Beyond Copyright Enforcement: Technological Protection Measures and User Rights in India

Aadhithya Narayanan Madhusudhanan[1], Sabarigirish Manikandan[2], S. Akash[3]

[1]*Electronics and Computer Engineering, Vellore Institute of Technology, Chennai, India*

[2]*Computer Science and Engineering, Shiv Nadar University (Delhi-NCR), India*

[3]*Computer Science and Engineering, Shiv Nadar University (Delhi-NCR), India*

[1]aadhithyanm@protonmail.com; [2]sabari.girish2057@gmail.com; [3]s.akash2427@gmail.com

Authors contributed equally to this work.

Abstract*— *Technological Protection Measures (TPMs) have started playing a pivotal role in governing the use, modification, repair and interoperability of digital products. In India, anti-circumvention measures under the Copyright (Amendment) Act, 2012, demonstrate a comparatively more restrained and progressive approach and are intent-based in nature, without requiring liability for circumvention to be independent of copyright infringement as in the case of the United States' Digital Millennium Copyright Act (DMCA), yet remain contextually underspecified when deployed to tackle issues of copyright exceptions and consumer protection. This paper examines the legal uncertainty arising from the use of TPMs in modern software with emphasis on their potential to restrict repair, interoperability and security research. It explores the implications of this ambiguity for India's digital sovereignty and competition, and argues, without overlooking the legitimate functions that TPMs serve in copyright protection and user security, that the absence of clear limits on their use may lead to the use of private enforcement mechanisms superseding judiciary oversight.

***Keywords*—** *Digital Sovereignty, Cybersecurity, Digital Rights, Consumer Protection, Intellectual Property, Competition Policy, Information Technology Law*

I. Introduction

Digital products in India and around the world are often governed by technological restrictions that restrict how the end consumer may use, modify, repair, or interoperate them with other devices and software. These restrictions are technologically enforced through Technological Protective Measures (TPMs), which are technologies such as encryption, obfuscation, modification detection, and service/hardware lockouts. These are legally backed by the Indian Copyright (Amendment) Act, 2012 [1], which introduced Sections 65A and 65B into the Indian Copyright Act, 1957 [3]. Section 65A criminalises circumventing an "effective technological measure" that is applied for the purpose of protecting copyright, with the intention of infringing copyright, and Section 65B criminalises the act of removing or altering any Rights Management Information (RMI) tied to copyrighted works, or distributing and publishing works with RMI removed or altered. The Copyright Act specifically treats computer programs separately from other kinds of works, with different considerations and exceptions for fair-dealing conferred to the public under Section 52 which extends to source code, object code and relevant manuals [1]. While the Act grants copyright owners exclusive rights over their reproduction and distribution, it allows for limited scope of permission for copying or adapting software for specific purposes, interoperating with any other software, or conducting reverse-engineering research. Although, the relationship between these permissible acts and the anti-circumvention policies introduced in 2012 is not extensively clarified in any statutory text.

Anti-circumvention measures were introduced in India in the context of the broader landscape of copyright protection in digital markets. The US Digital Millennium Copyright Act (DMCA), 1998 [2], is one of the first of these regulations to follow suit during the modern period of digitalization and advances in information technology, primarily to fulfill the conditions listed out in the WIPO Copyright Treaty [4] and the WIPO Performances and Phonogram Treaty [5], collectively known as the WIPO Internet Treaties. These treaties require parties to provide legal protections against circumventing TPMs or otherwise removing any form of rights management information. It can be understood that although India was not a signatory to the same at the time, the implementation of anti-circumvention policies in 2012 was an effort to align Indian law with international norms pertinent to digital copyright protection and to keep India in similar footing to other players in technology markets.

Notably, these treaties do not specify any particular form of enforcement of anti-circumvention policies. No mentions are made on the requirement of criminal penalties nor do they mandate a blanket prohibition of circumvention, rather, they set a minimal basis for signatory states to work with, thus leaving signatories with significant autonomy in the determination of the trajectory of anti-circumvention law in their particular states. India became a signatory to the WIPO Treaties in 2018, six years after the introduction of the Copyright (Amendment) Act, 2012 [4].

Indian law surrounding this notably differs from the pioneering DMCA regime in that it is comparatively restrained in scope of application. Section 1201 of the DMCA defines liability for circumvention independently of copyright infringement, implying that circumvention of a TPM is considered unlawful even when its purpose is non-copyright-infringing, such as for research or repair [2]. Limited and temporary exemptions to this near-blanket prohibition of circumvention may be granted for specific circumstances of circumvention through a triennial Library of Congress process [2]. This framework represents a maximalist approach to anti-circumvention, only offering temporary relief to certain specific use cases, themselves limited to a three-year timeframe. Further, the DMCA also criminalises the act of distributing or creating any tool or part which is intended to circumvent TPM technology, regardless of the lack of infringing purpose [2].

In contrast, Section 65A of India's Copyright Act, 1957, explicitly takes into consideration user intent with penalties linked to circumvention with the intention of infringing copyright [3]. Similarly, it incorporates statutory exceptions for circumvention undertaken for purposes not expressly prohibited by the Act, as well as for certain specific use cases such as security research [1]. Although this list of exemptions is not exhaustive, it signals a conscious policy decision that not all acts of circumvention are considered inherently infringing or harmful. Further, based on analysis of the Copyright Act, Indian law does not maintain a prohibition on circumvention tools either, unlike DMCA 1201(2) [2]. These aspects of Indian legislation position India towards an infringement-agnostic model that explicitly lays emphasis on user rights, and permits a wider range of non-infringing conduct. Nonetheless, this model does not necessarily eliminate uncertainty in interpretation, as much of Indian law surrounding anti-circumvention and software modification uses general and underdefined language that is yet to be interpreted under judicial grounds.

II. TPM (Technological Protection Measures)

TPMs are broadly defined as technological measures applied for the purpose of protecting copyright, including measures designed to hinder reverse engineering and diagnosis, such as code obfuscation, encryption, and usage restrictions. Increasingly, they may be used for purposes beyond copyright protection, such as modification detection and unauthorised usage restriction on its own. Indian law criminalizes the breaking of TPMs while infringing copyright [1], but in turn there is no restriction on the scope of practical application of TPMs. The lack of restriction of TPM deployment coupled with the legal ambiguity of software ownership restrictions may lead to the following potentials for misuse.

A. Anti-Consumeristic Measures

Software-enabled devices are ubiquitous in modern life. TPMs may be used to tie device features with software based locks and forced internet-enabled updates, which may be used to enforce overt anti-consumer tactics such as removing, downgrading, or restricting product features after sale.

TPMs may be bundled with software subscriptions in hardware, where features are locked behind a digital payment-gate even if they are physically present and implemented within the bought property. Examples of this practice are observed in the consumer automotive industry: customers of the Volkswagen ID.3 EV were promised an electric vehicle with a 228bhp (brake horsepower) engine, however it would be digitally locked to 201bhp unless they paid for a subscription costing £16.50 per month or £165 per year, or paid a one-time fee of £649 [6]. The tactic of using TPMs to digitally prevent users from accessing features may permit manufacturers to charge owners a premium for accessing features already present in the sold property.

TPMs may also be used to arbitrarily impede or disable device functionality in a move known as “planned obsolescence”, where device features are artificially and intentionally degraded over time in order to incentivise owners to purchase new products from the manufacturer [7]. As consumers were typically unable to technically diagnose or repair their property due to TPMs applied on them by the manufacturer, they were incorrectly led to assume the device was obsolete or naturally degraded, influencing them to purchase new replacement products even if only repair was necessary to maintain functionality.

B. Security Issues and Lack of Transparency

TPM can be used to hinder product standards testing. In the case of the Volkswagen emissions scandal, cars were fitted with "defeat devices", software meant to check if the car was under a testing environment by monitoring various parameters such as speed, engine operation, air pressure, and then temporarily altered engine performance to underperform their cars and thwart emissions testing [8].

While a security analysis of remote-unlocking software is beyond the scope of this paper, we note in short that the practice of treating the “manufacturer” as the privileged party in this interaction yields a critical vulnerability; a malicious actor who obtains the relevant cryptographic private key material and control over the remote security infrastructure, may impersonate the manufacturer and deliver unwanted or malicious software to the user’s device without their consent or knowledge, posing potential risk for the security posture of millions of network-connected devices in India that are bound to over-the-air security updates. This practice requires a great level of trust in the manufacturer to maintain data security of their infrastructure and keys.

C. *The Right to Repair*

TPMs may also be potentially used to restrict user self-repair of user products by placing software locks of varying types to detect self-repair and impede functionality until first-party repair is done. This practice often leads to users being locked out of their property for performing repair on their own, requiring them to pay a premium for manufacturer-provided repair services even if safe, equal or superior free or third-party repair services exist. An example is John Deere's tractors, which could not be self-repaired even when requisite hardware fixes were performed due to the lack of software that Deere refused to provide to customers [9]. This may discourage competition in the form of third-party repair companies and parts, while also giving the manufacturers the ability to arbitrarily enforce planned obsolescence on older devices or devices with significant damage. Further, it causes a market-dependence on the manufacturer for proprietary parts and services, leaving owners of old products out of support if the manufacturer stops providing such services or components for that specific product, or goes out of business.

D. *Monopolies and Platform Lock-in*

TPMs may also be used as a tool to create walled garden ecosystems with a group of products, in which these groups of products are engineered to function together but with limited interoperability outside their ecosystem. These products may be designed to be highly interoperable with each other but are restricted to those devices only. By actively hindering support for third party clients and being highly isolated with respect to interoperability, certain platforms may grow a large customer-base whose best interest would be to stay on the same platform most of their colleagues, family, and friends are currently on. [10] An example of this would be the Apple ecosystem, where Apple's devices are built to interact with each other seamlessly but support for Apple products and services with other third-party products and services remain subpar, with efforts (including projects such as LibrePods [11]) subjected to limitations directly as a result of these TPMs [11]. Although the ethicality of these walled garden ecosystems is contested, it demonstrates the usage of TPMs to restrict interoperability as cryptographic TPMs may be used to ensure that third-party clients cannot connect to their services. These third-party clients may not necessarily be excluded by copyright law alone and are rather excluded by these cryptographic access controls.

III. Legality of Jailbreaking and Circumvention in India

Under Sec. 65A, Copyright Act, India criminalises the act of circumvention done only in support of the explicit aim of copyright infringement, permitting conduct other than piracy that relies on the circumvention of TPMs, and carving out explicit exemptions for purposes such as research and privacy [1]. This is a notable absence of blanket restrictions observed in other states, which prevent consumers and the public from circumventing TPMs for non-infringing conduct.

When a consumer purchases a software-based product, the ownership of that copy of that product is typically transferred to them, and with it the manufacturer or seller's intellectual property rights lapse to him. This is known as the Doctrine of Exhaustion, which India recognises in software [12]. Thus, software modification in and of itself does not constitute a copyright infringement, assuming the user legally owns their copy of the software.

However, the legality of the development and distribution of circumvention tools themselves is largely untested in Indian courts of law, and the perception of legal protection of TPMs puts security researchers and circumvention tool developers in a legal grey area. The overlapping intellectual property and cyber-law concerns associated with jailbreaking and circumvention shroud its practice as a consumer option and market force, leading to would-be businesses, researchers, and consumers not partaking in these practices due to a lack of awareness of the rights accorded to them, and fears of legal threats or service bans from rightsholders.

A. *Copyright View*

The Copyright (Amendment) Act, 2012 [1] of India defines what constitutes a copyright. Pertinent to software, it includes the right to adapt, transform, publish, and sell software. This right is seen as a statutory and exclusive right under Indian law, where parties who don't have copyright over the software in question are legally prohibited from exercising any of those rights of modification and publishing. However, the Act also contains provisions that lay out exceptions to copyright violation for certain practices of software modification and jailbreaking. Section 52(1)(aa), (ab), (ac), (ad) lay out what actions explicitly do not constitute copyright infringement of software in India, while Sections 65A and 65B lay out the pertinent anticircumvention clauses.

Sec.52(1)(aa) permits the act of adapting a legally owned copy of software in order to use it for the purpose it was supplied. However, this restriction of purpose may exclude the possibility of modifying software for innovative and unknown use cases beyond its original purpose.

Sec.52(1)(ab) permits any act done necessarily to obtain information necessary to operate interoperability of an independently created software program with other programmes, provided the information necessary to achieve that interoperability is not readily available. The permission of doing acts necessary for interoperating specifically "independent" software may imply that interoperating with modern network or external service dependent software, including but not limited to social-media clients and servers, video-games, or network-connected Internet-of-Things devices, is not permitted.

Further, the particular language used permits acts intended to attain information necessary to achieve interoperability, but does not prescribe criminality for the act of interoperation itself.

Sec. 52(1)(ac) broadly permits reverse engineering software. However, this does not necessarily imply that the knowledge gained from reverse engineering a software-based product may be used in turn to modify it, or integrate it into or with other software-based products.
Sec. 52(1)(ad) permits adaptation of a personally legally owned copy of software for non-commercial personal use. This raises the question of whether commercial jailbreaking done for profit is permitted. Criminality for commercial jailbreaking, interoperation, or software modification is nonetheless not defined in any relevant statute. As iterated above, these exceptions do not necessarily legally exempt the full integrated spectrum of activities necessary to perform jailbreaking from the potential to be copyright infringements in and of themselves.

The rights accorded under these clauses, while not necessarily constituting fair-dealing in a strict legal sense, taken together provide a framework for explicitly protecting software interoperation, adaptation, and research. However, the lack of definition for pertinent edge cases such as networked software interoperation, reverse-engineering derived development and modification, and possibility of commercial jailbreaking kit services and products, as well as unclear boundaries and intersections of each clauses' rights with each other and the anti-circumvention provisions for violating copyright may open researchers, consumers, prospective software jailbreaking businesses to legal risk.

B. Patent View

Under Section 3(k) of the Patents Act, 1970, India does not recognise works such as computer programmes, software, algorithms etc as patentable [13]. Thus, neither the act of circumventing software, nor distributing or creating circumvention tools run afoul of patent law in specific. Furthermore, patent exhaustion rights may apply to patented Computer Related Inventions once sold [13].

C. Trademark View

India's trademark laws allow certain unauthorised uses of a registered trademark under fair use, mainly Section 30(2)(d) of the Trade Marks Act of 1999 [14] which permits nominative fair use. These clauses may allow aftermarket circumvention and modification tools to be distributed referring to their target technologies, as it communicates the purpose or compatibility of the product without obscuring or confusing consumers about the original base goods. Nonetheless, manufacturers may seek to exercise their trademark rights over property after sale, potentially jeopardising users who wish to publish modified or unofficial versions of branded software, or tools for creating the same. Such possibilities require further clarity under the law.

D. Trade Secret View

The act of sharing, distributing, or publishing circumvention tools or private key material used in cryptographic TPM implementations without authorisation may be a violation of trade secret law. The private key material itself, or specific tools or techniques for repair, debugging, hidden test-modes, functionality, or modification of the technological product may themselves be protected trade secrets. Such cases require further clarity under the law.

E. IT and Cyber Law View

Indian information technology is regulated by the Information Technology Act, 2000 [15]. The provisions criminalise, pertinently, the actions of unauthorised tampering, hacking, password-theft, intrusion, breach of confidentiality, or disclosure of information in breach of contract.

It may be interpreted that sections 72, 72A (if the publisher has agreed to a EULA that prohibits sharing such private cryptographic material), 73, 74 of the IT Act forbid the sharing of private crypto-keys without the creators' permission. Thus, practices of jailbreaking, reverse engineering, and circumvention, if they are done with explicit access to trade secrets of cryptographic keys or debugging, repair, or modification methods may be considered a violation of privacy or confidentiality on the manufacturers' property. However, unclear ownership of software may complicate the question of whether the privacy of manufacturers as the owner of the software is being violated, or the consumer is the owner exercising rights over his property.

Sec.65, specifies that the act of, or facilitating the act of, intentionally concealing, destroying, removing, or altering a "computer source document" is a criminal offence. However, in this practice it is not clarified whether the definition of hacking may imply the manufacturer's owned licensed property is being hacked, or the user is "hacking himself" by modifying his own property. Such questions are contingent on whether ownership of the software copy rests with the consumer or the software vendor.

1. *Is unauthorised interoperability considered to be hacking or intrusion?*

Sec. 52(1)(ab), of The Copyright Act stipulates that any act done in service of interoperability of an independently created programme with other programmes cannot be considered a copyright infringement [1]. This begs the question of whether

this clause applies in the modern age, with different classes of network-reliant software. Today, software often relies on many moving networked parts, mostly increasingly reliant on cloud services run and owned by the rightsholder of the client. Users download a client application or programme and then remotely access content that is stored entirely on a separate operator's computer systems and networks.

In such a case, ownership of software is blurry. Typically, service operators such as Facebook and Google Drive grant the users a license to access their service and content, with multiple stipulations such as restrictions on use, abuse, and importantly bans on interoperation or access via "unofficial" methods or clients such as alternative clients. Users are not seen to "own" a copy of the programme under such a restrictive license in any substantive way [12], potentially conflicting with owner rights conferred under Section 52(1)(aa),(ab),(ac),(ad) [1]. In such cases where the "operator" of the computer system is legally considered the service provider or manufacturer rather than its licensed user, it may also open up the user to being liable for computer fraud, hacking, unauthorised modification, or intrusion for the act of circumvention, modification, alternative usage, or jailbreaking.

What could be assessed is the ownership of the computer system in question, and what the definition of "normal usage" is. For example, when a consumer buys a mobile phone from a phone company, it needs to be assessed whether the consumer or the manufacturer/seller is the operator of the phone. In practice, it may be observed that the business may require the consumer to sign or agree to a EULA contract that transfers the consumers' ownership of the product back to the company [12], or otherwise turns the user into a "licensee" of the software or hardware in question. For example, if, in a hypothetical sense, the particular software company inserts any form of technology into their software that intends to track and profile the users' habits without their consent, that may be considered the "normal usage" of the software, and thus it needs to be clarified whether the user would be "damaging" the system or "denying access to an authorised person" to access the system by performing a jailbreak or tracker-removal (notwithstanding the ethicality of the same, which is beyond the scope of this paper) on the particular technology. Such questions are critical in order to define the bounds of who truly has the ability to exercise ownership rights and who defines what "normal" and "abnormal" computing behaviour is.

The encumbrances and associated underdefined laws as underlined here still, owing to the vagueness of context, make it onerous for consumers and businesses that wish to publicly use circumvention tools and techniques for ethical purposes, thus potentially leading to a lack of commercial investment, relegating it only to small-scale technologically literate consumers, researchers, or communities. The restrictions and lack of clarity on commercial circumvention and circumvention-tools may imperil the prospects of startup businesses that wish to compete with dominant technology players by interoperating with their technology, providing new features, or removing undesired features.

2. Is commercial jailbreaking legal?

Under Section 52(1), The Copyright Act [1], by a seeming repeated specification of “personal” and “non commercial” conditions on research, interoperability, and adaptation of software, it implies that commercial jailbreaking practices may not be explicitly legal. Thus, practices such as selling TPM circumvention tools, jailbreak kits, alternative software, or jailbreak services on the market for profit may be legally risky. However, there are no penalties or criminality explicitly assigned to jailbreaking or circumvention done for profit or commercial purposes.

The advent of large-scale Generative AI systems, trained on large corpuses of potentially copyrighted materials and producing new outputs based on automatic techniques brings the questions of commercial jailbreaking, TPM circumvention, and transformative usage of software to the forefront of technological policy discourse [16]. Currently, copyright owners utilise various TPMs to directly protect their content from infringement. The continued efficacy and purpose of these TPMs is beyond the scope of discussion of this paper, though it is pertinent in the wider conversation. The proliferation of Generative AI systems, working with large scale networks of content, able to generate new content with ease (the ethics or efficacy of which is beyond the scope of this paper), seem to have brought end-users a new ability to further control and adapt technology to their will. Developing industry standards such as the Model Context Protocol, which aim to provide LLM based systems with universal and standardised interfaces to software technologies such as source code editors, web services and interfaces, and other software, serve a testament to the ability for interoperability of software to revolutionise the market and create novel, composite innovations with consumer benefits. Such practical acceptance of interoperability and circumvention in the case of large scale AI systems, and the benefits gained thereof, may raise the question of permitting access the same innovative potential in a personal, community, or commercial capacity by potentially softening any critical circumvention, interoperability, or reverse engineering restrictions applied on them by law, contract, or technology.

IV. Potential for Censorship on Research and competition

Incidents of major digital platforms utilizing a combination of IP claims, EULA/ToS restrictions and the threat of legal action even when given research may fall well within the law to restrict independent researchers and third-party tools have been observed. Certain incidents in particular have concerned researchers and regulators about the effects this may have on transparency and consumer freedom. The Electronic Frontier Foundation, in 2021, reported that Facebook (now Meta) banned the accounts of those NYU researchers involved in a project to analyse and gather ads shown to users [17]. The platform's reasoning for the same cited user privacy concerns and policy violations, although independent observers have asserted that the move shut down transparency research. Similarly, legal threats from Facebook resulted in AlgorithmWatch, a project attempting to analyze and monitor Instagram's algorithm, ceasing its operations [18], and the forced shutdown and legal threats against Barinsta, an independently developed open-source non-commercial Instagram client for mobile devices that let users access Instagram's services from an alternative frontend client using standard, public internet protocols [19].

The developer of the project claimed that Facebook forced him to shut down the project, cease relevant research and development, and further banned him from using Facebook's services in what observers claim is a bid to stifle competitive conduct. Notably, in light of such incidents, it is worth noting that the Delhi High Court observed that "if a person is under a fear of being sued, he may not express himself freely on public issues and this would chill the public debate. "in Ram Jethmalani vs Subramaniam Swamy on 3 January, 2006 [20].

A. Digital Sovereignty

In light of the context presented in this paper, India's digital sovereignty is a factor to consider when extending the scope of exceptions to the breaking of TPMs in certain scenarios. Digital sovereignty is a concept referring to one's capacity to act independently in controlling one's stake in digital economies that one relies on. Three distinctions can be made in the context of this term [21]. For nations, digital sovereignty means the capacity to enforce digital standards and infrastructures within their own territories on their own terms. This can then be extended to the next two distinctions: organizations and individuals wherein the scope of autonomy is the changing parameter; organizations with higher digital sovereignty have more control over digital dependencies like cloud providers and other software applications and individuals with higher digital sovereignty have more control over where their personal data and digital identities are seen. India's ability to understand, adapt, interoperate with and exit from foreign-controlled digital infrastructure that underpin Indian economic and social activity is crucial to embellish its self-reliance as a nation.

The leaks by former US intelligence contractor Edward Snowden, focusing on legal surveillance conducted by the USA's National Security Agency using the PRISM program, claimed that covert partnerships with software companies were facilitated to make commercial encryption software exploitable to eavesdropping and to insert backdoors into the software that makes them exploitable to remote control [22]. Much global security research on commercial software has uncovered many other vulnerabilities, intentional or unintentional, that may permit covert remote control and eavesdropping. In the case of internet-of-things enabled devices, these backdoors or vulnerabilities were easily exploitable and accessible, allowing large botnets and malware networks to arise owing to deep penetrations into consumer markets and businesses. This is a cause for concern for the Indian government and society, due to the potential for use in hardware and software infrastructure that many Indian administrative bodies rely on.

Thus, jailbreaking and circumvention may serve as critical practices by security researchers who wish to publish security fixes for vulnerable software and hardware even if the first-party vendor or rightsholder may not outright publish them in a timely manner, if at all. In such a case, the act of circumventing a technological lock reveals the live vulnerabilities they may intentionally or unintentionally conceal, and the act of modification serves to remove or neuter those vulnerabilities. For instance, the OpenWRT community firmware project routinely investigates and patches router vulnerabilities and then publishes fixes for devices that are no longer actively supported by developers [23]. Similarly, reverse-engineering groups such as fail0verflow have exposed security flaws in software, the public disclosure of which has led to community fixes and have enabled more comprehensive understandings of security design [24]. Such security research could be a pivotal part of the Government of India's repertoire of security practices intended to ensure sovereignty, independence, and security of technology used, by hiring and employing skilled security researchers to improve technical security.

Members of major global organisations such as the European Union, the French Government, and NATO are increasingly switching to open-standards based communications protocols such as Matrix, and are underlining what they claim is a “desperate” need to switch away from American-owned technology stacks such as those of Microsoft [25]. Further, the EU’s Digital Markets Act and Digital Fairness Act require online platforms to explicitly support practices of interoperability and create provisions by which digital markets could be made more competitive and amenable to the EU’s domestic policy objectives such as digital sovereignty. [26]

B. Threats caused by technological circumvention and interoperability

Anticircumvention technology was originally developed in order to prevent the unauthorised copying of copyrighted material. Under the WIPO Copyright Treaty and Section 65A and 65B of the Indian Copyright Act, these technologies are vital parts of the copyright enforcement and protection regimes, empowering creators and copyright holders to control access to their work and prevent unauthorised modifications [3], [4].

In the case of networked services, the practice of platform lock-in and walled gardens were evolved in response to the growing threats of scams, proliferation of unregulated content, and lack of safety caused by a lack of guardrails on consumer technology. Technologies to ensure environment integrity and authenticity of the client's software thus aim to protect service integrity and make the service safer to use for the general population of its' users, leading to an increased perception of trust and integrity.

The presence of TPMs has certainly raised perceptions of trust surrounding internet-connected technologies and ensures integrity of critical processes such as communication and finance. The ability to detect tampering, which is a heuristic sign of potentially malicious, hacked, or fraudulent activity, serves as a safeguard used by critical documentation or financial applications in order to ensure a standardised and secure operating environment and debar entire classes of fraudulent activity.

An increase in proliferation of circumvention and interoperability technologies would cause an increase in unregulated and potentially illegal activities owing to the lack of control and regulation that service providers may provide, potentially causing a lack of capability for oversight and regulation. While hardware-level TPMs raise questions of hardware control and security vulnerability it is undeniable that on average they have raised the bar for security for the average non-technical consumer, guarding against unauthorised third-party tampering, and ensuring that the vast majority of consumers enjoy a safer experience.

V. Conclusion

This paper serves as an analysis of the role of Technological Protection Measures (TPMs) and anti-circumvention law in India across multiple introspects in terms of consumer protection, copyright, interoperability, cybersecurity and digital sovereignty. While Sections 65A and 65B of the Indian Copyright Act, 1957 adopt a significantly intent-based approach, wherein circumvention is only criminalized when undertaken for copyright infringement, the broader legal context is still vastly underdefined in terms of specific context and use case, especially when applied to modern software [1]. Although Indian law is permissive compared to other regimes such as the DMCA 1201, it does not practically regulate the misuse of TPMs themselves, which may extend beyond copyright protection into anti-consumer or monopoly-reinforcing use-cases [2].

Although Section 52 (of the Indian Copyright Act, 1957) recognises non-infringing circumvention, research, and modification, the absence of judicial precedents on the limits of liability of circumvention tools, potential encumbrances surrounding embedded cryptographic private key material, and lack of clarity on software ownership leaves researchers, consumers and even prospective businesses in a legal grey area [1]. This lack of contextual elaboration may risk reinforcing market concentration by dominant platforms, suppress interoperability and consumer rights, and legally encumber security research. Such issues may also undermine India's prospects for full digital sovereignty. Technological independence is built on the ability to use, adapt, and modify software and hardware without encumbrance. Circumvention and jailbreaking within the framework of the law have historically played a crucial role in exposing security risks, particularly in cases where the original vendors may no longer extend active support. In the absence of clear legal context, Indian research and export participation in foreign-dominated digital markets may be significantly undermined.

Nonetheless, TPMs serve very legitimate functions in safeguarding copyrighted works and users. The paper thus suggests that TPMs cannot be rejected altogether, and rather that the regulatory challenge is clearly defining their lawful scope. Without statutory backing or clarity, particularly for cases of circumvention for non-infringing purposes [1], there exists the risk of private contracts superseding the legal balances between rightsholders, consumers and the public. Clarifying the legal context of circumvention is thus essential to preserve consumer rights, enable healthy competition through interoperability and support India's long-term digital security and sovereignty. Notably, much of the uncertainty stems from the absence of jurisprudence clarifying much-needed context tying anti-circumvention provisions to contractual and technological enforcements in digital markets. This paper does not seek to conclusively pinpoint the ethicalities of non-infringing circumvention, but to help outline the legal boundaries within which future legislative clarification and judicial interpretations may occur.

References

[1] Government of India, "The Copyright (Amendment) Act, 2012," India Code.

[2] United States Congress, "Digital Millennium Copyright Act," 1998.

[3] Government of India, "The Copyright Act, 1957," India Code.

[4] World Intellectual Property Organization, "WIPO Copyright Treaty," 1996.

[5] World Intellectual Property Organization, "WIPO Performances and Phonograms Treaty," 1996.

[6] Fortune, “Car buyers have to pay extra to unlock horsepower on Volkswagen vehicles—an ‘uphill battle’ subscription model that has drawn the ire of customers”, Aug 2025

[7] Federal Trade Commission (USA), “Nixing the Fix: An FTC Report to Congress on Repair Restrictions,” May 2021.

[8] BBC News, “Volkswagen: The scandal explained”, Dec 2016

[9] NBC News, “Right-to-repair revolution: Farmers challenge John Deere's control over equipment repair”, Apr 2025.

[10] Lina M. Khan, “Amazon’s Antitrust Paradox,” Yale Law Journal, 2017.

[11] K. Devar, "LibrePods," GitHub.

[12] Engineering Analysis Centre Of ... vs The Commissioner Of Income Tax (2021), AIRONLINE 2021 SC 102, Supreme Court of India, 2 March, 2021

[13] Government of India, "The Patents Act, 1970," India Code.

[14] Government of India, "The Trade Marks Act, 1999," India Code.

[15] Government of India, "The Information Technology Act, 2000," India Code.

[16] U.S. Copyright Office, “Copyright and Artificial Intelligence,” 2023.

[17] Electronic Frontier Foundation, "Facebook's Attack on Research is Everyone's Problem," EFF Deeplinks, Aug. 2021.
[18] AlgorithmWatch, "Towards a Monitoring of Instagram," AlgorithmWatch.
[19] Austin Huang, "Barinsta," GitHub.
[20] Ram Jethmalani v. Subramaniam Swamy, 126 (2006) DLT 535, High Court of Delhi, Jan. 3, 2006.
[21] NITI Aayog, “National Strategy for Artificial Intelligence,” 2018.
[22] E. MacAskill and G. Dance, "NSA files decoded: Edward Snowden's surveillance revelations explained," The Guardian, Nov. 2013.
[23] OpenWrt, "OpenWrt security hardening," OpenWrt Wiki.
[24] fail0verflow, "Reversing," fail0verflow Blog.
[25] Liam Proven, “'The EU runs on Microsoft' – and Uncle Sam could turn it off, claims MEP”, The Register, Feb. 2026
[26] Tambiama Madiega, “Digital sovereignty for Europe”, European Parliamentary Research Service