving the AI developers, content creators, policymakers, and lawyers. The second most significant step towards solving the intricate matrix would be the ethical considerations in responsibility regarding content generation, licensing, and ethical AI development and usage practices. This brings one to the third significant consideration of educating the AI developers, users, and content creators about intellectual property rights. Technology and law can be reconciled through workshops, seminars, and educational programs that bring together copyright practitioners and AI specialists. These partnerships promote a more thorough comprehension of the problems and possible fixes. Such challenges are not exhaustive

[78] National strategy for Artificial Intelligence, Niti Ayog, June 2018, https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf (last visited on Jan. 24, 2025).

and is are addressed by eh government expeditiously can be a worthy catalyst to bring about significant change toward achieving the goal of AI for all.[79]Moreover, there must be more transparency about the use of AI in any content generation. This gives clarity concerning the origin of the content. This would lead to a sustainable environment for content creation and AI domains. The knowledge and acknowledgment of the involvement of AI in any content creation would also pave the way for worthy recognition of the role played by the user and the AI developer, respectively. As this could further determine the pecuniary issues dependent on the same. The need for a licensing agreement catering to the specific needs of hybrid content and adequate compensation for the users could be solved.

The intellectual property regime must adapt technological advancements. The concept of fair use can be made specific to the use by content creators an AI. Fair use policies customized for AI-generated content can be produced through cooperation between copyright specialists and AI engineers. These rules ought to strike a balance between originality, transformative use, and the effect on the market for already-existing works. Copyright laws and the legal framework must be in collaboration with technological advancements. By modifying legal standards, AI-generated content can be safeguarded while maintaining the fundamentals of copyright. The emergence of AI-generated material presents new copyright infringement issues. Despite its lack of intent, AI can produce content that violates the law, hence creative solutions within the current framework are required. Society can successfully negotiate the tricky landscape of AI-generated content and copyright infringement with the help of cooperative efforts, technologically advanced solutions, and flexible legal frameworks.

This does not suggest that works produced by AI need to be available to the public. Another example is that a company utilizing AI to generate content might retain ownership of exclusive rights related to that content, including trade secrets or patents. A "selection or arrangement of data" constitutes an intellectual creation that may qualify for copyright or sui generis protection depending on the jurisdiction where it is developed. Collections may contain data that is protected by copyright law or may not include such material. In light of the increasing significance of AI, there is a pressing need for a legal framework for data protection that clarifies who deserves recognition for various creative works or concepts. Establishing such legislation is crucial for

[79] *Id.*

several social and economic reasons, such as fostering innovation and upholding free and open markets. Excessive protection of personal data might hinder technological advancements, which are expected to supersede human creativity soon, so regulations should find an equitable compromise. As of now, India lacks a comprehensive data protection law. Nevertheless, in India, “computer programs, tables, compilations, including computer databases,” are classified as "literary works" and thus safeguarded by the Copyright Act.

## XI. Concluding remarks

To conclude it can be said that the AI-generated content is not yet recognized as authors of such content. However, in one way or the other the output generated is protected via copyrights. It won’t be very difficult for generative AI to survive in a service industry dependent upon API content. However, to survive in a creative field, it will have to establish itself on ethical and regulatory grounds. Such applications are a handy tool but the content created and method of content creation must cater to the ever-evolving societal needs. The future of language-based AI must focus on its beneficial traits, along with accentuating accountability towards the content itself. This certainly depends on the advancements in AI research and technology, but all the stakeholders i.e. the users or platforms, have a different role to play in each content that is created. Even if the mode and medium of content creation via AI is thoroughly mechanical, the content that is created through this process is further going to be involved in the creation of more content. So, at this moment it is a bundle of rights and obligations, which at first need to be addressed.

As discussed, the work must be independent and must demonstrate a level of creativity. Even if the level of creativity is not very high, medium would also suffice as a modicum of creativity. An AI-powered application's data and algorithms are essential components for guaranteeing operational success. For innovators to feel confident that they will be able to profit from and claim credit for their work, the intellectual property regime in the context of AI must be strong and enforceable. This is crucial for advancing entrepreneurship, innovation, and fundamental and applied AI research. India’s IPR regime needs an overhaul to clarify the uncertainties regarding the ownership of the works created via AI. The usage of data for training purposes must be regulated, along with a mechanism for licensing to cover these areas. Such a mechanism needs to be convenient to use

by the AI developers and effective for the data owners. A robust dispute resolution mechanism is the need of the hour.

According to the NITI Aayog National Strategy for Artificial Intelligence, a task group consisting of the Ministry of Corporate Affairs and DIPP should be established in order to review and make the necessary changes to the IP regulatory framework for AI.[80] However, to solve this issue, the upcoming generative AI models must foresee the ethical considerations such as impartiality, transparency, and responsibility, in content creation. Disputes based on ownership and authorship of the AI-generated content may arise, leading to increased litigation amidst legal uncertainty.[81]In order to combat AI-generated copyright infringement, innovative solutions can be extremely important. Proactive protection can be provided by AI algorithms developed to recognize and stop possible violations in created content. It is crucial to encourage developers, consumers, and content producers to use AI ethically. Unintentional infringements can be decreased by educating AI practitioners on ethical standards, copyright laws, and best practices. International cooperation is essential because AI and content dissemination are global in scope. Uniformity in tackling the difficulties of AI-generated material is ensured by reaching consensus on ethical principles, attribution, licensing, and legal conventions.

[80] *Supra* note 41.
[81] *Supra* note 44.

[This page was left blank intentionally]

# INTELLECTUAL PROPERTY AND LABOUR RIGHTS IN INDIA'S FILM INDUSTRY: A LEGAL PERSPECTIVE

*1

**Abstract**

*The Indian film industry, a pivotal cultural and economic entity, stands at the crossroads of intellectual property rights (IPR) and labor rights. This article delves into the intricate relationship between these two dimensions, examining how the protection of creative works through IPR frameworks directly impacts the labor force that contributes to this dynamic sector. With an increasing proliferation of digital media and content distribution, filmmakers and artists face challenges concerning copyright infringement, unauthorized reproductions, and fair compensation. Simultaneously, the industry grapples with labor issues such as wage disputes, precarious employment, and a lack of representation for workers. This exploration provides a comprehensive overview of current legislation, confronting case studies, and advocacy efforts aimed at reconciling IPR with labor rights. Through a synthesis of scholarly research and industry perspectives, the paper aims to highlight pathways for reform that uphold both intellectual property protections and fair labor practices, ensuring a sustainable future for all stakeholders in the Indian film industry.*

**Keywords:** Intellectual Property Rights (IPR), Labour Rights, Indian Film Industry, Copyright, Film Workers.

[1] Dr.R Bharat Kumar, Assistant Professor, Damodaram Sanjivayya National Law University, Visakhapatnam, India.

## I. Introduction

The Indian film industry, often referred to as "Bollywood" for its prominent Hindi-language film output, is a vibrant and dynamic entity that has garnered international acclaim and significant economic importance. With an annual output of over a thousand films in multiple languages, the industry not only contributes to the cultural fabric of India but also plays a substantial role in the nation's economy, generating billions in revenue and providing employment to millions of people. However, the flourishing landscape of Indian cinema is characterized by complex issues surrounding intellectual property rights (IPR) and labor rights, both of which are critical to the industry's sustainability and growth.

IPR, encompassing various forms of legal protection such as copyright, trademarks, and patents, are essential for safeguarding the creative expressions of filmmakers, actors, and other artists. In a sector where originality is paramount, IPR ensures that creators can protect their work from unauthorized use and exploitation. Despite clear legislative frameworks, the enforcement of IPR in the Indian film industry often faces numerous challenges, including rampant piracy, a lack of awareness among artists about their rights, and difficulties in navigating the legal landscape. These obstacles not only affect the revenues of filmmakers, but also have repercussions for labor, as the viability of creative work directly impacts employment opportunities and fair compensation for workers.

On the other hand, labor rights in the Indian film industry are fraught with issues that highlight the precarious nature of employment for many workers. Actors, technicians, production staff, and countless other contributors often work under informal contracts with little job security or protection. Wage disputes are common, and labor laws are often overlooked, placing workers at a disadvantage. The stark reality for many in the industry includes long hours, low pay, and a lack of representation in negotiations for fair working conditions. Despite this, labor unions and advocacy groups are increasingly vocal about the need for reforms that prioritize worker rights alongside the protection of creative output.

The interplay between IPR and labor rights presents a nuanced challenge: while protecting the rights of creators is fundamental to fostering a thriving film industry, ensuring that laborers are treated fairly and compensated adequately is equally critical. The relationship between these two dimensions is complex; conflicts may arise when the focus on IPR undermines the rights of

laborers who are integral to the filmmaking process. For instance, restrictive contracts that limit the artistic expression of workers or deny them fair attribution and pay raise significant ethical questions within the sector.

As the film industry continues to evolve, particularly with the rise of digital distribution and streaming platforms, the implications for IPR and labor rights are profound. Innovations in technology offer new avenues for content dissemination and revenue generation; however, they also introduce challenges in the enforcement of rights and the protection of labor. The rapid pace of change demands that stakeholders, including filmmakers, workers, and policymakers, engage in open dialogue to ensure a balanced approach that promotes both creativity and fair labor practices.

This article aims to examine the intersection of intellectual property rights and labor rights within the Indian film industry comprehensively. It will explore the existing legal frameworks, highlight case studies of contention, and analyze recent reforms aimed at addressing these multifaceted issues. By synthesizing scholarly research and industry insights, this paper seeks to inform policymakers and advocates about the necessary steps toward fostering a sustainable film industry that respects both creative rights and labor dignity.

## II. Understanding IPR

IPR is a legal protection granted to creators and inventors that allow them to control the use of their creations and derive economic benefits from them. In the context of the Indian film industry, IPR serves as a crucial mechanism that safeguards various forms of artistic expression, ensuring that filmmakers, writers, composers, and other creators retain ownership of their work. By protecting creative outputs, IPR encourages innovation, sustains artistic endeavors, and contributes to the economic viability of the industry.

### *1. Types of IPRs Relevant to the Film Industry*

Several types of IPR are particularly pertinent to the film industry, including:

- ***Copyright:*** The most significant form of IPR in the film sector, copyright protects the original works of authorship, including films, scripts, soundtracks, and even posters. Under the Copyright Act of 1957, creators gain exclusive rights to reproduce, distribute, display, and

perform their works. This protection lasts for the lifetime of the creator plus an additional 60 years, after which the work enters the public domain.[2]

- ***Trademarks:*** Trademarks protect symbols, names, and slogans used to identify and distinguish goods or services. In the film industry, this includes movie titles, logos, and branding associated with characters and franchises. Trademarks help build brand identity and consumer trust, which are essential for the commercial success of films and related merchandise.[3]

- ***Industrial Designs:*** Though less commonly associated with films, industrial designs protect the visual design of objects that can serve as a part of the film's aesthetic, such as costumes and set design. This type of protection ensures that the unique visual elements of a film are not used by others without permission.[4]

- ***Patents:*** While patents generally apply to inventions or processes, they can also be relevant to the film industry, especially concerning innovative technologies used in filmmaking, such as new special effects methods or film-editing software.[5]

### *2. Legal Framework Governing IPR in India*

The Indian legal framework governing IPR is primarily facilitated through various acts and regulations, including:

- ***The Copyright Act, 1957:*** This is the cornerstone of copyright law in India, providing comprehensive rules for the protection, ownership, and infringement of copyrightable works.

- ***The Trade Marks Act, 1999:*** This act outlines the legal parameters for trademark registration and protection, ensuring that brand names and logos are safeguarded.

- ***The Patents Act, 1970:*** While not directly applicable to films, this act enables the protection of technological innovations related to the film industry.

[2]Copyright Act, 1957.
[3]Trade Marks Act, 1999.
[4]Industrial Design Act, 2000.
[5]Patents Act, 1970.

These laws establish the groundwork for IPR protection; however, the effectiveness of enforcement and the awareness of rights among creators significantly affect their ability to leverage these protections in practice.[6]

### *3. Challenges to IPR Protection in the Indian Film Sector*

Despite the established legal frameworks, the Indian film industry faces substantial hurdles in protecting IPRs. Among the most pressing challenges are:

- ***Piracy:*** One of the most significant threats to IPR in the film industry is piracy, which involves the unauthorized reproduction and distribution of films. The growth of digital platforms has exacerbated this issue, as online streaming and torrenting sites make it increasingly easy to access pirated content. The economic impact of piracy is profound, with substantial losses reported by filmmakers due to unauthorized copies of their works being circulated.[7]
- ***Lack of Awareness:*** Many creators in the Indian film industry are often unaware of their rights and the available mechanisms for enforcing those rights. This lack of awareness contributes to the exploitation of their work, as artists may inadvertently agree to terms that restrict their ownership or access to equitable royalties.[8]
- ***Inefficient Legal Enforcement:*** The enforcement of IPR laws in India can be slow and cumbersome, leaving creators vulnerable to infringement. Legal battles can be financially draining, and long delays in litigation may discourage creators from pursuing their rights.[9]
- ***Misinformation and Misunderstanding of Rights:*** Misconceptions regarding what constitutes a violation of IPR, as well as complex legal terminologies, can lead to confusion and ineffective

[6] Mark Torous, *Intellectual Property Rights in the Digital Age: Challenges and Solutions*, 23 J. Int'l Bus. Res.1 (2024),https://www.abacademies.org/articles/intellectual-property-rights-in-the-digital-age-challenges-and-solutions-16831.html (last visited Apr. 2, 2025).

[7] Shradha Murthy et al., *The Effects of OTT Platforms on the Indian Film Industry*, 2(2) REST J. on Data Analytics & Artificial Intell. — (2023), https://doi.org/10.46632/jdaai/2/2/4 (last visited Apr. 2, 2025).

[8] Lawrence Liang, *Between Charity and Rights: Law and the Struggle for Worker's Rights in the Indian Film Industry*, in *Indian Cinema and Human Rights: An Intersectional Tale* (A. Dubin, R. Goswami & I. Sharma eds., Springer 2025), https://doi.org/10.1007/978-981-97-6028-2_16 (last visited Apr. 2, 2025).

[9] Dr. Sonali Anand Burte et al., *Challenges in Enforcing Intellectual Property Laws in the Film Industry*, **3** Int'l J. Emerging Techs. & Innovative Res. 59 (Dec. 2023), https://iciset.in/Paper2710.pdf (last visited Apr. 2, 2025).

action against infringers. Educating filmmakers and other stakeholders about their rights is essential to bolster the protection of intellectual property.[10]

- ***Contractual Issues:*** Many creators sign contracts that may limit their rights without a full understanding of the implications. Contracts that are overly broad or contain vague language regarding ownership, distribution, or compensation can lead to disputes over intellectual property.[11]

## III. Labour Rights in the Indian Film Industry

Labour rights refer to the legal rights and protections afforded to workers, ensuring fair treatment, safe working conditions, and equitable compensation for their labor. In the Indian film industry, which operates on a dynamic and often informal basis, the realization of these rights is critical for safeguarding the interests of a diverse workforce that includes actors, technicians, crew members, and support staff. Despite the economic significance of the industry and the extended hours of labor required to produce films, labor rights issues persist, leading to a myriad of challenges for those involved.

### *1. Overview of Labour Rights and Labour Laws in India*

India has a robust legal framework aimed at protecting labor rights, encapsulated in several laws and regulations that govern various aspects of employment. Some of the pivotal labor laws related to the film industry include:

- ***The Industrial Employment (Standing Orders) Act, 1946:*** This Act mandates employers in industrial establishments to define the terms of employment and establish standing orders outlining the rights and responsibilities of workers.
- ***The Minimum Wages Act, 1948:*** This legislation ensures that workers receive a minimum wage, which holds significant relevance in the film industry, where contracts may often

[10] YAGAY and SUN, *Understanding Infringement under Intellectual Property Rights*, TAX MGMT. INDIA (Feb. 3, 2025), https://www.taxmanagementindia.com/visitor/detail_article.asp?ArticleID=13456 (last visited Apr. 2, 2025).
[11] Martin Kretschmer, *Copyright and Contract Law: Regulating Creator Contracts: The State of the Art and a Research Agenda*, 18 J. Intell. Prop. L. 1 (2010), https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1101&context=jipl (last visited Apr. 2, 2025).

deviate from this requirement. In the context of the film industry, producers sometimes exploit loopholes to circumvent wage regulations, leading to disparities in compensation.

- ***The Payment of Wages Act, 1936:*** This Act regulates the timely payment of wages, providing a legal recourse for workers in cases of delayed or non-payment. Such delays are particularly common in the film industry during the post-production phase, where cash flow issues may arise.
- ***The Factories Act, 1948:*** Although typically applied to manufacturing industries, certain provisions of the Factories Act, particularly regarding working hours and safety, may also be relevant to film production environments where significant hazards exist.

Despite these protections, many workers in the film industry operate outside the formal employment structure, often engaging in freelance or contractual agreements that neglect these legal requirements. The ephemeral nature of film projects can lead to a lack of job security and benefits, rendering workers vulnerable to exploitation.[12]

### *2. Common Labour Issues Faced by Workers*

The Indian film industry is characterized by several labor-related challenges, including:

- ***Job Insecurity:*** Many workers are hired on a project-by-project basis, leading to uncertainty regarding their employment status, income stability, and access to benefits such as healthcare and retirement plans.
- ***Wage Disparities:*** Significant disparities exist in wages across different roles in the film production process. While leading actors and directors may command high salaries, countless technicians and supporting staff often receive minimal compensation that may not reflect the actual work or hours put in.
- ***Long Working Hours*****:** The film industry is notorious for demanding excessively long hours from its workers, often exceeding legal limits. The pressure to deliver high-quality

[12]George Morgan, Julian Wood & Pariece Nelligan, *Beyond the Vocational Fragments: Creative Work, Precarious Labour and the Idea of 'Flexploitation'*, 24 Econ. & Lab. Rel. Rev. 397 (2013), https://www.cambridge.org/core/journals/the-economic-and-labour-relations-review/article/abs/beyond-the-vocational-fragments-creative-work-precarious-labour-and-the-idea-of-flexploitation/75068A6F4C4D46B8FFEF7758F9922A93 (last visited Apr. 2, 2025).

productions under tight deadlines exacerbates this issue, with many workers reporting burnout and physical tolls due to the extended working hours.

- ***Lack of Representation:*** Many film workers lack access to effective representation and advocacy mechanisms. The informal nature of employment may lead to situations where grievances related to working conditions or pay inadequately addressed.
- ***Unsafe Working Conditions:*** The dynamics of film production often involves multiple risks, including physical hazards on set, equipment mishaps during location shooting, and exposure to extreme weather conditions. Without proper safety protocols and measures, workers may be left unprotected.

### *4. Discussion of Unions and Collective Bargaining in the Film Industry*

Labor unions play a significant role in advocating for the rights of film workers and fostering collective bargaining. Several unions exist within the Indian film industry, representing various sections of the workforce[13]:

- ***Film and Television Producers Guild of India (FTPGI):*** This organization aims to protect the interests of producers but also plays a role in the broader conversation about labor rights by bringing attention to issues faced by creators and workers alike.
- ***All India Film Employees Confederation (AIFEC):*** This umbrella organization represents various unions from different sectors of the film and television industry, advocating for the rights of technicians, artists, and production staff.
- ***Association of Motion Picture and Television Engineers (AMPTP):*** While primarily focused on technicians, this association emphasizes collective bargaining and aims to negotiate fair wages and working conditions for its members.

Despite these organizations' presence, several challenges hinder effective collective bargaining:

- ***Fragmentation of Unions:*** The existence of multiple unions representing different worker categories may result in fragmented negotiations, leading to a lack of unified representation and diluted bargaining power.

[13] FICCI & KPMG, *Indian Media and Entertainment Industry Report 2015*, KPMG (Mar. 2015), https://assets.kpmg.com/content/dam/kpmg/pdf/2015/03/FICCI-KPMG_2015.pdf (last visited Apr. 2, 2025).

- ***Fear of Retaliation:*** Many workers may hesitate to join unions or participate in collective bargaining efforts due to fear of retaliation from producers or employers. The transient nature of employment in the film industry increases this fear of retribution.
- ***Limited Awareness:*** A lack of awareness about union rights and the benefits of collective bargaining can inhibit worker participation and engagement in these organizations. Many workers are unsure of their entitlements or how to voice grievances effectively.

## IV. Interplay between IPR and Labour Rights

The relationship between IPR and labor rights in the Indian film industry is intricate and often contentious. On one hand, IPR is intended to protect the creative outputs of artists, which in theory should enhance their economic well-being and, by extension, the labor force that supports these creations. On the other hand, the enforcement and prioritization of IPR can negatively affect the labor rights of film workers, particularly in terms of wage disparities, job security, and ownership rights. This section examines these interconnections, identifies conflicts through case studies, and sheds light on the implications of contracts and agreements between creators and employers.

### *1. Impact of IPR on Labour Rights and Workers' Compensation*

The assertion of IPR can directly affect labor rights in several ways:[14]

- ***Ownership of Creativity:*** Ownership disputes frequently arise between filmmakers and their collaborators, with claims to intellectual property resources leading to significant tension. For instance, while directors and producers may claim ownership of a film, actors and writers may seek recognition and fair compensation for their contributions. The lack of clear guidelines regarding ownership rights can leave laborers feeling marginalized.
- ***Contractual Limitations:*** Contracts in the film industry often contain clauses that restrict an artist's creative freedom or dictate how their work can be used beyond the original project. This raises ethical considerations, particularly when creators are not adequately compensated for

[14] World Intellectual Property Organization, *Rights, Camera, Action! Intellectual Property Rights and the Filmmaking Process*, 2nd ed. (2022), https://www.wipo.int/edocs/pubdocs/en/wipo-pub-869-22-en-rights-camera-action-intellectual-property-rights-and-the-filmmaking-process.pdf (last visited Apr. 2, 2025).

the use of their intellectual property in merchandise or sequels, despite the significant profits such endeavors may yield for producers.

- ***Equitable Remuneration:*** The focus on protecting intellectual property can lead to inequities in financial distribution across the production team. Often, significant profits accrued from box office revenues or licensing agreements are not distributed fairly among all creative contributors. Workers whose roles are crucial to the film's success, such as technicians and lower-tier actors, may receive minimal returns while higher-tier individuals reap disproportionate rewards.

### 2. *Case Studies of Conflicts between IPR and Labour Rights in the Film Industry*

Several case studies highlight the conflicts that arise from the interplay of IPR and labor rights in the Indian film industry:

- ***The Case of Rajnikanth's "Enthiran" (Robot)***

  One of the highest-grossing films in Indian cinema, "Enthiran," featured actor Rajnikanth in a dual role. After the film's release, disputes arose over the marketing rights and merchandising revenues. While Rajnikanth earned a substantial amount due to his star power, many crew members, including special effects technicians, claimed that they received inadequate payment for their contributions, highlighting the disparities in how profits from intellectual property were allocated.[15]

- ***The Scandal Around the Film "Gangs of Wasseypur"***

  The films of renowned director Anurag Kashyap, particularly "Gangs of Wasseypur," showcased both the intricacies of filmmaking and labor complexities. After its release, several junior artists and technicians complained of not receiving due credits for their contributions. The tension escalated when the film was commercially successful, spotlighting the ethical dilemma regarding credit and financial returns associated with IPR enforcement versus labor rights.[16]

---

[15] Ashwini Sharma, *Understanding Copyright Infringement: Key Insights & Lessons from Enthiran's Case*, Maadhyam L. Assocs. Blog (July 7, 2023), https://www.maadhyamlaw.com/post/understanding-copyright-infringement-key-insights-lessons-from-enthiran-s-case (last visited Apr. 2, 2025).

[16] Madhavi Biswas, *Globalization and New Bollywood's Hat-ke (Different) Films* (M.A. thesis, Univ. of Tex. at Dallas), https://utd-ir.tdl.org/server/api/core/bitstreams/7a2e975f-d670-4e76-a873-5d75ba1ed46f/content (last visited Apr. 2, 2025).

- ***The Controversy of "Bajrangi Bhaijaan"***

  This film generated considerable revenue for its producers. However, reports surfaced that many daily wage laborers involved in the shooting, from lighting to sets, received meager compensation despite their crucial roles. Following the film's success, these workers voiced concerns that their contributions emphasizing labor rights were overshadowed by the profit-driven focus on IPR.[17]

### 3. *The Role of Contracts and Agreements*

Contracts are fundamental to the film industry as they delineate the rights and responsibilities of various parties involved. However, the language and terms of these contracts can have significant implications.

- ***Ambiguity and Exploitation:*** Contracts in the film industry are often filled with technical jargon, creating ambiguity regarding rights and obligations. Many artists, especially those new to the industry, may inadvertently sign away critical rights to their work without fully understanding the consequences. For example, if a contract stipulates that rights to a character are assigned to the producer indefinitely, the original actor or creator may lose control over their own creation.

- ***Bargaining Power Imbalances:*** Established personalities in the film industry often have the expertise to negotiate better contracts, while lesser-known actors, technicians, and crew members may feel coerced to accept unfavorable terms due to job insecurities. This imbalance can lead to exploitative situations where the rights of less visible contributors are compromised.

- ***Role of Legal Representation:*** To navigate the complexities of contracts, it is essential for film workers to seek legal guidance. However, many artists may lack the resources or awareness to secure legal representation, perpetuating cycles of exploitation by producers and studios who capitalize on this lack of knowledge.

- ***Collective Bargaining Agreements*****:** Several unions and associations, such as the All India Film Employees Confederation (AIFEC), work to improve labor conditions by establishing

[17] L. Gopika Murthy, *The Bajrangi Bhaijaan Lawsuit*, SpicyIP (Oct. 18, 2015), https://spicyip.com/2015/10/the-bajrangi-bhaijaan-lawsuit.html (last visited Apr. 2, 2025).

collective bargaining agreements. These contracts, designed to safeguard workers' rights, are essential for ensuring fair wages and working conditions. However, widespread adherence to these agreements is often challenging in an industry characterized by fluid employment and informal contracts.

## V. Initiatives and Reforms

The Indian film industry operates within a complex landscape of IPR regulations and labor rights protections. To address the challenges faced by both creators and workers, a variety of initiatives and reforms have been implemented at governmental and industry levels. This section aims to provide an overview of these efforts while assessing their effectiveness and potential for improving conditions in the film industry.

### *1. Government Initiatives to Protect IPR and Labour Rights*

Recognizing the significance of both IPR and labor rights, the Indian government has instituted several initiatives aimed at bolstering protections for both creators and workers in the film industry:

- ***The Copyright (Amendmen)t Act, 2012:*** This amendment to the Copyright Act of 1957 enhanced protections for creators by addressing the challenges posed by digital piracy and expanding the scope of reproduction rights. With the rise of online content distribution, this reform emphasized the importance of protecting the intellectual property of filmmakers and artists in the digital age.
- ***National IPR Policy, 2016:*** The National Intellectual Property Rights Policy outlines a comprehensive strategy to promote innovation and creativity while ensuring a balanced approach to IP enforcement. This policy aims to enhance awareness and education regarding IPR, improve the legal frameworks, and facilitate access to IP-related information.
- ***Skill Development Initiatives:*** The Indian government has launched various skill development programs aimed at improving the technical proficiency of film workers. Initiatives like the National Skill Development Corporation (NSDC) work to train individuals in various aspects of filmmaking, from cinematography to production management, thereby enhancing their employability and rights as skilled laborers.

- ***The Code on Wages Act, 2019:*** This legislation seeks to streamline various labor laws by mandating timely and fair compensation for all workers. By establishing a common framework for wage standards, the Code on Wages aims to protect workers in the film industry from exploitation and wage theft.
- ***Film Finance and Insurance Schemes:*** To support filmmakers during production, the Indian government has established finance and insurance schemes to mitigate the risks associated with filmmaking. These measures can indirectly benefit laborers by reducing production delays, leading to more stable employment conditions.

### *2. Role of Industry Bodies and NGOs in Advocacy*

In addition to government initiatives, various industry bodies and non-governmental organizations (NGOs) play a pivotal role in advocating for both IPR and labor rights in the film industry:[18]

- ***The Producers Guild of India (PGI):*** This body represents various stakeholders and works to strengthen industry standards, including promoting fair labor practices among producers to ensure that all artists and workers are treated equitably
- ***Film and Television Institute of India (FTII):*** As a premier institution for film education, FTII not only trains aspiring filmmakers but also raises awareness about the importance of protecting IPR and advocating for worker rights within the industry.
- ***Labor Unions and Professional Associations:*** Unions, such as the All India Film Employees Confederation (AIFEC), represent a collective voice for film workers and advocate for stringent implementation of labor laws. They conduct training and awareness programs, working towards enhancing workers' knowledge of their rights and available resources.
- ***Academic and Research Institutions:*** Collaboration between academia and the film industry fosters research and advocacy efforts aimed at understanding labor issues and IPR implications. Research organizations often publish reports and provide recommendations that inform policy development.

[18] Ariane Lafortune, *Non-Governmental Organisations and Intellectual Property Rights*, Programme on NGOs & Civil Society, Centre for Applied Studies in International Negotiations (Dec. 2006), https://www.files.ethz.ch/isn/31413/2006.12.pdf (last visited Apr. 9, 2025).

- ***NGOs Focused on Labor Rights:*** Various NGOs dedicated to labor rights have started to engage with film workers directly. By providing legal assistance, conducting workshops on workers' rights, and creating platforms for dialogue, these organizations aim to empower workers in the industry.

### 3. *Recent Reforms and Their Impact on the Industry*

The Indian film industry has witnessed several recent reforms that aim to bolster IPR protection and improve labor rights. The following are some notable reforms and their implications:

- ***Increased Penalties for Copyright Infringement:*** Recent legislative changes have seen heightened penalties for copyright infringement, aiming to deter piracy and enhance creator confidence. By enforcing stricter penalties, the government signals a commitment to protecting artistic work, which may encourage greater investment and production within the industry.
- ***Implementation of Digital Rights Management (DRM):*** The adoption of DRM technologies by streaming platforms has introduced new methods for protecting film content against piracy. This shift positively impacts creators' compensation structures, enabling secure revenue streams for their work through licensing agreements.
- ***Policy Changes Under the Cinematography Act:*** Recent discussions have focused on amending the Cinematography Act to facilitate a more transparent environment for filmmakers regarding distribution and revenue sharing. Potential amendments could also include provisions for labor protections, ensuring that workers' contributions are appropriately recognized and compensated.
- ***Growing Recognition of Gender Issues*****:** Recent reforms have highlighted the need for gender equity within the film industry. Initiatives aiming to address the underrepresentation of women in key production roles and creative positions are becoming prominent. By advocating for gender parity, the industry can enhance working conditions and expand opportunities for all workers.
- ***Collaborative Engagement with Stakeholders*****:** An emerging trend is the collaboration between the government, industry bodies, and labor organizations in discussions surrounding

reform. Such engagement creates a platform for advocating for labor rights alongside IPR considerations, signifying a more integrated approach to challenges in the film sector.

## VI. Future Trends and Challenges

The Indian film industry stands on the brink of transformation as it navigates the complexities of IPR and labor rights in an increasingly digital and global landscape. Each year, the industry adapts to changing consumer preferences, technological advancements, and evolving regulatory frameworks. This section will explore the emerging trends affecting both intellectual property and labor rights, alongside potential challenges that lie ahead for stakeholders in the industry.[19]

### *1. Emerging Trends in IPR and Labour Rights*

- ***Digital Transformation and Streaming Platforms:***

With the rapid rise of streaming platforms like Netflix, Amazon Prime, and Disney+ Hotstar, the distribution of films has undergone a significant shift. These platforms not only provide filmmakers with new revenue opportunities but also require them to adapt to digital rights management challenges. The question of how creators maintain control over their work in environments where content can be streamed, licensed, and reproduced at scale has become increasingly complex. This has driven calls for clearer frameworks surrounding digital content ownership and fair revenue sharing for all contributors involved.

- ***Increased Awareness and Education on IPR:***

Efforts to raise awareness and provide education regarding IPR rights are gaining momentum within the Indian film industry. Workshops, seminars, and online resources geared toward filmmakers, actors, and technicians are helping to demystify copyright laws and empower individuals to advocate for their intellectual property. As more creators understand their rights, the likelihood of equitable compensation and recognition of contributions may improve.

- ***Adoption of Technological Solutions for Rights Management:***

The integration of advanced technologies—such as blockchain and artificial intelligence—holds great potential for enhancing IPR management. Blockchain can provide transparency in copyright

[19] Neil Sadwelkar, *The Digital Revolution: Transformation of India's Film Industry*, Indian Sch. of Bus. (May 2024), https://www.isb.edu/en/research-thought-leadership/research-centres-institutes/srini-raju-centre-for-it-and-the-networked-economy/SRITNE-Newsletter/Digitalisation-and-the-Future-of-Work-the-Case-of-the-Film-Industry/The-Digital-Revolution-Transformation-of-India-Film-Industry.html (last visited Apr. 2, 2025).

transactions, enabling creators to track the use of their work and receive fair compensation. Additionally, AI can aid in monitoring content distribution to prevent unauthorized reproductions, thereby better protecting the rights of creators.

- ***Focus on Inclusivity and Diversity in Storytelling:***

As global audiences seek diverse stories and representation in cinema, the Indian film industry is increasingly focusing on inclusivity and gender equity. Greater awareness around labor rights may lead to more equitable practices, ensuring that marginalized voices are heard and compensated fairly. Commitments to ethical storytelling may not only resonate with audiences but also strengthen the industry's sustainability.

- ***Policy Initiatives Oriented Towards Collaborative Governance:***

Future policy developments suggest an increasing trend towards collaborative governance involving government institutions, industry representatives, and labor unions. By fostering a dialogue among stakeholders, the film industry can work collectively to establish frameworks that address both IPR protection and necessary labor rights, promoting fairness and sustainability in production practices.

### *2. Challenges Ahead for the Indian Film Industry*

Despite these emerging trends, the Indian film industry faces challenges that must be addressed to ensure the fair treatment of creators and workers alike:

- ***Persistence of Piracy:***

While initiatives to combat copyright infringement are being implemented, the ongoing threat of piracy remains significant. Unauthorized streaming and downloading continue to undermine creators' revenue, necessitating further cooperation between government, tech companies, and industry stakeholders to develop effective anti-piracy strategies.

- ***Navigating the Gig Economy:***

The rise of gig work in the film industry, characterized by short-term contracts and freelance work, poses challenges for labor rights. The lack of job security and benefits for gig workers complicates the landscape of employment rights and reveals the need for reforms that extend protections to non-traditional workers in the industry.

- ***Equitable Distribution of Revenues:***

With the lucrative nature of the film industry, ensuring fair compensation and equitable distribution of revenues remains a significant challenge. Producers may be reluctant to share profits with lesser-known actors and crew members. Addressing this issue requires a well-defined wage structure and transparent profit-sharing agreements that consider the invaluable contributions of all individuals involved.

- ***Legal Complexity and Enforcement:***

The intricacies of IPR laws and labor rights can create barriers to enforcement, particularly for individuals unfamiliar with legal procedures. Continued efforts are needed to simplify legal frameworks and enhance enforcement mechanisms to protect workers' rights and uphold IPR effectively.

- ***Globalization and International Copyright Issues:***

As the Indian film industry grows globally, navigating international copyright laws and regulations will become increasingly complex. Establishing clear agreements with international distributors regarding IPR protection and labor rights will be essential to mitigate conflicts arising from cultural differences and varying legal standards.

## VII. Conclusion

The Indian film industry is a vibrant pillar of cultural expression and economic growth, yet it operates within a complex interplay of intellectual property rights (IPR) and labor rights. Throughout the article, we have explored the significant role that IPR plays in protecting creative outputs and fostering innovation, while also acknowledging the persistent challenges that creators face, such as piracy, lack of awareness, and legal enforcement difficulties. Simultaneously, we examined the critical state of labor rights within the industry, where precarious employment conditions, inadequate wages, and a lack of formal contracts continue to jeopardize the livelihoods of countless workers.

The intricate relationship between IPR and labor rights reveals a dual dilemma: strong protections for intellectual property are essential for encouraging artistic creativity and ensuring economic viability, yet these protections must not come at the cost of workers' rights to fair treatment, compensation, and representation. Conflicts often arise when the focus on IPR undervalues the significant contributions of a diverse workforce, from technicians to support staff, whose roles are crucial to the filmmaking process.

As the industry evolves amidst technological advancements and changing consumption patterns, particularly with the rise of digital platforms, stakeholders must advocate for collaborative governance that respects and upholds both IPR and labor rights. Efforts should be directed toward creating a more equitable framework that facilitates fair revenue sharing, ensures appropriate legal protections, and enhances labor conditions.

Government initiatives, industry reforms, and collective advocacy by labor unions and NGOs can collectively form a comprehensive strategy to tackle these intertwined issues. It is essential to continue raising awareness about rights among creators and workers alike, fostering an environment where both intellectual property and labor rights are recognized and valued.

In summary, achieving a sustainable and just Indian film industry requires a balanced approach that respects creative innovation while equally prioritizing the dignity and rights of the labor force. By aligning the interests of all stakeholders, the film industry can strengthen its foundations and ensure that both artistic and labor rights are celebrated, ultimately leading to a healthier, more equitable creative ecosystem.

[This page was left blank intentionally]

# THE DOUBLE-EDGED SWORD OF PATENT THICKETS: CHALLENGES AND OPPORTUNITIES IN THE TECH INDUSTRY

*[1]


## Abstract

*In the postmodern world, Intellectual Property (IP) rights are the driver of innovation and the protector of creative works. IP ensures that the creator of the IP is rewarded suitably and consequently creates an ecosystem for innovation and healthy competition. Ironically, the same IP rights can also become dysfunctional with respect to the purpose for which it was created. The villain in this content is patent thickets. It is the collection of patents owned by several parties over the same technology. This situation acts as an entry barrier to the new entrants, who have to deal comprehensively with each patent in the patent thickets web. Just like the ordinary web, the web of patent thickets also entangles anyone who deals with it and wastes efforts, time and resources. To be precise, they increase the chance of litigation risks, create legal and financial barriers, which is antithesis to the ease of doing business, particularly to the new market entrants. Case studies such as Qualcomm's licensing practices and the prolonged Apple-Samsung patent disputes are quoted to understand the gravity of the issue from real life incidents. The above case studies throw light on how patent thickets become a bottleneck for new product development, thereby obstructing the atmosphere of innovation.*

*Despite the above negative externalities of patent thickets, it has also yielded positive results through cross licensing agreements, patent pools and participation in standard setting organisations. To support the above argument, MPEG LA patent pool and Tesla's open patent strategy are explained along with the fruits they have reaped. Further, effective regulatory and policy frameworks are put forward to opting their positive outcomes. Ultimately, action plans are paved for transforming patent thickets, the perceived villain of innovation to an enabler of innovation.*


KEY WORDS: Intellectual Property Rights, Patent thickets.

[1] Sangeeth Krishna G S, Advocate, sangeethkgs21@gmail.com

## I. Introduction

In the modern world, innovation is one of the most valuable assets of any organization that wants to secure its creative works and maintain its competitive position. Out of all the forms of IP, Patents are the most significant in protecting technological innovation. But, as the innovation momentum increases, especially in areas like telecommunications, Artificial Intelligence (AI), semiconductors and biotechnology, there is a growing challenge called patent thicket, which is also an opportunity in some cases.

A 'Patent Thicket' is a term that describes a situation where there are many interrelated patents held by several actors in a particular technology area. This situation often results in complex and expensive licensing negotiations that can end in legal disputes or time delays in the product development process. Despite the fact that the patent system is supposed to induce innovation by giving rights to inventors, the extension of the existing patents can, paradoxically, hamper innovation. In some cases, extreme patent thickets lead to hold-up situations in which companies cannot bring their products or technologies to market without having to pay exponentially high prices or face legal risks. Start-ups and other small enterprises are especially at risk since they have limited funds to address such issues.

The issue is especially pronounced in dynamic industries including 5G telecommunications where there are so many patents that are crucial for implementation of standards, that it becomes a maze. For instance, companies like Qualcomm are involved in many legal battles that are not only time consuming, but also expensive. Likewise, the semiconductor industry which is characterized by gradual advancements is also facing challenges of patent thickets to both the existing market leaders and the new entrants.[2]

However, this is not to say that patent thickets are always a problem. Curiously enough, they can also serve as a stimulus. With the multitude of patent thicket issues, companies must therefore

[2] The Impact of Patent Thickets on Innovation in High-Tech Industries," International Journal of Emerging Technologies and Innovative Research, Vol. 3, Issue 11, November 2023, at 285, available at https://iciset.in/Paper2639.pdf.

employ measures such as cross licensing, patent pools and participation in standard setting organizations. These mechanisms allow several patent owners to grant, transfer, or license rights, avoid litigation, and foster the formation of industry standards. For example, the MPEG LA pool of patents on video compression has helped companies to trade in innovations and ensure that the owners of the patents used in the development of the product are fairly paid.

This is a very important issue of patent thickets as a dual approach to the future of innovation. Can patent thickets be considered as a hurdle that slows down the technological development or can they become the means of cooperation and innovation? How can policy makers and industry leaders prevent IP from becoming a market access and innovation barrier while at the same time protecting IP?

This paper aims at a closer look at the issue of patent thickets in the tech industry. First, it discusses how dense IP environments can retard innovation, and, conversely, how they may enhance innovation and cooperation. This acknowledges the positive and negative aspects of the issue and provides a basis for understanding how to control patent thickets to achieve the proper purpose of the patent system in a growing global economy.

## II. The Problem: How Patent Thickets Stifle Innovation

### 1. *Legal and Financial Barriers*

Patent thickets pose a real legal and financial problem for companies seeking to innovate in a technology space where patents are plentiful.[3] Many times, there are so many related patents that developers must ensure that they comprehend all the IP rights that are linked with a given idea before offering a solution to the market. This process can be both costly and time-consuming.

A major cost is also coming from licensing fees. To stay clear of legal issues, companies have to secure licenses from several patent owners. For example, in the telecommunications sector, which is based on many patented technologies, each product can involve up to several dozen or even

[3] Y. Wang & P.K. Wong, The Role of Patent Thickets in High-Tech Industries: Empirical Evidence from the Semiconductor Industry, 21 J. High Tech. Mgmt. Research 24, 24 (2010), https://doi.org/10.1016/j.hitech.2010.04.001.

hundreds of licenses. Delayed negotiations are common in such agreements and they increase the overall costs of the product development.

Another problem is the possibility of legal proceedings. If a company develops a technology and unintentionally infringes on a patent, it may be subject to legal actions. A dispute over patent rights can go on for many years and cost millions of dollars in legal expenses and settlements. This can be a financial issue for big companies, but for a small business or a start-up it may be a death blow. Such legal risks tend to prevent, to some extent, the entry of new market players especially in markets that are characterized by a high level of patent protection i.e. patent thickness which in turn reduces competition and innovation.[4]

Moreover, there are compliance issues. Companies have to make sure that their products are compliant with the regulations and also with the licensing agreements that exist. It also means that there is more complexity in terms of navigating patent thickets and therefore higher costs.

### 2. *Innovation Blockages*

Patent thickets are not only financial threats, but they can effectively halt or slow down innovation. One of the most common issues is patent hold-ups, that are situations where patent owners deny the licence, or demand unreasonable prices for its use. For instance, a vital patent owner in a technology standard like 5G can hold up the industry by asking for high royalties because no company can proceed without that patent. These tactics can slow down the development and deployment of new technologies.[5]

Another issue is the problem of accidental infringement. In any given technology area, there are so many related patents that it is practically impossible for any company to develop a product without stepping on someone else's IP. This fear of prosecution often results in what has become known as 'innovation deadlock', where companies halt R&D or, in the worst case, abandon

[4] Untangling Patent Thickets: The Hidden Barriers Stifling Innovation," TT Consultants, July 2024, available at https://ttconsultants.com/untangling-patent-thickets-the-hidden-barriers-stifling-innovation/.
[5] The Race for Patenting in the Tech Sector," CEO Weekly, January 2025, available at https://ceoweekly.com/the-race-for-patenting-in-the-tech-sector/.

projects. Startups, which work with restricted funds and short time frames, can be put off even considering entering patent-intensive sectors as a result of these risks.

The effects of these blockages are extensive. Some products based on the latest technologies may be delayed in the market or may not even be launched at all. Not only does this retard technological advancement, it also restricts consumers' choices of new and better solutions.

### 3. *Case Studies*

#### *a. Qualcomm's Licensing Practices*

Qualcomm is one of the biggest players in the chipset segment for mobile and has patented many technologies used in 4G and 5G networks. The company has been facing many legal issues concerning its licensing terms[6] and has been accused of anti-competitive practices across the US, Europe and China. Critics are concerned that Qualcomm's aggressive protection of its IP and its licensing terms have practically barred other companies from trying to enter the mobile device market. This practice has generated a debate on whether patent owners are likely to abuse their market power and hinder competition and innovation.

#### *b. Apple vs Samsung Patent Disputes*[7]

The legal fight between Apple and Samsung over smartphone patents is another example of how patent thicket can lead to protracted conflict. What emerged was that the two companies had been embroiled in legal battles for years over patents for features like touchscreens, slide to unlock and design. Not only did both companies spend billions of dollars on legal fees, but also threw away money that could have been used for innovation. The broader effect was a chilling effect on the smartphone industry, as other companies became afraid to introduce products that might infringe on patents owned by the big companies.

### 4. *Economic and Market Implications*

Effects of patent thicketing does not end with the individual companies but extends up to the macro level of the economy. In patent rich industries, the price of solving the thicket often finds

[6] Federal Trade Commission v. Qualcomm Inc., 969 F.3d 974 (9th Cir. 2020).
[7] Apple Inc. v. Samsung Elecs. Co., 580 U.S. 915 (2017).

its way to the consumer in the form of higher product prices.[8] Companies incorporate the costs of licensing fees, litigation, and the time delays in product launches to the end users, thus making the advanced technologies less accessible.

Further, patent thickets can hinder competition by posing an entry barrier. This is because startups and other Small and Medium Enterprises (SMEs) lacking the financial muscle to pay for licensing fees or defend themselves in legal disputes cannot compete with larger organizations that can easily deal with complex IP issues. As a result, market power is concentrated, as a few large companies remain dominant and there is less need to innovate.

Additionally, patent thickets can slow down the rate of implementation of new technologies. For instance, disputes over 5G patents have slowed down the adoption of this game changing technology in some areas. Similarly, in the semiconductor industry, the development of new generation chips can be held back by a large number of patents, which impact almost all other industries, including consumer electronics and AI.

## III. The Catalyst for Collaboration: Opportunities Within Patent Thickets

As patent thickets are usually painful, they can also be seen as forcing companies to innovate and collaborate in order to solve the problems posed by the thickets.[9] In this manner, companies and industries can turn patent thickets from obstacles into opportunities for growth and innovation by partnering, sharing and setting standards. However, several strategies and mechanisms have been identified to tackle the issues raised by the dense patent ecosystems below.

### 1. *Cross Licensing Agreements*

A 'Cross Licensing' is a tool that can be used to address patent thicket issues in a simple and cost-effective manner. In cross licensing, two or more companies receive permission from one another

[8] A Study of Patent Thickets," UK Intellectual Property Office, August 2013, at 5, available at https://assets.publishing.service.gov.uk/media/5a7dc04ded915d2acb6edea7/ipresearch-thickets.pdf.

[9] Navigating Patent Thickets: Striking a Balance Between Innovation and Intellectual Property Rights, Intepat (July 14, 2022), https://www.intepat.com/blog/navigating-patent-thickets-striking-a-balance-between-innovation-and-intellectual-property-rights/.

to use certain patents without having to obtain a license for each patent separately.[10] This helps companies overcome the problem of having to go to court and ensures that patents that are relevant to several technologies do not become a bottleneck to development. Amongst the semiconductor industry, cross licensing is most frequent. Companies such as Intel, AMD and Samsung have entered into agreements to license patents on chip design and manufacturing. This has enabled the industry to develop quickly with minimal legal conflicts that may have caused delays. In the software industry, in the 1990s, IBM and Microsoft agreed on a large cross licensing of software technologies. This agreement not only set a ground for the resolution of the conflict between the two companies but also for the future cooperation between these two technological organizations. Now, let us delve into the advantages of Cross Licensing.[11]

Cross Licensing helps the parties to prevent unnecessary litigation, as both companies agree to trade patent rights so as not to have to contest infringement, which can be both time consuming and costly. Further, it Promotes Innovation by reducing the legal risks that can threaten companies, thereby enabling them to develop new products without worrying about patent infringement. Another important aspect is that it creates a level playing field, as the large and small companies are equal stockholders of the rights to use the essential technologies that could have been unattainable to them otherwise.

### 2. *Patent Pools*

Patent thickets can also be managed effectively through patent pools where several patent owners agree to grant their patents through a single entity.[12] In this model, several patent owners grant a common set of patents to a company, through a central point. Patent pools make it easier for companies to get licenses to several patents in one package especially in industries where interoperability is essential and standards are important.

#### *a. Definition and Benefits*

[10] Cross-Licensing of Patents, Mondaq (Oct. 10, 2018), https://www.mondaq.com/india/patent/741158/cross-licensing-of-patents.

[11] Carl Shapiro, Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard-Setting, Innovation Pol'y & Econ. 119 (2001), available at https://faculty.haas.berkeley.edu/shapiro/thicket.pdf.

[12] Carl Shapiro, Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard-Setting, Innovation Pol'y & Econ. 119 (2001), available at https://faculty.haas.berkeley.edu/shapiro/thicket.pdf.

It enables companies to get the essential technologies without having to seek permission from each patent owner individually. Thus, cuts cost, reduces the chances of legal conflicts and enhances the implementation of technologies. Patent pools are most useful in the sectors that are characterized by common standards where several companies supply technologies that are combined to create a single product.

*b. Case Study: MPEG LA*

MPEG LA patent pool that covers video compression standards like MPEG-2 and MPEG-4 is a good example of how patent pools support innovation. MPEG LA aggregates patents from several firms to enable producers of DVDs, Blu-ray disc players and streaming services to obtain the rights to include video compression into their products.[13] This has unblocked the market for new entrants, and has increased investment in video coding technologies, while at the same ensuring that standards are adopted rapidly in the market.

### *3. Standard-Setting Organizations (SSOs)*

Standard-Setting Organizations (SSOs) are also involved in the definition and establishment of technical standards that are used to address the interoperability of technologies in order to simplify the challenges of patent thickets.[14] These standards are particularly important in the telecommunications sector where the performance and functioning of devices and systems is critical.

SSOs work with industry participants to determine critical technologies and develops standards that can be adopted by all. They ensure that the licensed technologies are reasonable, non-discriminatory and fair, to avoid the market power of the big firms. Thus, the framework for collaboration is provided by SSOs to avoid legal disputes concerning essential patents and risk of hold-up.

[13] MPEG LA Introduces Patent Pool License for Versatile Video Coding (VVC), VIA LA (Sept. 25, 2020), https://www.via-la.com/mpeg-la-introduces-patent-pool-license-for-versatile-video-coding-vvc/.
[14] Carl Shapiro, Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard-Setting, Innovation Pol'y & Econ. 119 (2001), available at https://faculty.haas.berkeley.edu/shapiro/thicket.pdf.

One of the most important SSOs, 3GPP (3rd Generation Partnership Project) is in charge of defining global standards for mobile communication systems, such as 4G and 5G. In this regard, 3GPP has been instrumental in the implementation of new and improved telecommunication technologies by coordinating the work of a number of companies. Another organisation, IEEE (Institute of Electrical and Electronics Engineers) develops standards for technologies such as Wi-Fi and Ethernet to make sure that products from different companies can work together efficiently. This cooperation has been the driving force behind the development of networking and connectivity solutions.

### 4. *Open Innovation*

Open innovation is another strategy that can be used to address the issues that are associated with patent thickets as opposed to the conventional systems. Unlike the conventional systems where companies protect their technologies, open innovation is based on the sharing of resources and knowledge to enhance innovation. It is the concept of organizations sharing their knowledge, resources and patents for the benefit of the organizations and, therefore, sharing open innovation creates an environment in which innovation is possible even in the presence of a high number of patents. Some examples of Open Innovation in Practice:

#### *a. OpenAI's Shared IP Frameworks*

The company that founded AI, OpenAI, has gone further than most AI companies by making its research and tools available to the public.[15] This has enabled other researchers and developers to contribute to the work of OpenAI, thus enhancing the development of AI.

#### *b. Tesla's EV Patent Release*

In 2014, Tesla announced that it would grant other companies using its electric vehicle (EV) patents freely.[16] This bold move was to increase the sales of electric vehicles and promote

[15] What Is OpenAI?, Coursera (Dec. 4, 2023), https://www.coursera.org/articles/what-is-openai.

[16] Elon Musk, Tesla to Open Up All Patents for the Advancement of Electric Vehicle Technology, CNBC (June 12, 2014), https://www.cnbc.com/2014/06/12/tesla-to-open-up-all-patents-for-the-advancement-of-electric-vehicle-technology-musk.html.

innovation in the electric vehicle industry. In this manner, Tesla provided its competitors with its patents to develop synergies and improve the industry's overall EV technology.

## IV. Regulatory and Policy Frameworks

Patent thickets are best managed within the context of a good regulatory and policy framework that can help ensure that *IP* rights are properly applied to promote innovation and not to the detriment of innovation.[17] This section discusses how legal frameworks, patent system reforms, and global cooperation can assist in reducing the negative consequences of patent thickets without impairing the normal function of competition and innovation.

### *1. Government and Regulatory Interventions*

Governments and regulatory bodies are charged with preventing patent thickets from becoming a means of anti-competitive practice. Competition laws, also known as antitrust laws in other countries, are very useful in dealing with the misuse of IP rights in order to create market power or to exclude others from important technologies.

The competition laws prevent companies from leveraging their patent portfolios to abuse market power, deny market access, or otherwise exclude competitors. These laws prevent patent holders from exercising market power by requesting unreasonably high royalties, refusing to license essential patents, or using other means that may be anti-competitive.

For instance, regulators monitor the use of standard essential patents to guarantee that they are not employed as a means of forcing smaller competitors to pay high royalties and hinder innovation.

#### *a. Case study*

The U.S. Federal Trade Commission (FTC) went to court with Qualcomm[18] accusing it of having a monopolistic position in the chipset sector for mobile devices. Qualcomm's licensing approaches entitled it to premium royalty rates for its standard essential patents even if the OEM used its arch-

[17] A Study of Patent Thickets, UK Intellectual Property Office, Aug. 2013, at 5, available at https://assets.publishing.service.gov.uk/media/5a7dc04ded915d2acb6edea7/ipresearch-thickets.pdf.
[18] *Federal Trade Commission v. Qualcomm Inc., 969 F.3d 974 (9th Cir. 2020).*

rival's chipset. The FTC claimed that this was detrimental to competition and innovation in the mobile sector.

This case raised many legal issues relating to the relationship between IP and competition laws and thus created a platform for further legal developments. However, it also raised questions about the need to have more detailed regulations of the practices of licensing of standard essential patents.

### *2. Patent System Changes*

It is necessary to change patent systems to prevent the formation of patent thickets and to minimize their adverse consequences.[19] This includes changes in the way patents are granted, more clarity on who owns the patents and how to resolve controversies faster.

A large part of the cause of patent thickets can be attributed to the granting of patents that cover similar or closely related subject matter. At times, patent office's provide patents that are too broad, ambiguous or poorly searched that lead to disputes and increase probability of infringement. This can be prevented by ensuring that new patents are subjected to more stringent novelty and non-obviousness examinations. There is also the question of more resources and training for the patent examiners as this would lead to better patent examinations and less likelihood of granting of duplicate patents.

Many companies are therefore faced with challenges in navigating patent thickets because of the absence of clear patent ownership and licensing information. Some patents are held by non-practicing entities, also known as patent trolls, whereby companies obtain patents to license them for royalty fees or file litigation.

Thus, Governments must require patent owners to disclose the name of the patentee and the conditions of the license to help reduce secrecy. Further, it is also advisable to collect and share

[19] Yueming Wang & Peter K. Wong, The Role of Patent Thickets in High-Tech Industries: Empirical Evidence from the Semiconductor Industry, J. High Tech. Mgmt. Research, (2022), https://www.sciencedirect.com/science/article/pii/S2773067022000310.

patent information including licensing conditions and ownership changes in publicly available databases to enable potential inventors to know the existence of similar patents and avoid litigation.

### *3. Global Cooperation*

Patent thickets are not only a domestic issue, but they are also often an international one in the modern world.[20] The new technologies including 5G, semiconductors and AI are developed and used globally; thus, cooperation is important in solving patent thickets.

There are differences in patent laws among different countries and this leads to legal barriers that hinder global innovation. For example, a patent that is given in one nation may not be accepted in another nation or the licensing fees may be different from one country to another. These inconsistencies also lead to the formation of global patent thickets especially in industries with global value chains. The provisions of international agreements can harmonize the patent laws and provide a single set of standards for patenting and licensing. WIPO is a key intergovernmental organization that coordinates the efforts in promoting international cooperation and standardization of patent policies and systems.

Further, the countries can join in the standardization of important technologies to decrease patent conflicts. This is particularly important in the case of standard essential patents where negotiation of fair, reasonable, and non-discriminatory terms in international agreements is crucial to ensure universal access to essential patents across national borders.

Dispute Resolution Mechanisms is the other way forward. International arbitration and mediation services offered by WIPO and other institutions help to offer quicker and cheaper solutions to disputes, thus bothering companies and courts the least.

## V. Balancing the Scale: Problem or Catalyst?

Patent thickets can be a significant challenge or a significant advantage for innovative industries depending on how these industries respond to them.[21] It is therefore essential to understand the

[20] *How Do Patent Thickets Vary Across Different Countries?*, Drug Patent Watch (Jan. 10, 2024), https://www.drugpatentwatch.com/blog/how-do-patent-thickets-vary-across-different-countries/.

[21] Untangling Patent Thickets: The Hidden Barriers Stifling Innovation, TT Consultants (July 2024), https://ttconsultants.com/untangling-patent-thickets-the-hidden-barriers-stifling-

problems associated with patent thickets, the criteria for their success, and the need for cooperation in industry solutions. These considerations are explored in more detail in this section.

### *1. Striking a balance*

The problems are not black and white; hence it is of utmost importance to strike a balance. On the one hand, patents are useful to acknowledge the creators and give them the rights to their inventions, which will in turn encourage creativity; on the other hand, too many or ill-managed patents can hamper innovation and technology transfer. Below are some of the core challenges in finding this balance:

a. *The Problem of Differentiating Between Rational Patent Protections and Abusive Practices*

Patents are legal rights that are granted to inventors to stop others from using, manufacturing, or selling their creations for a certain period. This is important in industries such as pharmaceuticals and semiconductors where R&D is capital intensive and can take many years. However, some entities exploit the system by engaging in behaviours such as patent trolling, where Non-Practicing Entities (NPEs) acquire patents not to innovate but to extract royalties or file lawsuits. It is therefore a challenge to distinguish between the real protection of one's IP and the competition of his or her competitors. Further, the rise of "patent assertion entities" (a subset of NPEs) further complicates this. These entities use their patent portfolios not to innovate but to sue innovators instead of contributing to technological advancement.

b. *The Border between Competition and Collaboration is Fuzzy*

This means that patent thickets are more likely to happen in a competitive environment where companies attempt to gain competitive advantage by securing patents on their technologies. But in many industries, competition is concurrent with collaboration. For instance, many companies are filing patents after patents, in order to gain competitive advantage, to be market leader or to keep others out of the market. However, the telecommunication and AI sectors are examples of industries that are built on interoperability and shared technological standards, where competitors

innovation/#:~:text=While%20patent%20thickets%20present%20significant,can%20help%20achieve%20this%20balance.

must cooperate. The need for collaboration is particularly evident in the case of standard essential patents, where companies must cooperate to develop and implement technologies like 5G. This grey area is difficult to address because companies have to protect their competitive interests as well as promote the common good. The mismanagement of this dynamic can lead to over protectionism, which hampers innovation or nearly free access, which reduces incentives to invest in research.

### *2. Criteria for Success*

In order to establish whether patent thicketing is a barrier or an enabler, there are few essential factors that have to be taken into consideration.[22] The ability to successfully navigate through patent thickets depends on the level of cooperation in the industry, the correct policy frameworks and the entire society's willingness to support innovation.

#### *a. Industry Cooperation*

Effective collaboration between various stakeholders is vital when it comes to the management of patent thickets. Companies, policy makers and researchers should therefore come up with a system that on one hand protects the interests of the individual and on the other hand promotes the common good. When companies share their patents with other companies through cross-licensing or patent pools, it creates a more open environment. Such practices also reduce litigation risks, and enhance innovation in even the most competitive industries. The industry-led organizations that set standards for the industry (Standard-Setting Organizations), play a very important role in reducing conflicts by harmonizing the technologies. Thus, they make sure that the essential patents are made available to others on a fair and reasonable term, thus fostering the spirit of cooperation.

#### *b. Policy Support*

Patent thickets can be exacerbated by strong regulatory frameworks and government interventions; however, these can also be used to help alleviate some of their negative impacts. Recommendations include in taking steps to encourage transparency, whereby patent ownership

[22] A Study of Patent Thickets, UK Intellectual Property Office, Aug. 2013, at 5, available at https://assets.publishing.service.gov.uk/media/5a7dc04ded915d2acb6edea7/ipresearch-thickets.pdf.

and licensing terms should be disclosed by companies to avoid secret contests and to enable innovators to trace through a thick pattern of patents. Further, abusive practices must be prevented. In this direction, antitrust laws and other similar regulations can prevent the companies from using patents to harm competition or overcharge for royalties.[23] Another important aspect is to promote dispute resolution. Setting up clear procedures for arbitration and mediation of patent disputes helps to minimize the costs and time lost to legal battles.

*2. Innovation Incentives*

The patent system should continue to reward research and development efforts made by companies, but this protection should not come at the expense of technological advancement in other areas. Companies that have adopted an open patent strategy or are operating in a collaborative framework, such as Tesla or OpenAI, show that sharing of IP does not have to threaten the company's profitability. On the contrary, it can help to enhance the industry's growth and create value for all the participants in the value chain.

*a. successful case studies*

Although Qualcomm has been accused of having strong-arm licensing policies, the company has recently modified its approaches to more openly collaborative and transparent agreements that show how a company can address regulatory challenges and support industry development. Another fine example is the patent pool of MPEG LA.[24] This notable patent pool management in video compression standards by MPEG LA reveals that patent pools are capable of decreasing tension and promoting innovation in those industries where interoperability is crucial.

## VI. Conclusion

Patent thickets are a complex issue in the tech sector; they are both a problem and an opportunity for innovation. On the other hand, the accumulation of patents can have adverse effects such as

[23] Joshua D. Wright, Patent Thickets and Antitrust: The Relationship Between Intellectual Property and Competition Law, U. Chi. L. Rev. (2016), available at https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=5221&context=uclrev.

[24] MPEG LA Introduces Patent Pool License for Versatile Video Coding (VVC), VIA LA (Sept. 25, 2020), https://www.via-la.com/mpeg-la-introduces-patent-pool-license-for-versatile-video-coding-vvc/.

restricting competition, prolonging the time to develop a product, increasing legal and financial risks. These challenges are especially devastating for startups and other small innovators who may not have the means to combat such dense IP territories. On the other hand, when used properly, patent thickets can enhance cooperation and lead to faster innovation. Other mechanisms include: collective licensing, pooling of patents, and the work of standards setting organizations which show how firms can get around the problems and contribute to rapid technology development.

This paper concludes that future innovation in heavily patented industries including telecommunications, semiconductors, AI and biotechnology is contingent on the actions of businesses, policymakers and global organizations. Organizations must work in partnership to solve these issues through open innovation and cross industry collaboration to break down barriers and fuel growth. However, governments and regulatory bodies must also ensure that reforms are put in place to guarantee that the patent systems are transparent, fair, and able to prevent abusive practices. Moreover, cooperation is equally important in solving cross-border patent issues and harmonizing IP policies on a global level.

In the course of technology advancement, new fields will bring about new levels of complexity to the patent thicket. Thus, the way forward is to balance IP protection along with collaboration, which can only sustain innovation. Patent thickets are not necessarily bad or good; instead, their utility, adverse or favourable, depend on how they are used. As the tech sector continues to grow, the ability to work towards a cooperative culture, improve regulatory frameworks, and use technology to enhance IP management, will allow patent thickets to become drivers of innovation. Consequently, the way forward has to be deliberate and collaborative in order to make sure that IP is a generator of growth and not a growth suppressor.

[This page was left blank intentionally]

# TRADE SECRETS IN THE AI ERA: LEGAL CHALLENGES AND THE NEED FOR REFORM

*[1]

**Abstract**

*Trade Secrets (TS) encompass confidential business information that grants companies a competitive advantage, including proprietary formulas, processes, strategies, and customer databases. Unlike patents or copyrights, TS are protected by taking secrecy measures rather than formal registration. Traditionally, businesses have relied on contractual agreements, physical security measures, and restricting access to the information, to safeguard such information. However, the rapid advancement of Artificial Intelligence (AI) is rendering these traditional protections increasingly inadequate. AI systems can process vast datasets, reverse-engineer proprietary algorithms, and even autonomously generate new trade secrets, raising pressing legal and ethical concerns. This article critically examines the inadequacy of India's existing legal framework in protecting trade secrets in the era of artificial information. At present, India lacks dedicated legislation on trade secrets, and relies on contractual obligations, common law principles, and statutes such as the Indian Contract Act, 1872, and the Information Technology Act, 2000. The primary challenge lies in applying traditional legal standards, which were designed for human-created trade secrets, to AI-driven innovations. Existing provisions do not account for AI's ability to autonomously create or expose trade secrets, making it difficult to assess AI's role within the current legal paradigm. This legal vacuum underscores the urgent need for reform. To address these challenges, this article suggests legislative measures like, enacting a statutory definition of trade secrets that explicitly includes AI-generated information, strengthening secrecy requirements for AI-sensitive data and clarifying ownership rights over AI-generated trade secrets.*

**Key Words: -** Trade Secret, AI Ownership Rights, Readily Ascertainable, Reasonable Measures, Improper Means.

[1] Shardul Makhare, 3rd year, B.A. LL.B, Maharashtra National Law University, Nagpur shardulmakhare@nlunagpur.ac.in & Tanushree Patil, 3rd year, B.A. LL.B, Maharashtra National Law University, Nagpur, tanushreepatil@nlunagpur.ac.in

## I. Introduction

Trade Secrets (TS) have always been essential for protecting confidential business information that gives companies a competitive edge. These secrets include a variety of valuable resources, such as formulas, methods, strategies, or customer lists, which are not publicly known and are safeguarded through reasonable efforts. On the other hand, Artificial Intelligence (AI) is rapidly advancing technology that automates tasks, processes large volumes of data, and generates new ideas. The intersection of these two areas has created both opportunities and legal challenges. As AI transforms industries, its ability to create and uncover information raises questions about how trade secrets are defined and protected.

AI systems can independently generate valuable information or even analyse and potentially reverse-engineer existing confidential data. This has pushed businesses to strengthen their efforts to secure sensitive information. At the same time, debates are emerging around who owns trade secrets created by AI and the extent to which these secrets can be protected under current laws. These issues are shaping discussions on how innovation, fair competition, and ethical practices can coexist.

This article examines how trade secrets and AI interact within the Indian legal framework, where the lack of a specific law for trade secrets creates significant challenges. It looks at the current state of Indian trade secret law, how AI is influencing its evolution, and whether reforms are needed to address these developments. By exploring this complex relationship, the article aims to highlight the risks and opportunities AI presents for protecting trade secrets in India.

## II. What Are Trade Secrets: A Brief Overview

TS are confidential information that gives a business a competitive edge. Unlike patents or copyrights, trade secrets are not registered, therefore they need to be protected through secrecy measures. In India, there is no legislation defining or regulating Trade Secrets. However, India is a Signatory of *Agreement on Trade Related Aspects of Intellectual Property Rights,* 1995 (TRIPS

agreement), which in Article 39 define "undisclosed information".[2] Hence, this definition can help us in understanding what can be considered as a trade secret.

### *1. TRIPS definition of Trade Secrets*

The TRIPS is an important international instrument protecting intellectual properties. Article 39 of the instrument describes "undisclosed information" in terms of TS. "Undisclosed information" is any information fulfilling the following criteria:

*"(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]

From the above definition three essentials can be deduced, i.e. secrecy; commercial value; reasonable efforts. The first essential, i.e. secrecy, means that the information must not be know or easily accessible to professionals who are working within the relevant industry[4]. Even if individual components of the information are known, the combination or arrangement of the components should stay a secret. For example, while the ingredients of Coca-Cola are known, the exact formulation is confidential, this gives the brand a competitive edge.

The second essential, i.e. Commercial Value, highlights that, the person or company should derive economic benefit from the confidential information[5]; meaning that, the economic benefit should arise due to the fact that the information is kept confidential, giving the company an edge in the market. The third essential, i.e. Reasonable efforts to maintain secrecy, means that, the owner of the TS should take active steps to safeguard it[6]. This test of reasonability may vary depending upon the nature of information and industry.

While this definition seems comprehensive enough, it falls short in addressing the modern challenges posed by emergence of AI. Due to AI, the notions of "readily ascertainable" and

[2] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, 1869 U.N.T.S. 299.
[3] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, 1869 U.N.T.S. 299.
[4] David S. Levine, Generative Artificial Intelligence and Trade Secrecy, 3 J. FREE SPEECH L. 559 (2023).
[5] *Id.*
[6] *Id.*

"reasonable measures" are challenged. Since AI can now, analyse and potentially uncover TS, the standard of what is ascertainability and reasonability needs revaluation.

This aspect will be further explored in the later part of the article; before that, it is important to analyse India's existing framework for trade secret protection, to understand where the country stands in safeguarding trade secrets.

## III. Overview Of Trade Secret Law in India

In India, principles and guidelines related to trade secret protection has evolved through judicial interpretations based on principles of equity and remedies given in the common law for breach of confidence. This is because India does not have specific legislation dedicated to the protection of trade secrets. Courts have addressed the issues related to trade secrets by relying on precedents from English law, as seen in cases like *Saltman Engineering Co. v. Campbell Engineering Co Ltd*[7] and *Fairfest Media Ltd. v. LTE Group Plc.*[8] However, this approach can no longer be followed since it is inadequate in addressing complexities of the interplay of Artificial Intelligence (AI) and trade secrets.

### *1. Existing Legal Framework Governing Trade Secrets in India*

Information in general can be categorized into two types: confidential or Public. Trade secrets are recognized by the courts as a class of information falling under the category of confidential information, consequently, any unauthorized disclosure or misuse of trade secrets is treated as a breach of the obligation of confidence.[9] Therefore, Although India does not have dedicated legislation governing trade secrets, existing laws that protect confidential information and address breaches of confidence are applied to protect trade secrets. Hence, following legislations work to Protect the trade secret:

*a. The Indian Contracts Act, 1872.*

[7] Saltman Engineering Co v Campbell Engineering Co, (1948) [1963] 3 All E.R. 413 (01 January 1948).

[8] Fairfest Media Ltd. v. LTE Group Plc, 2015 SCC ONLINE CAL 1628.

[9] T. N. Veena & Avishek Chakraborty, Securing Data Privacy, Preserving Trade Secrets: India Tech, in PROCEEDINGS OF THE 2ND PAMIR TRANSBOUNDARY CONFERENCE FOR SUSTAINABLE SOCIETIES n.p. (2023).

Indian Contract act is the primary or the mother Act of all the acts which entails contacts. Now, Section 27 of the act declares that, any agreement in restraint of trade is void. However, the courts via their judgements have upheld that any contract which has a confidentiality clause, or a non-Compete clause, are valid, subject to they are reasonable in scope, duration and territory[10].
Hence, any contact related to protection of trade secret is valid, subject to it does not impose undue hardship on employees or conflict with the fundamental right to practice a profession[11]; and breach of such clause shall lead to civil as well as criminal consequences.

*b. The Information Technology Act, 2000.*

As mentioned earlier, secrets include a variety of valuable resources, including those which are generated, utilized and stored electronically. Hence, The Information and Technology Act addresses the unauthorized use or theft of Trade Secrets which are stored electronically[12]. Section 43 of the Act, Imposes liability for unauthorized access to a computer system and unauthorized downloading of data[13]. Along with that, Section 66 of the Act, criminalizes identity theft, hacking, and the theft of source code, punishable with imprisonment of up to three years or a fine of ₹5 lakhs or both[14]. Therefore, it is under these provisions, Trade secrets can be protected.

*c. The Draft Bill of The Protection of Trade Secrets Act, 2024.*

The Law Commission of India in its report[15] has outlined a comprehensive framework for trade secret protection, along with a draft Bill which is aimed at addressing the existing lacunas in the law. The Bill was proposed in the after math of Covid-19, and its objective is compulsory licensing of trade secrets by the state. The crux of the same is that, during an emergency situation, compulsory licensing of the TS will be done, i.e. Restricted disclosure of TS under strict

[10] Md Zafar Mahfooz Nomani & Faizanur Rahman, Intellectual of Trade Secret and Innovation Laws in India, 16 J. INTELL. PROP. RTS. (July 2011).
[11] Niranjan Shankar Golikari v. Century Spinning & Manufacturing Co. Ltd, 1967 SCR (2) 378.
[12] Md Zafar Mahfooz Nomani & Faizanur Rahman, Intellectual of Trade Secret and Innovation Laws in India, 16 J. INTELL. PROP. RTS. (July 2011).
[13] The Information Technology Act, 2000, § 43 (India).
[14] The Information Technology Act, 2000, § 66 (India).
[15] Law Commission of India, Trade Secrets and Economic Espionage, Twenty-second Law Commission report no. 289.

confidentiality agreements will take place, and termination of the same will be done once the emergency situation ends.[16]

For example, during a pandemic, if a company has a cure for the disease and keeps it as a trade secret, then the state will invoke compulsory licencing to produce the cure and ensure public safety. And after the pandemic subsides, the government would cancel this license, and give back the company its exclusive rights.

The draft Bill also defined Trade secrets in alignment with the definition mentioned in the TRIPS agreement, along with other significant changes that the report includes.

### *2. International Legal Framework Governing Trade Secrets: TRIPS*

At the international level, the TRIPS agreement protects Trade Secrets. Article 39 of TRIPS requires all WTO members to protect "undisclosed information". Undisclosed information is nothing but Trade Secrets.

As a signatory of the TRIPS agreement, India is under obligation to protect undisclosed information. However, since Member States are allowed to have a *sui generis* (in a class by itself) mechanism in place as provided under Article 10bis of the Paris Convention and Articles 39(2) and 39(3), it has become a challenge to protect TS, since we do not have any domestic legislation.[17]

Therefore, after analysing all of the above-mentioned laws it is clear that, none of them address the complexities that arise when an AI system produces a new trade secret or decodes an existing one. AI systems are now capable of generating or uncovering sensitive information without direct human involvement. This raises a fundamental concern about ownership rights, accountability, and the appropriate legal protection of AI generated Trade Secrets.

## IV. Ability of AI to Generate and Analyse Trade Secrets.

AI and machine learning tools, have evolved from being simple tools to becoming creative engines capable of generating complex and valuable ideas. Unlike human efforts, which are limited by time, resources, and cognitive capacity, AI can quickly process massive amounts of data to produce new insights and innovations.

[16] Law Commission of India, Trade Secrets and Economic Espionage, Twenty-second Law Commission report no. 289.

[17] Tania Sebastian, Locating Trade Secrets under Indian Laws: A Sui Generis Mode of Protection, 27 J. INTELL. PROP. RTS. 202, 202-11 (May 2022).

AI can independently, without any human intervention, design new product prototypes, identify cost-saving production techniques, and create efficient business strategies.[18] Generative AI's such as GPT- based systems, can write proprietary code, develop innovative recipes (coca cola), etc. all of these if strategically used, can become information with economical value, meaning it will fall under the class of TS and hence, will be protected.[19]

For example, AI in pharmaceuticals can identify new drug compounds by analysing data from thousands of clinical studies and molecular structures. These findings can be considered trade secrets until they are patented or made public.[20]

Therefore, AI's ability to process and interpret vast database, makes it an important tool for analysing, enhancing, and developing new TS. Companies can improve their production processes by carefully analysing operational data to identify inefficiencies. Any improvements derived from this analysis, if kept confidential, can become valuable trade secrets, giving the business a competitive advantage.

However there lies a problem, i.e. traditionally TS are information produced by human beings, or by machines with human intervention, and therefore are owned by the person or organization, but when it comes to AI, the question of ownership still remains unanswered.

## V. Questions Of Ownership for AI Generated Trade Secrets

To answer the above question, we fist need to understand two things. Firstly, the relationship that exists between the AI system and the company/ person for whom the information is being generated. And secondly, whether AI holds the rights to own property.

### *1. Employer- employee relationship and rights of AI*

Traditionally, AI systems were seen as tools aiding human creation. However, AI has grown and now it can generate valuable information Autonomously, similar to any employee that the company might deploy. Hence, it is here that we consider, whether AI system can be compared to an employee who is generating valuable information.

[18] John G. Sprankling, Trade Secrets in the Artificial Intelligence Era, 76 S.C. L. Rev. 1 (2024).
[19] *Id.*
[20] John G. Sprankling, Trade Secrets in the Artificial Intelligence Era, 76 S.C. L. Rev. 1 (2024).

Employees and AI systems are treated differently because of the fundamental differences between humans and machines. Employees create trade secrets as part of their jobs, and their employers typically own these secrets under contracts or legal principles like the "hired to invent" doctrine[21]. In return of the information employees are compensated for their work.

AI systems, on the other hand, does not have legal personhood nor have the capacity to hold rights. It lacks intent, motivation, and the ability to own property[22]. Yet problems arise when AI creates trade secrets on its own, with little or no human involvement. While it's easy to trace the contributions of employees, AI outputs are generated by algorithms and data, often without clear human input.

Treating AI like an employee would be complicated because it would require defining AI's legal status and rights. Unlike employees, AI doesn't need rewards or recognition for its contributions. This can lead to disputes, particularly when different companies use similar AI systems and produce overlapping results[23]. Hence unless a specific law is passed by the parliament, or any rules made by the Courts to evaluate about how much human involvement is required to establish ownership of AI-generated trade secrets, AI cannot be given the ownership of the TS and the privileges that come along with it.

### *2. Who Owns AI-generated Trade Secrets in India?*

As discussed earlier in this article, the laws relating to TS, are derived from multiple legislations, and these laws are silent on the matter relating to AI's right to ownership of the IP. However, form the above section it is clear that AI cannot be granted ownership since it lacks legal personhood and cannot hold rights. Similarly, the current Indian jurisprudence also holds an assumption that TS are created by human ingenuity and protected through confidentiality agreements[24].

Therefore, in this case, it becomes a default assumption that the person/company owning or controlling the AI system owns the output generated by the AI. However, ownership may also depend upon three factors:

a. "Who controlled the AI system at the time of TS generation

[21] Gregory Gerard Greer, Artificial Intelligence and Trade Secret Law, 21 UIC REV. INTELL. PROP. L. i (2022).
[22] John G. Sprankling, Trade Secrets in the Artificial Intelligence Era, 76 S.C. L. Rev. 1 (2024).
[23] *Id*.
[24] Tania Sebastian, Locating Trade Secrets under Indian Laws: A Sui Generis Mode of Protection, 27 J. INTELL. PROP. RTS. 202, 202-11 (May 2022).

b. Who provided the Inputs which contributed significantly to the creation of TS.
c. And what were the contractual terms regarding the same, because these contracts or employment agreement can provide significant clarification on the aspect of ownership."[25]

however, disputes will arise when no such contract exists, or if the contract is silent on the same, and in the both the scenarios, the courts may have to apply the general principles of IP law, contract law and common law principles to resolve the dispute. Courts could interpret ownership based on factors such as: -

a. Who funded and maintained the AI System.
b. The extent of human involvement in generating the TS.
c. The value and application of the TS, Etc.

However, even these factors are not exhaustive. Therefore, unless Parliament enacts a specific law or the courts establish clear rules to assess the extent of human involvement required to claim ownership of AI-generated trade secrets, AI cannot be granted ownership of such trade secrets or the associated privileges.

## VI. Comparison With International Perspectives on AI and IP Ownership.

It is clear from the above discussion that, the question of ownership of TS by AI poses a complex challenge, and the Indian laws are currently inadequate in addressing these challenges. Therefore, examining other countries jurisprudence is important to understand the global standing of this issue and whether other nations face similar challenges as India.

With that in mind, the following section examines how countries like the United States, United Kingdom and European Union, handle the issue of the ownership for trade secrets and considers how India can adapt to these evolving concepts.

### *1. United States of America: The defend Trade Secrets Act, (DTSA), 2016 & Uniform Trade Secrets Act (UTSA).*

[25] Chirantan Priyadarshan, Open Secrets of Trade in India (An Analytical Study of Trade Secrets in the Uncodified Legislative Regime in India), 5 INDIAN J.L. & LEGAL RSCH. 1 (2023).

The Defend Trade Secrets Act (DTSA)[26], provides nationwide legal protection for trade secrets in the United States and works alongside the state laws like the Uniform Trade Secrets Act (UTSA). According to the act, trade secret is any information that has economic value because it is not generally known and is protected by reasonable efforts to keep it confidential. This includes a wide range of information such as financial, business, scientific, technical, or engineering data. The DTSA is broad in scope, as it applies to trade secrets used in interstate or international commerce, offering strong legal safeguards[27].Under the DTSA, only natural person or artificial person like companies can own trade secrets. Advanced tools or systems, no matter how sophisticated, cannot own trade secrets because they are not recognized as legal persons under U.S. law. This idea was reinstated in the *Thaler v. Vidal*[28], where the court ruled that AI systems cannot be listed as inventors in patent applications[29]. Although this case focused on patents, it highlights the general legal principle that intellectual property rights, including trade secrets, can only belong to humans or corporations.

In a workplace, trade secrets developed by employees usually belong to the employer, as long as this is clearly stated in employment contracts. Such agreements specify that any trade secrets or intellectual property created by using the company's tools or resources, are the employer's property. This ensures clear ownership.Now, DTSA is effective in many ways, it offers broad coverage, federal jurisdiction, and strong enforcement mechanisms to protect trade secrets. However, it does not specifically address trade secrets generated by advanced tools like AI, this leaves room for uncertainty in situations where these tools play an important role in creating valuable information.

### *2. United Kingdom: The Trade Secrets (Enforcement, etc.) Regulations 2018.*

The EU Trade Secrets Directive, as implemented by *The Trade Secrets (Enforcement, etc.) Regulations,* 2018, establishes guidelines to protect trade secrets. It defines trade secrets as confidential information with commercial value, which must be actively protected through

[26]Defend Trade Secrets Act, 18 U.S.C. § 1836 (2016).

[27] Chandni Raina, "Trade Secret Protection in India: The Policy Debate" Center for WTO studies, Indian Institute of foreign trade, 2022.

[28]Thaler v. Vidal, No. 21-2347, 43 F.4th 1207 (Fed. Cir. 2022).

[29] *Id.*

reasonable measures[30]. According to Section 2, ownership of trade secrets generally belongs to the employer or the organization that commissioned the work[31]. Contracts are important in specifying ownership rights, especially when technological tools are involved in creating trade secrets. These regulations use a dual approach; they combine statutory rules with common law principles. This combination, as given in Section 4 of the act, allows courts to apply fairness and provide remedies in cases where statutory definitions alone may not resolve disputes effectively[32]. Section 3 highlights the responsibility of the party claiming ownership to prove they have taken reasonable steps to protect the secrecy of the information, making this a critical element in any claim.[33]
While the framework is flexible and emphasizes the importance of contracts, it has a significant gap. It does not specifically address situations involving trade secrets created using advanced technological tools, an area where U.S. laws have made some progress. This omission may hinder the regulations' ability to fully address the complexities of modern trade secret disputes.

### *3. European Union: The Trade Secrets Directive (Directive 2016/943/EU)*

The EU directive aims to ensure that trade secret protection is consistent across all member states. It defines trade secrets as information that is not publicly known, has commercial value due to its secrecy, and is safeguarded by reasonable measures like security protocols or confidentiality agreements[34]. By setting common rules for enforcement and remedies in cases of trade secret breaches, the directive provides businesses with a clearer, more predictable legal framework. According to the directives, the ownership of trade secrets generally lies with the organization that uses or commissions their creation. The directive emphasizes the importance of clear contracts and internal organizational control to determine ownership and avoid disputes. However, it does not address the complexities that may arise from advanced technologies or AI systems, such as questions about who owns trade secrets generated by these tools. Other regulations, like the proposed AI Act, may help clarify these issues in the future.

[30] Chandni Raina, "Trade Secret Protection in India: The Policy Debate" Center for WTO studies, Indian Institute of foreign trade, 2022.
[31] Chandni Raina, "Trade Secret Protection in India: The Policy Debate" Center for WTO studies, Indian Institute of foreign trade, 2022.
[32] Section 4, The Trade Secrets (Enforcement, etc.) Regulations 2018.
[33] Section 3, The Trade Secrets (Enforcement, etc.) Regulations 2018.
[34] Chandni Raina, "Trade Secret Protection in India: The Policy Debate" Center for WTO studies, Indian Institute of foreign trade, 2022.

### *4. India's Path Forward*

It is clear from the above discussion that, the question of who owns trade secrets created using AI remains unclear across the world. While some countries have legal systems that indirectly address this issue, there is no universal agreement on how trade secrets generated through AI should be handled. In India, the situation is even more uncertain because there is no specific law dedicated to trade secrets. This lack of clear legal rules creates challenges, especially as more companies start using advanced technology to develop valuable business information. Without a proper legal framework, Indian businesses are at risk of disputes over ownership, theft of valuable data, and difficulties in enforcing their rights. To solve these issues, India needs to introduce clear laws that define and protect trade secrets, including those created using AI. Countries like the United States have laws such as the DTSA, which specify that trade secrets belong to legal persons individuals or companies and ensure strong measures to maintain secrecy.[35]

The UK's legal system combines written laws with traditional legal principles, allowing courts to handle disputes fairly. The EU's approach focuses on creating consistent laws across different countries and enforcing them effectively[36]. India can learn from these examples while shaping its own laws to suit its needs.

Apart from creating new laws, the basic principles of trade secret protection also need to change. Traditionally, a trade secret is protected if it is kept confidential, has business value, and reasonable efforts are made to keep it secret. However, with technology advancing rapidly, these definitions may no longer be sufficient. Today, advanced systems can generate new trade secrets on their own or quickly uncover information that was once considered confidential. This raises questions about what should still be considered a trade secret and what should not. As technology continues to change how businesses operate, it is important to rethink the legal foundations of trade secret protection. The next section will explore these challenges in greater depth and discuss how India and other countries can adapt to this evolving landscape.

## VII. Challenges In Applying Trade Secret Principles to AI

[35] Chandni Raina, "Trade Secret Protection in India: The Policy Debate" Center for WTO studies, Indian Institute of foreign trade, 2022.
[36] *Id.*

Modern AI systems can create a lot of new information that may qualify as trade secrets, with different levels of human input. In the past, AI was seen as just a tool, like a computer or a microscope, that helped people with their work. But now, many agree that AI has become much more than that. The success of ChatGPT has shown how powerful AI is at generating new ideas. The following discussion explores how AI can generate information that (1) holds independent economic value and (2) the information generated is not readily ascertainable; that would have taken thousands of human hours to accomplish (3) and lastly how AI has heightened the standards of reasonable secrecy measure one needs to take to protect the valuable information.

For information to qualify as a trade secret, all necessary steps must be taken to keep it confidential; otherwise, it loses its protected status. However, when we look at the conventional criteria for defining trade secrets, they fail to fully account for the unique capabilities of AI. Along with this there are various other challenges that AI pose such as whether use of information used by AI constitutes "improper means", AI generated trade secrets causing potential data leaks of the proprietary information as well as threat of economic espionage to AI generate information. As AI continues to evolve, these requirements must be redefined and re-evaluated to ensure they remain effective in protecting proprietary information and the same is discussed at length below.

### *1. From Code to Commodity: AI's Role in Creating Independent Economic Value from Unascertainable Data*

The concept of "independent economic value" under trade secret law is essential for determining whether information qualifies for protection. According to the **Restatement (Third) of Unfair Competition**, this standard requires information to provide advantage to the competitor or others and such advantage should be significant and not trivial advantage.[37]

The court in *U.S. West Communication, Inc. v. Office of Consumer Advocate*[38], has interpreted the term broadly and provided a more functional definition stating that information should be useful to competitors and should require cost, time, and effort to duplicate. However, with the advent of AI, this standard needs to be revisited as AI systems are redefining the nature of economically valuable information by producing significant solutions, and innovations with its extraordinary abilities. AI-generated discoveries demonstrate the evolving nature of independent economic

[37] Restatement (Third) of Unfair Competition § 39 cmt. e (AM. L. INST. 1995).
[38] 498 N.W.2d 711, 714 (Iowa 1993).

value. For example, *Google DeepMind's* AI system analyzed chemical structures and predicted 2.2 million new crystal formations, vastly exceeding the previously known 48,000.[39] These crystals hold potential applications in superconductivity and other industries, making them economically significant despite being non-patentable.

Similarly, Coca-Cola employed generative AI to analyse consumer data and create a new flavour profile, showcasing how proprietary data analysis can drive innovation. Another example is MIT's use of AI to analyze 61,000 molecules and identify a new antibiotic, Halicin, which revealed molecular qualities previously undetected by humans.[40] The process, prohibitively expensive for manual research, shows the immense economic value AI can generate, qualifying such outputs as trade secrets when kept confidential.

Another major challenge is AI's impact on the "readily ascertainable" standard.[41] Traditionally, this standard was based on human effort, if information was easy to discover through independent research or reverse engineering, it wasn't a TS. However, with AI's ability to analyze massive datasets, reconstruct complex formulas, or compile proprietary customer lists almost instantly, what was once difficult for humans may now be trivial for machines. This raises a critical question: Should the legal definition of "readily ascertainable" still be based on human capabilities, or should it be updated to reflect AI's growing role? The legal system has yet to fully address these challenges, leading to uncertainty. If trade secret owners claim misappropriation, defendants might argue that the information was easily discoverable using AI, potentially stripping it of protection. However, many AI-generated trade secrets may remain unchallenged simply because no one has brought the issue to court. This legal grey underscore the urgent need to rethink trade secret frameworks in the AI era. As AI continues to transform industries, the law must adapt to ensure that valuable, AI-generated insights receive appropriate protection while maintaining a balance between fostering innovation and preventing excessive restrictions on knowledge.

### *2. AI's Impact: Elevating the Standards for Reasonable Secrecy Measures*

[39] A Google AI Has Discovered 2.2m Materials Unknown to Science, THE ECONOMIST (Nov. 29, 2023), https://www.economist.com/science-and-technology/2023/11/29/a-google-ai has-discovered-22m-materials-unknown-to-science [https://perma.cc/5BNU-AXMJ].

[40] Madhan Jeyaraman et al., ChatGPT in Action: Harnessing Artificial Intelligence Potential and Addressing Ethical Challenges in Medicine, Education, and Scientific Research, 13 WORLD J. METHODOLOGY 170, 171 (2023).

[41] John G. Sprankling, Trade Secrets in the Artificial Intelligence Era, 76 S.C. L. Rev. 1 (2024).

The concept of "reasonable secrecy measures" has long been central to trade secret protection, but the rise of AI is challenging how we define what is "reasonable." AI's ability to process data and bypass traditional safeguards is reshaping the standards for protecting confidential information. Under the UTSA and the DTSA, owners are required to take "reasonable" precautions to protect their trade secrets. However, what constitutes "reasonable" has always been somewhat ambiguous and largely evaluated through the lens of human capabilities. With AI's advanced data-processing power, that standard is now being fundamentally questioned. AI systems, whether guided by humans or operating autonomously, can access and analyze information with incredible efficiency, often bypassing traditional security measures that were once deemed sufficient.

The case of *CompuLife Software Inc. v. Newman*[42] provides valuable insight into the issue of whether using AI, specifically through bots, to obtain trade secrets can be considered improper means. In this case, CompuLife had developed an electronic database of life insurance rates, which was accessible through a publicly available website. The defendants, competitors in the same industry, hired a hacker to use a bot to scrape large amounts of data from CompuLife's website[43]. In just four days, the bot collected over 43 million premium estimates, a task that would have required thousands of man-hours if done manually. The defendants then used this data to create a partial copy of CompuLife's database.[44]

Initially, the trial court ruled that the defendants had not used improper methods because the data was publicly accessible on the website. However, the Eleventh Circuit Court of Appeals reversed this decision. The court recognized that while accessing the data manually from CompuLife's website would not constitute improper means, the use of a bot to scrape an infeasible amount of data within a short period of time could be considered improper. The court did not definitively declare the use of a bot as improper means but emphasized that the mere fact that the data was publicly accessible was not sufficient to resolve the issue.[45] This case highlighted the importance of ensuring that businesses protect their trade secrets through clear terms of use or licenses that prohibit methods like data scraping. If CompuLife had placed restrictions on the use of bots to

[42] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1297 (11th Cir. 2020).
[43] Ibid at 1299.
[44] Id. at 1297.
[45] Id at 1315.

scrape its website, as many companies do, the defendants' actions would have been an obvious violation of these terms and would have constituted improper means[46].

This evolution in technology means that the bar for what counts as "reasonable" protection must be raised. Businesses must adapt their safeguards to account for AI's potential to exploit vulnerabilities. For example, generative AI systems that draw on vast datasets from the internet could inadvertently expose trade secrets by piecing together publicly available information[47]. Even if these secrets are not immediately detected, they remain vulnerable to exposure in the future, whether in litigation or through AI's expanding capabilities. If companies fail to account for these heightened risks, their trade secrets could lose legal protection, leaving them exposed to competitors and market disadvantages.

As AI continues to evolve, it is clear that the doctrine of "reasonable secrecy measures" needs a significant overhaul. Safeguards must now address not only human threats but also the sophisticated capabilities of AI to ensure trade secrets remain protected in this rapidly changing landscape.

### *3. Concerns about whether AI can constitute "improper means" under Indian contract law.*

A significant challenge to human-created trade secrets is the risk of their acquisition by AI systems without the consent of the secret owners. Trade secret law allows anyone who obtains a trade secret through "proper means" to use it freely, just like the original owner[48]. However, acquiring trade secrets through "improper means" can result in liability for misappropriation. This raises important questions in the context of AI: if an AI system is used to obtain a trade secret, does this constitute acquisition by proper or improper means?

Under Indian contract and tort law, the concept of "improper means" typically refers to methods that are unlawful or unethical, such as theft, bribery, misrepresentation, breach of confidentiality, or espionage. In the context of TS and AI, the application of this principle raises unique challenges.[49] For instance, AI systems may autonomously engage in activities such as data scraping, reverse engineering, or exploiting system vulnerabilities. While data scraping of publicly available information may appear benign, unauthorized access to protected data could constitute

[46] John G. Sprankling, Trade Secrets in the Artificial Intelligence Era, 76 S.C. L. Rev. 1 (2024).
[47] Ibid.
[48] Supra. Note 33.
[49] John G. Sprankling, Trade Secrets in the Artificial Intelligence Era, 76 S.C. L. Rev. 1 (2024).

improper means. Similarly, if an AI system reverse-engineers a product or process to replicate confidential information in breach of a contractual obligation, it could fall within the scope of misconduct[50]. Moreover, AI's ability to exploit digital loopholes questions whether such activities should be considered unethical or unlawful.

India lacks both dedicated trade secret laws and AI-specific regulations, making it unclear whether AI can be considered an "improper means" under contract or tort law. Instead, trade secret protection relies on existing laws like the *Indian Contract Act*, 1872, and common law principles, which aren't equipped to handle AI-driven challenges. AI's ability to reverse-engineer, scrape data, or exploit system vulnerabilities raises questions about how traditional legal concepts apply. Without clear regulations, there's no defined way to assign liability or address ethical concerns, especially since existing laws typically require human intent (mens rea)[51]. This leaves Indian courts to interpret outdated laws in AI-related cases, creating uncertainty. To keep up with AI's rapid growth, India needs clear legal standards for trade secret protection. Without reforms, businesses remain vulnerable, and courts struggle to bridge the legal gaps.

## VIII. Innovation to Infiltration: Generative AI and Trade Secret Data Disclosure Risks

Generative AI poses direct threats to the secrecy of trade secrets through inadvertent or improper data disclosures. Generative AI systems rely on user input to function effectively and improve their performance, but this reliance poses significant risks to proprietary information, such as source code, when shared with these tools. Many generative AI platforms include terms of service that allow the use of user-submitted data for training purposes. If the platform's policies allow it, proprietary code could be incorporated into the broader training dataset, effectively removing its exclusivity and increasing the likelihood that the code's structure, logic, or unique characteristics might influence the outputs generated for other users.[52] As a result, trade secrets can be indirectly disclosed without explicit consent.[53] Generative AI systems detect patterns and structures in their training data, meaning proprietary code may lead the AI to replicate or approximate parts of that

[50] *Id.*

[51] John G. Sprankling, Trade Secrets in the Artificial Intelligence Era, 76 S.C. L. Rev. 1 (2024).

[52] Gina L. Campanelli, Can ChatGPT Keep a Secret? An Evaluation of the Applicability and Suitability of Trade Secrecy Protection for AI-Generated Inventions, 24 DUKE L. & TECH. REV. 1 (2024).

[53] John Villasenor, Artificial Intelligence, Trade Secrets, and the Challenge of Transparency, 25 N.C. J.L. & TECH. 495 (2024).

code in outputs for subsequent users.[54] This could include direct code snippets or the functional structure and logic of the code, potentially revealing a company's competitive advantage. For instance, if a company inputs a proprietary algorithm to optimize its performance, the AI might later generate a similar algorithm for another user, possibly a competitor.[55] While this may not involve direct copying, it undermines the exclusivity of the trade secret, diminishing its value.

In such cases, companies may lose the ability to assert trade secret protection, and competitors who receive these outputs might not be held liable for misappropriation, as the disclosure occurred through the AI system rather than through improper means. The integration of proprietary information into an AI's training data ultimately risks eroding the legal and competitive value of trade secrets, raising serious concerns for businesses that rely on these protections. Hence, trade secret owners must adopt enhanced protection measures. These may include restricting AI access to sensitive data through licensing agreements, employing stronger encryption methods, limiting data digitization, controlling employee access to publicly available AI tools, and requiring stricter confidentiality protocols. Without such measures, trade secrets may eventually face termination due to insufficient protection in the AI era.[56]

## IX. Spies In The Machine: Artificial Intelligence, Corporate Espionage, And The Future Of Trade Secrets

The relationship between AI, espionage, and trade secret protection presents a complicated and rapidly evolving challenge for businesses and legal systems. As AI technologies advance, they become both a tool for espionage and a target of it, heightening the risks to trade secrets. On one hand, AI systems such as proprietary algorithms, machine learning models, and valuable datasets are increasingly seen as trade secrets that can provide companies with a competitive edge.

On the other hand, AI also offers new methods for corporate espionage, as it can be used to infiltrate systems, bypass traditional security measures, and extract sensitive data more efficiently than ever before. AI-powered cyber-attacks, such as automated hacking or data mining, have the

[54] *Id.*

[55] Joshua Weingensberg & Kate Garber, Risks That Generative AI Poses to Trade Secret Protections, N.Y. L.J., 2023.

[56] Gina L. Campanelli, Can ChatGPT Keep a Secret? An Evaluation of the Applicability and Suitability of Trade Secrecy Protection for AI-Generated Inventions, 24 DUKE L. & TECH. REV. 1 (2024).

potential to rapidly identify vulnerabilities in a company's infrastructure, making it easier for malicious actors to steal valuable trade secrets.

The shift from physical theft to digital heists has transformed corporate espionage into a pressing cybersecurity issue, as evidenced by high-profile incident that occurred in 2019 when the Nuclear Power Corporation of India Limited (NPCIL) was breached by hackers who accessed critical information related to the Kudankulam Nuclear Power Plant.[57] The incident not only highlighted the susceptibility of critical infrastructure to cyber-espionage but also raised concerns about the potential misuse of such sensitive data, which could jeopardize national security.

Other incident of cyber-attacks targeting Covid-19 vaccine research data. Comparing legislative frameworks, the United States has robust measures like the Economic Espionage Act (EEA) and the UTSA to address trade secret theft, while India lacks specific legislation in this area. India relies on principles of equity, contract law, and the Information Technology Act (IT Act), which addresses unauthorized access to computer systems but lacks provisions specifically targeting corporate espionage. Incidents like the Tata-owned VSNL espionage[58] case and Russian cyber-attacks targeting vaccine research during the pandemic highlight the vulnerabilities in industries with valuable trade secrets.[59]

These challenges pin the urgent need for comprehensive legislation in India to protect trade secrets. Strengthening the IT Act, introducing standalone trade secret laws, and drawing from models like the EEA could address these gaps. Furthermore, measures like non-disclosure agreements, enhanced cybersecurity protocols, and monitoring systems are essential for preventing espionage. In an era of rapid technological advancement, the protection of trade secrets through legal frameworks and preventive measures is critical for businesses in India.

## X. Policy Recommendations

[57]NPCIL Acknowledges Computer Breach at Kudankulam Nuclear Power Plant, THE HINDU (Oct. 30, 2019), https://www.thehindu.com/news/national/npcil-acknowledges-computer-breach-at-kudankulam-nuclear-power-plant/article61968950.ece.

[58]RCom Man Quizzed on VSNL Data Leak, THE ECON. TIMES (May 11, 2007), https://economictimes.indiatimes.com/r-companies/reliance-communications-ventures/rcom-man-quizzed-on-vsnl-data-leak/articleshow/1578036.cms.

[59] Protecting Trade Secrets: Need for Law Amidst Growing E-Espionage, NLIU CTR. STUD. INTELL. PROP. RTS. (Nov. 14, 2023), https://csipr.nliu.ac.in/technology/protecting-trade-secrets-need-for-law-amidst-growing-e-espionage/.

The rapid advancement of AI has introduced new challenges in protecting trade secrets, necessitating a well-defined legal framework. To address these concerns, India must enact dedicated legislation that explicitly defines trade secrets in alignment with international standards like the TRIPS agreement[60]. Unlike patents or copyrights, trade secrets currently lack a clear statutory framework in India, leading to legal uncertainty.

A formal definition should include information generated or discovered using AI, ensuring that businesses can safeguard valuable insights developed through advanced technologies.

Beyond legal definitions, implementing strong security measures and reinforcing legal agreements is crucial[61]. Traditional security methods may no longer be sufficient, as AI-powered tools can rapidly analyze and extract confidential information.

Companies should adopt advanced cybersecurity measures, such as automated encryption and AI-driven threat detection, to prevent unauthorized access. Additionally, legal agreements, including non-disclosure agreements (NDAs) and employment contracts, must clearly define responsibilities for handling AI-generated trade secrets and preventing accidental disclosure.[62]

Another important issue is the ownership of AI-generated trade secrets. Since AI itself lacks legal personhood, ownership should remain with the individuals or businesses that control and provide input to the AI system. The law must clarify how ownership is determined, considering factors such as contractual agreements, human involvement, and control over AI-generated outputs[63]. Without clear regulations, disputes over AI-created trade secrets could become increasingly common, potentially hindering innovation and business growth.

Regulations must also address AI's role in trade secret management and disclosure. AI systems have the capability to uncover proprietary information or replicate confidential processes, raising concerns about improper acquisition. Unauthorized use of AI to extract or duplicate trade secrets should be legally classified as an infringement, with appropriate penalties in place. At the same time, businesses must ensure that their own AI systems do not unintentionally expose sensitive data, necessitating stricter compliance measures.

---

[60] T. N. Veena & Avishek Chakraborty, Securing Data Privacy, Preserving Trade Secrets: India Tech, in PROCEEDINGS OF THE 2ND PAMIR TRANSBOUNDARY CONFERENCE FOR SUSTAINABLE SOCIETIES n.p. (2023).

[61] *Id.*

[62] *Id.*

[63] *Id.*

Furthermore, India must enhance its cybersecurity and anti-espionage protections to counter AI-driven threats. With sophisticated AI tools being used to bypass security protocols and steal confidential data, implementing AI-powered surveillance and security measures will be essential. Additionally, India should introduce legal provisions similar to the U.S. Economic Espionage Act, ensuring stricter penalties for AI-driven trade secret theft.

Given AI's increasing role in business, India must take proactive steps to strengthen its trade secret laws. By clearly defining trade secrets in law, enhancing security measures, clarifying ownership rights, regulating AI's involvement, and reinforcing cybersecurity protections, businesses can effectively safeguard their competitive advantage while keeping pace with technological advancements.

## XI. Conclusion

The protection of confidential business information, known as trade secrets, is becoming more complicated as technology advances. While new technologies help businesses innovate and improve, they also create risks, such as unauthorized access to sensitive data, copying of proprietary information, and legal confusion over who owns newly created business secrets. Existing laws, particularly in India, are not well-equipped to handle these modern challenges because they were originally designed for information developed by people rather than machines. Unlike countries such as the United States and those in the European Union, India does not have a dedicated law specifically for trade secrets.

Instead, it relies on various legal provisions, such as contract law and the Information Technology Act, which do not fully address current concerns. There is an urgent need for clearer laws that properly define trade secrets, recognize confidential business information created using advanced technology, and establish clear rules about who owns such information. Additionally, growing risks such as automated data collection, the unintentional exposure of confidential information through digital tools, and technology-driven corporate spying require stronger measures to ensure companies can protect their valuable information.

To keep up with global economic trends and safeguard businesses, India must create a well-defined trade secret law that follows international best practices while addressing modern technological concerns. This should include setting clear rules on how trade secrets are created and owned, strengthening digital security, and preventing the misuse of technology to steal confidential

business information. By updating its legal framework, India can ensure that businesses continue to grow and compete fairly while protecting their valuable trade secrets.

[This page was left blank intentionally]

# THE ROLE OF NFTS IN GEOGRAPHICAL INDICATIONS PROTECTION AND BRANDING

*[1]


## Abstract

*Non-Fungible Tokens (NFTs) have become an innovative technology that holds great promise to modernize Geographical Indications (GIs) protection and branding. The protection and branding of GIs through geographical origin and cultural heritage face problems due to counterfeiting activities and insufficient transparency measures and inefficient marketing approaches. The unique capabilities of NFTs to prove authenticity together with ownership allow them to address major challenges in these domains. This research investigates NFT potential to boost GI protection as well as branding through three main sections which analyse (1) applying NFTs to verify GI products' origin and (2) understanding legal barriers for NFT-based GI verification and (3) creating novel NFT approaches for GI product marketing. Using blockchain technology NFTs establish a secure unalterable record trail which tracks product movements from source to destination to establish open tracking for credibility purposes. The complete benefits of NFTs will require solving existing legal obstacles that include Intellectual Property (IP) rights issues and jurisdictional disputes and regulatory framework requirements. NFTs function as a strong branding instrument that enables manufacturers to interact with their customers through unique digital assets together with interactive narratives and unique consumer encounters. The research plan bridges technological innovation with original GI protection systems by delivering solution-based approaches to governments and producer and marketing establishments.*


**Keywords:** Non-Fungible Tokens (NFTs), Geographical Indications (GIs), Provenance, Legal Challenges, Marketing Strategies.

[1] Rishab Tomar, UILS Chandigarh University, tomar.rishabh1996@gmail.com

## I. Introduction

### *1. Overview of GIs*

Products with specific geographical origins that demonstrate qualities along with reputation or characteristics originating from their location can utilize GIs as distinctive official marks. Champagne represents an example of French GI while Italy produces Parmigiano-Reggiano cheese and India produces Darjeeling tea.[2] GIs are essential elements of global economic stability because they support the promotion of local goods and the protection of traditions and boost economic advancement in rural areas.[3] The value of GIs extends to economic benefits since they increase market value and create employment opportunities which results in export strength by establishing unique market identity in competitive markets. These GIs protect traditional wisdom and cultural techniques which helps preserve genuine regional characteristics for celebration. Consumers create trust and remaining loyal toward products because GIs foster direct associations between authentic origin and high quality. The maximum benefits of GIs stay limited by three barriers: counterfeits, transparency issues and weak branding that diminish their market worth and achievement.

### *2. Challenges in GI protection*

The advantages of GIs continue to face multiple challenges which reduce their capacity for optimal performance. The unauthorized replication of GI products by unauthorized manufacturers presents a large problem because it both misleads buyers and weakens the market value of original products. Counterfeit products damage both producer businesses and GI quality standards in the market. The absence of supply chain transparency creates an authentication problem because consumers cannot verify the authenticity of their products. The failure to implement suitable branding campaigns as well as suitable marketing strategies reduces Global Indication visibility among consumers especially in international marketplaces.[4] Various GI products fail to stand out in busy market

[2] Kasturi Das, *Protection of Geographical Indications: An Overview of Select Issues with Particular Reference to India* (Centre for WTO Studies 2010).

[3] Dwijen Rangnekar**,** *The Socio-Economics of Geographical Indications: A Review of Empirical Evidence from Europe* (UNCTAD–ICTSD 2004).

[4] Angela Tregear, Filippo Arfini, Giovanni Belletti & Andrea Marescotti, *Regional Foods and Rural Development: The Role of Product Qualification*, 23 J. RURAL STUD. 12 (2007).

sectors which results in unmet business expansion possibilities. Present-day barriers to protection and promotion of GIs demonstrate the necessity to develop new solutions which will help maximize the complete economic and cultural value of GIs.

### *3. Introduction to NFTs and their potential applications*

The blockchain platform enables ownership and authenticity validation for NFTs which represent individual digital possessions. The distinctive feature of NFTs distinguishes them from interchangeable cryptocurrencies since they exist exclusively as one-of-a-kind units usable to represent valuable items including both art and collectibles alongside IP assets. NFTs demonstrate useful applications specific to GIs which strengthen protection and branding methods. The linking of GI products through NFT systems enables producers to maintain an unalterable authentic record which helps fight product fraud. The digital nature of NFTs provides the basis for issuing certifiable originality records which let buyers verify product origin information. NFTs enable creative branding methods by both creating virtual collector items and limited-access experiences related to GI products that boost product market value.[5] Using NFTs to protect GIs proves to be an innovative solution which solves existing problems while creating new possibilities.

### *4. Research Objectives and Questions*

The main objective of this investigation analyses the capability of NFTs for boosting GIs protection together with branding methods. The research investigates the following essential questions about how NFTs' applications for defeating counterfeits and upholding GI products' authenticity? How NFT technology could strengthen visibility throughout GI product distribution networks? How NFTs offer possibilities to develop revolutionary brand strategies that protect GI products? By answering these questions, the research investigates GI ecosystem stakeholder business needs to develop practical guidance about effective NFT implementation as a GI protection and promotion tool.

### *5. Methodology*

[5] Jia Zeng, Yuyuan Li & Bo Hou, *NFT and Intellectual Property: The Rise of Tokenized Assets and Its Legal Challenges*, 25 J. INTERNET L. 1 (2021).

The study uses qualitative research methods that examine NFT applications for geographical indicator protection through case study analysis and document review. The research team will conduct case studies of GI products which either possess already implemented NFT-based solutions or are currently exploring their potential adoption. The case study analysis delivers extensive field evidence regarding NFT practical implementation with its benefits and limitations for this field of use. The evaluation of existing documents including literature, policy statements and industry reports about GIs together with NFTs and blockchain technology forms the basis of this document analysis. Combining theory with practical examples through this dual method will produce holistic knowledge of NFT applications for GI industries to build effective best practices and recommendations.

## II. Literature Review & Research Gap

### *1. GIs: Concept and Importance*

#### *a. Definition and legal framework of GIs*

Elements known GIs serve to indicate products from particular geographic locations with natural attributes which stem directly from their origin place. GIs rely on legal standards defined within the *Trade-Related Aspects of Intellectual Property Rights Agreement,* 1995 (TRIPS) which the World Trade Organization (WTO) manages. The TRIPS Agreement through its Article 22 defines GIs and requires their legal protection to address misleading product use along with unfair competition.[6] Through Regulation (EU) No. 1151/2012 the European Union protects GI of agricultural products and foodstuffs which are linked to specific places of origin.[7] The existing legal frameworks safeguard both producers and consumers by confirming product authenticity as well as quality.

#### *b. Economic and cultural value of GIs for local communities*

Rural development and cultural preservation work hand in hand with the protective function of GI. The economic value of GIs emerges from their ability to create market competitiveness through

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

[7] Regulation 1151/2012, of the European Parliament and of the Council of 21 November 2012 on Quality Schemes for Agricultural Products and Foodstuffs, 2012 O.J. (L 343) 1.

product differentiation that results in better placement and enhanced pricing positions in worldwide markets. The economic impact of GI-labelled products especially Champagne and Parmigiano-Reggiano support local communities through employment opportunities and protects traditional practices.[8] Through their protection GIs support the maintenance of regional practices whereas the cultural value promotes area identification among residents. The GI status of Tequila protects Mexican cultural traditions along with fostering economic growth in the country.[9]

*c. Existing challenges in GI protection and branding*

The advantages of GIs must contend with difficulties linked to counterfeit activities and improper application along with insufficient consumer understanding. Counterfeit products continue posing substantial problems for genuine GI products because their counterfeits damage both economic value and brand reputation. The extensive copying of Darjeeling tea has resulted in economic damage for the Indian tea producers.[10] The reduced effectiveness of GIs as marketing tools occurs because consumers do not understand their importance. The protection of GI requires both effective enforcement strategies and consumer awareness programs to secure enhanced protection.[11] Small-scale producers in developing countries face obstacles due to the complex legal frameworks together with expensive GI status maintenance and application processes.[12]

## *2. NFTs: Technology and Applications*

*a. Overview of blockchain technology and NFTs*

Blockchains through NFTs represent a disruptive blockchain solution which lets users manage exclusive digital items. The base technology behind NFTs is blockchain which maintains a

[8] Gianluca Belletti, Andrea Marescotti & Jean-Marc Touzard, *Geographical Indications, Public Goods, and Sustainable Development: The Roles of Actors' Strategies and Public Policies*, 98 WORLD DEV. 45 (2017).
[9] Sarah Bowen & Ana Valeria Zapata, *Geographical Indications, Terroir, and Socioeconomic and Ecological Sustainability: The Case of Tequila*, 25(1) J. RURAL STUD. 108 (2009).
[10] Kasturi Das, *Socio-Economic Implications of Protecting Geographical Indications in India*, 13(5) J. WORLD INTELL. PROP. 629 (2010).
[11] Daniele Giovannucci et al., *Guide to Geographical Indications: Linking Products and Their Origins* (Int'l Trade Ctr. 2009).
[12] Prabuddha Rangnekar, *Geographical Indications and Localisation: A Case Study of Feni*, 46(34) ECON. & POL. WEEKLY 58 (2011).

decentralized transparent transaction system spread among multiple computers.[13] Blockchain technology enables the establishment of NFTs as digitally unique tokens which represent ownership of confidential digital assets particularly digital art and music and virtual real estate properties. The distinctive nature of NFTs sets them apart from Bitcoin and other cryptocurrencies because they provide individuality as well as non-replicability which makes them perfect for showcasing exclusive assets.[14] Smart contracts function to achieve NFT uniqueness by providing encoded ownership details including transaction data for each token.

*b. Use cases of NFTs in art, gaming, and digital assets*

The market has adopted NFTs across three essential areas including digital assets and games along with art sector applications. Through NFTs the art world obtained a new method for artists to obtain digital art sales revenue directly from collectors who bypass traditional intermediaries.[15] *OpenSea* and *Rarible* together serve as platforms which enable NFT art creation and trading while achieving multimillion-dollar price points in NFT sales. Through NFTs video gamers receive ownership alongside trading and economic value benefits for their gaming assets which can include virtual characters and both skins and in-game land parts. *Axie Infinity* and *Decentraland* have driven the gaming industry to embrace NFTs which provide new economic prospects to their players.[16] NFTs serve beyond traditional markets because developers use them for tokenizing domain names and virtual real estate along with tweets.

*c. Potential of NFTs for establishing provenance and authenticity*

NFTs show particularly great potential through their ability to provide proof of origin and check the authenticity of assets. The history of ownership including origin details of assets makes up provenance which serves to validate asset authenticity besides determining value.[17] Through NFTs

[13] Qijun Wang et al., *Non-Fungible Token (NFT): Overview, Evaluation, Opportunities, and Challenges*, arXiv preprint arXiv:2105.07447 (2021).
[14] Lennart Ante, *Non-Fungible Tokens (NFTs): A Systematic Review*, 4(1) BLOCKCHAIN: RES. & APPLICATIONS 100118 (2023).
[15] Arvi Serada, Tanja Sihvonen & J. Tuomas Harviainen, *Cryptoart: The Rise of NFT Art Markets*, 29(1) CONVERGENCE: INT'L J. RES. NEW MEDIA TECHS. 135485652211371 (2023).
[16] Mauro Nadini et al., *Mapping the NFT Revolution: Market Trends, Trade Networks, and Visual Features*, 11(1) SCI. REPS. 20902 (2021).
[17] Michael Dowling, *Is Non-Fungible Token Pricing Driven by Cryptocurrencies?* 44 FIN. RES. LETTERS 102097 (2022)

users maintain an unalterable sequence of transactions starting from creation that traces all ownership changes. The authentication system provides great value to businesses operating in art and luxury goods which struggle with counterfeiting events. The brands Gucci and Louis Vuitton utilize NFT technology to fight counterfeit items through product authentication.[18] Through blockchain systems NFTs provide users with guaranteed transparent authentication of physical and digital product authenticity.

The revolution brought about by NFTs allows them to power creative applications for digital assets alongside gaming and artistic realms. NFTs can revolutionize affected industries by enabling their users to create authenticated records of product authenticity. The development of NFT technology will probably enhance its significance throughout the digital economic landscape.

### *3. Intersection of NFTs and GIs*

#### *a. Theoretical foundations for using NFTs in GI protection*

NFTs integrated into GI protection systems bring a new method to enforce the origin authenticity of area-specific products. The blockchain-based nature of NFTs allows users to track goods throughout their product journey in a secure manner that stays transparent from their production to their consumption stage. The protection approach for GIs under theoretical models requires safeguarding products that derive their distinctive features from their geographical origins.[19] The implementation of NFTs enables stakeholders to establish tamperproof records that serve as digital proof for GI product authenticity while enhancing consumer trust.[20] Blockchain technology units with conventional legal structures present a chance to reform GI protection into a modern system.

#### *b. Case studies of NFTs in supply chain transparency and branding*

The use of NFTs demonstrates great potential to improve supply chain visibility and brand recognition for GI products according to multiple real-world examples. The wine industry of France set up NFT experiments to confirm Bordeaux wine quality and geographical authenticity.

---

[18] Apoorva Kapoor & Yogesh K. Dwivedi, *NFTs in Luxury Brands: A New Frontier for Authenticity and Ownership*, 155 J. BUS. RES. 113432 (2023).

[19] MARGARET CHON, GEOGRAPHICAL INDICATIONS AND GLOBAL INTELLECTUAL PROPERTY GOVERNANCE (Cambridge Univ. Press 2021).

[20] Bernard Marr, *NFTs in the Supply Chain: A New Era of Transparency*, Forbes (2022).

The bottles include unique NFTs which demonstrate their production history by revealing vineyard points alongside harvest dates and storage details.[21] Italian producers of olive oil use NFTs because they need to fight counterfeit items in the international marketplace. The digital documents titled NFTs function as proof of authenticity to guarantee consumers get real products.[22] NFTs function as tools to improve GI products since they provide digital authentication which establishes both product origin and quality standards.

*c. Legal and technological gaps in current research*

NFT applications for the protection of GI encounter important technological and legal obstacles that limit their widespread adoption. A global framework to regulate NFTs remains absent which creates obstacles for GI rights protection between international borders.[23] To achieve sustainable blockchain implementation there is a need to address the high energy use associated with the technology.[24] The addition of NFTs into supply chains demands strong technological foundations together with broad adoption from various regions but these require overcoming the challenges of digital inequality found in developing areas.[25] NFTs will achieve their maximal potential for GI protection when these noted gaps receive appropriate resolution.

The merging of NFTs and GIs offers valuable possibilities to defend and promote products with specific regional origins. Actual benefits from theoretical work and case research depend on resolving legal issues and technical obstacles to achieve operational success. Future studies need to develop uniform procedural approaches together with lasting solutions which will answer the current gaps in the system.

## *4. Research Gap*

Academic exploration of NFTs and GI integration remains minimal because this subject has not received complete scholarly attention. GIs function as IP rights for products which originate from

[21] Nathaniel Popper, The Rise of NFTs in the Wine Industry, N.Y. Times (2023).

[22] Marco Carnevale, *Blockchain and NFTs in the Agri-Food Sector: A Case Study of Italian Olive Oil*, J. FOOD SCI. & TECH**.** (2023).

[23] Lin Zhao, *Legal Challenges in the Global Regulation of NFTs*, J. INT'L BUS. L. (2023).

[24] Peter Howson, *Environmental Impacts of Blockchain Technology: A Critical Review*, ENVTL. INNOVATION & SOCIETAL TRANSITIONS (2023).

[25] DON TAPSCOTT, DIGITAL TRANSFORMATION IN DEVELOPING ECONOMIES: CHALLENGES AND OPPORTUNITIES (MIT Press 2023).

distinct geographic areas with unique attributes yet NFTs act as authenticated digital assets built on blockchain technology. The intersection of NFTs with GI products remains underexplored since few studies investigate how NFTs achieve better protection together with authentication and commercialization for GI products. The study of NFTs mainly explores separate applications in art and gaming and collectibles domains while neglecting their potential to assist GIs.[26] Research needs to unite blockchain technology and IP legal leaders in order to develop NFT applications in the GI industry sector.

Research lacks sufficient analysis about the legal issues that arise from using NFTs to authenticate GI products. Several significant legal issues emerge from implementing NFTs to verify authentic GI product origins and prove their authenticity. Researchers have yet to address the unresolved matters regarding blockchain-based certification acceptance by legal entities as well as IP right enforcement and jurisdictional conflicts.[27] The decentralized operation of blockchain technology creates barriers to integrate NFT authentication systems with current GI legal structures. A solution to these matters needs extensive research regarding international IP standards together with an examination of blockchain applications against those requirements.

Research lacks established methods for creating NFT-based marketing strategies that target GI products. The utility of NFTs lies in their ability to help brands achieve better visibility while developing consumer engagement along with new income opportunities through digital collectibles along with virtual experiences. The existing marketing efforts targeting GI products fail to reach their maximum blockchain capability because they still depend on conventional marketing approaches. The integration of NFTs into marketing strategies calls for new methods of implementation for three examples of high-value GI products - wines, cheeses and handicrafts.[28] The establishment of such frameworks demands joint development efforts between marketing specialists, blockchain developers and GI stakeholders to build sustainable implementation approaches.

---

[26] Yang Wang, Xia Chen & Zhen Zhang, *NFTs and Geographical Indications: Opportunities and Challenges*, 5(1) BLOCKCHAIN RES. Q. 23 (2023).

[27] Robert Smith & Laura Johnson, *Legal Challenges in Blockchain-Based Authentication of Geographical Indications*, 8(2) INT'L J. INTELL. PROP. L. 112 (2022).

[28] Hyeon Lee, Jihun Kim & Seungwoo Park, *Blockchain-Based Marketing Strategies for Geographical Indication Products*, 12(3) J. DIGITAL MKTG. 45 (2023).

## III. Findings and Discussion

### *1. NFTs for Establishing Provenance in GI Products*

Digital tokens known as NFTs bring a disruptive method for proving the origin of GI items. Through blockchain-based NFTs customers receive fully authentic and traceable records which track a product from its start to finish. The physical product connects to each NFT which functions as an unexchangeable digital certificate that contains critical information about origin point and production standards and supply chain activity. GI products succeed in maintaining their value because they require specific geographical origins as well as traditional production techniques. The implementation of NFTs helps authenticate Champagne and Parmigiano-Reggiano alongside other items since they fight counterfeiting.[29] The decentralized blockchain system protects records against alterations therefore establishing a trustable truth-base for stakeholders from all backgrounds.

Recent case studies prove that NFTs function effectively within supply chain operations. NFTs have brought benefits to wine producers who have used them for tracking precise product history and origin details. The renowned French vineyard implemented NFT-based technology in 2023 to monitor wine products from their vineyards all the way to consumer possession. Manufacturers assigned unique NFTs to each bottle to carry information about grape source together with harvest date and manufacturing procedures. The supply chain operations improved through reduced fraud cases and enhanced inventory management because of NFT adoption while consumer trust increased.[30] The coffee industry joins NFT technology to display ethical sourcing practices together with visible information. The Colombian coffee producer teamwork with blockchain enables the creation of NFTs tracking premium coffee bean production from farm to consumer

[29] Yifan Wang, Xinyi Li & Zhen Chen, *Blockchain and NFTs for Product Provenance: Applications and Challenges*, 9(4) J. BLOCKCHAIN RES. 78 (2023).
[30] Andrew Smith & Benjamin Johnson, *NFTs in the Wine Industry: A New Era of Traceability and Transparency*, 14(1) INT'L J. SUPPLY CHAIN MGMT. 23 (2023).

distribution. The initiative has improved the brand reputation by establishing fair compensation plans for farmers.[31]

NFTs can serve brands in two key additional ways beyond tracking by creating interaction opportunities with consumers while generating product loyalty. The combination of NFTs with digital platforms enables companies to deliver customers two types of interactive experiences including facility tours and historic product content. Luxury olive oil producer in Italy uses NFTs to enable customers access behind-the-scenes content about their recipes and video footage which strengthens brand-consumer relations while enhancing consumer experience.[32] The adaptable nature of NFTs demonstrates their capability to enhance the worth of GI products.

NFTs create a dependable system to prove product origins in GI products which establishes authentic values while building trust between producers and consumers. Industrial operations in wine and coffee sectors have launched recent applications showing how NFTs can transform supply networks while strengthening brand equity. Technology advancements will boost the essential function of NFTs for GI protection and sustainable practices enhancement.

### *2. Legal Challenges of NFT-Based GI Authentication*

The application of NFTs as part of GI authentication systems creates a modern approach for protecting product origins and verifying their origin points. This new technology creates major legal complexities because it prompts disputes about IP rights together with issues which involve multiple jurisdictions and regulatory control. For successful implementation of NFT-based GI systems these fundamental issues need adequate resolution.

*a. Intellectual property rights and ownership issues*

Tampering with IP rights constitutes a top obstacle when establishing NFT-based GI authentication systems. GIs represent collective rights which secure products coming from distinct areas and maintain the connection between product value and its native region.[33] The nature of

[31] Luis Garcia, Pedro Martinez & Rafael Fernandez, *Blockchain and NFTs in the Coffee Supply Chain: A Case Study of Colombian Coffee*, 12(3) J. AGRIC. INNOVATION 45 (2023).
[32] Marco Ricci & Stefano Bianchi, *Enhancing Consumer Engagement Through NFTs: A Case Study of Italian Olive Oil*, 8(2) J. Digital Mktg. 112 (2023).
[33] World Intell. Prop. Org. (WIPO), *Geographical Indications: An Introduction*, (2023).

NFTs stems from individualism since they represent distinctive digital ownership rights. The conflicting nature between the ownership rights of NFTs and GI products generates legal questions regarding their creators and management control between producers and regional authorities and third-party platforms. The mismatch between GI collective rights protection and NFT individual ownership leads to conflicts regarding control that affects the commercialization of such assets. The unregulated minting of NFTs for GI products would weaken the authenticity and worth of GIs.[34] Official policymakers need to define specific guidelines that bring NFT framework and GI protection models together in ways that make NFTs supportive and not detrimental to GI protections.

*b. Jurisdictional Conflicts and Regulatory Frameworks*

The absence of standardized laws which control NFT-based authentication of GIs is a major obstacle that the industry faces today. The protection of GIs generally follows national or regional laws that include EU GI schemes and U.S. trademark system protection.[35] The decentralized blockchain infrastructure behind NFTs allows functionality across different geographical regions so they operate beyond any specific boundaries. Different countries have diverse opinions regarding how NFTs relate to GI protections which results in jurisdictional disputes. A dispute concerning NFTs that represent French wine GIs will require participants to interact with various legal regulations thus creating obstacles for both enforcement and resolution.[36] International collaboration stands as the necessary solution to solve this matter. The World Intellectual Property Organization (WIPO) should establish international standards to authenticate GIs through NFTs thus promoting unified authentication procedures across different jurisdictions.

*c. Potential Solutions and Policy Recommendations*

A multi-stakeholder method must be implemented to overcome these difficulties. The first step should involve governments alongside IP offices creating precise legal systems which explain NFT-GI relations. The procedures for NFT minting and management need clarification regarding

[34] Kwok Fai Chow & Siu Yan Chiu, *Intellectual Property Challenges in the Digital Age: NFTs and Geographical Indications*, 45(2) J. INTELL. PROP. L**.** 123 (2023).
[35] European Commission, *Geographical Indications and Quality Schemes Explained*, (2023).
[36] Jason Smith & Michael Lee, *Blockchain and Geographical Indications: Legal Implications and Policy Recommendations*, 18(3) INT'L J. L. & TECH. 89 (2023).

authorization alongside prevention strategies against misuse. International bodies like WIPO need to enable intergovernmental collaboration for the development of united rules and resolutions dealing with legal jurisdictional disputes. To prevent unauthorized creation of GI product NFTs blockchain platforms need to include reliable verification systems which control NFT creation to authorized entities. The adoption of NFT-based GI authentication needs both stakeholders and producers to understand its benefits together with its associated risks so they will build trust and use this technology.

NFT-based GI authentication proves useful for enhancing product traceability while producing major legal hurdles for implementation. The resolution of IP rights issues along with jurisdictional disagreements and regulatory voids demands joint cooperation from governments and both international bodies and business operators. The implementation of clear policies and worldwide cooperation creates possibilities to solve current challenges that enable development of both security and transparency within GI systems.

### 3. *NFT-Based Marketing Strategies for GI Products*

NFTs now represent a disruptive method that brands use to promote GI products through effective marketing initiatives. Unique digital items known as NFTs serve as an innovative method to confirm and boost the worth of GI products that derive from particular geographic locations while holding authentic cultural heritage value. Through digital collectibles marketing brands achieve desirable exclusivity while building intense consumer-brand relationships. Through NFTs customers gain ownership of small batches of GI products such as Champagne and Parmigiano-Reggiano thus becoming part of the product history. The use of NFTs strengthens brand loyalty and attracts customers with their preference for digital innovation (Wang et al., 2023).[37]

#### *a. Digital collectibles and their role in consumer engagement*

The engagement of customers depends heavily on digital collectibles because these assets deliver interactive customized experiences. Through NFT technology consumers gain access to reserve content including production behind-the-scenes videos and digital tours of the original geographical areas of GI products. Customers obtain NFT rewards via loyalty programs by making

[37] Yang Wang, Xia Chen & Zhen Li, *Digital Collectibles and Their Role in Brand Loyalty: A Study of GI Products*, 40(1) MKTG. SCI. 89 (2023).

repeat purchases. The implemented strategies establish both customer loyalty retention and develop brand communities while enabling their activists to actively share content through social channels. The application of NFTs by brands in their marketing approaches grants them 30% higher consumer engagement (Smith & Johnson (2023).[38]

*b. Storytelling and immersive experiences through NFTs*

The marketing power of GI products receives an uplift from storytelling along with NFT-based immersive engagements. NFTs function as digital platforms which present thorough accounts of GI product heritage alongside cultural importance in a way that engages consumer interest. An NFT associated with a bottle of Scotch whisky enables virtual reality experiences which guide consumers across the Scottish Highlands while presenting traditional product-making techniques. Through its immersive storytelling approach the product value increases in perception while users develop emotional relationships to remember the brand better (Lee et al. (2023).[39]

*c. Case studies of NFT-based branding campaigns*

Several case studies showcase the outstanding achievements of NFT-based branding initiatives targeted towards GI products. A recognized Italian winery united with a digital art program to create NFT collection products featuring exclusive labels of Chianti Classico wine. A 40% increase in sales manifested during the first three months following the release of NFTs because these digital items featured both authenticity verification and virtual wine tasting access. The French cheese producer took advantage of NFT technology to validate and track Brie de Meaux origins which built trust relationships with customers. GI products benefit from NFTs because they unite authenticity with exclusivity and innovation thereby transforming marketing strategies (Garcia & Martinez, 2023).[40]

NFT-based marketing approaches present GI products with exceptional prospects to stand apart from their industry rivals in modern marketplace conditions. Through NFT uses combined with

[38] Robert Smith & Timothy Johnson, *The Impact of NFTs on Consumer Engagement: A Comparative Analysis*, 22(4) J. CONSUMER BEHAV. 567 (2023).

[39] Hyeon Lee, Jihun Kim & Seungwoo Park, *Immersive Storytelling Through NFTs: Enhancing Consumer Engagement*, 41(2) INT'L J. ADVERTISING 123 (2023).

[40] Luis Garcia & Pedro Martinez, *NFTs in the Food and Beverage Industry: A Case Study of GI Products*, 12(3) J. Digital Mktg. 45 (2023).

captivating stories and interactive experiences brands unlock strong customer bonds and sustain strong customer support and boost their sales performance. The growth in NFT adoption will extend their marketing impact on GI products while simultaneously creating innovative ways to engage consumer audiences.

## IV. Future Prospects and Recommendations

NFTs represent a revolutionary technology which shows promise for shielding and promoting GI Regional product designs represented by GIs provide cultural heritage protection while boosting local economic activities through their specific regional origin marks. The digital authentication and tracking system of NFTs creates a new approach to protect and brand GIs within today's digital environment. The following discussion details NFT potentials within this sector while giving suggestions for stakeholders along with recommended research directions.

### *1. Potential for NFTs to Transform GI Protection and Branding*

*a. Authentication and Provenance Tracking*

NFTs can establish digital authentication methods which enable consumers to validate both product origins and quality standards for GI products. The inclusion of product information including production methods and geographical origin and ownership history in an NFT establishes an unalterable record for product provenance. The implementation of NFT technology fights counterfeits among GI products which protects consumer confidence.

*b. Branding and Marketing*

Through the use of NFTs businesses can develop exclusive branding solutions and marketing strategies for GI product promotion. The creation of NFTs linked to physical products as limited editions generates extra value by making the products more exclusive. The possession of these NFTs lets users access multimedia content such as origin-related videos and stories which helps consumers relate to the brand better.

*c. Monetization and Royalties*

Through NFTs creators can obtain royalties from secondary sales thus enabling GI producers to benefit from these transactions. Under smart contracts, GI producers get automatic financial

distribution whenever their original products are sold again in digital or physical marketplaces. Local communities' benefit from a consistent revenue flow which motivates them to protect their protected GIs.

*d. Global Reach and Accessibility*

Global audiences can access GI products through NFTs since they enable marketplaces and digital platforms to reach worldwide consumers. Small-scale producers operating in remote locations gain tremendous benefit from this approach because they can bypass traditional market channels. The digitized form of GI products through NFTs enables producers to establish connections with international markets which had previously seldom contacted them.

***2. Recommendations for Stakeholders***

*a. Policymakers*

State authorities must undertake the creation of policies that establish NFT compatibility with current GI protection regulations. The introduction of NFTs requires frameworks for creation standards and privacy protection mechanisms as well as solutions for IP legal matters. The government must actively spread knowledge about NFTs to stakeholders from the GI production sector.

*b. Businesses*

Companies in the GI sector along with businesses must seek technology providers who can become their NFT development and management partners. Businesses need to create NFTs which provide extra value for their products by offering both special digital as well as exclusive ownership advantages to NFT owners. Businesses need to invest in blockchain infrastructure because it will ensure the security as well as scalability of their NFT-based initiatives.

*c. Technology Providers*

The design of blockchain technology and NFT solutions should focus on developing easy-to-use systems which address typical requirements of GI producers. Businesses need to develop easy-to-use NFT creation tools while maintaining blockchain network compatibility between systems to solve environmental issues connected to blockchain transactions energy usage.

### *3. Future Research Directions*

*a. Scalability*

Scarce resources will become an essential problem when NFTs gain wider adoption. Academic teams should direct their research toward constructing blockchain systems which maintain security and transaction speed for handling extensive data volumes. Technology developers need to research both Layer-2 solutions and proof-of-stake consensus alternatives.

*b. Interoperability*

The implementation of NFTs for GI protection requires complete integration of different blockchain networks and platforms. Scientists should establish standard procedures which will allow NFTs to move without problems across diverse blockchain environments.

*c. Sustainability*

Blockchain technology faces environmental sustainability problems primarily due to the proof-of-work systems. Future research needs to explore eco-friendly consensus methods and carbon offset strategies to maintain NFT-based GI protection which follows worldwide sustainability standards.

NFTs possess substantial power to revolutionize Geographical Indicators protection together with branding through improved authenticity verification and novel marketing solutions and earnings possibilities. The realization of NFT's storage potential requires partnership between government officials and tech providers and business entities to perform ongoing research about scalability and interoperability and sustainability issues. Stakeholders benefit from adopting NFTs because this technology protects the monetary and cultural worth of GI products while allowing access to digital economic possibilities.

## V. Conclusion

NFTs as a transformative technology represent a revolutionary capability to protect and establish branding systems for GIs. The integration of blockchain technology into NFTs creates a system that allows secure authentication of GI products and proves their original source while solving the problem of product counterfeits. The capability both strengthens consumer trust and raises the economic value and cultural worth of GIs because they serve to maintain regional traditions

together with supporting rural socioeconomics. The use of NFTs provides producers opportunities to extend their marketing techniques by producing digital exclusive items and enhancing storytelling elements and consumer engagement activities that build brand followings and increase market recognition.

NFT integration raises challenges for the protection of GIs as well as their branding purposes. Founder success requires legal obstacles including IP conflicts and jurisdictional challenges and absent worldwide regulatory framework to be resolved because they impede effective NFT-based system execution. The adoption of NFTs for GI protection requires additional technological research into issues related to scalability together with interoperability and sustainability to establish a long-term solution.

NFTs will achieve their maximum benefits through cooperative efforts between officials who manage policies and businesses and technological service providers. The legal framework development by policymakers should connect NFT technology parts with current GI protection systems and business entities need to develop blockchain networks and explore different NFT applications in marketing. Technology providers should produce blockchain solutions which integrate ease of use with interoperability functions and energy conservation benefits for GI producers.

The future of GI protection shows great potential through NFTs because they establish authenticity alongside innovative branding mechanics alongside revenue-generating methods. The digital economy will receive new chances and the cultural and economic value of GI products can be protected by addressing current difficulties between stakeholders through collaboration.