

LEGAL AND TECHNOLOGICAL CHALLENGES IN ADDRESSING COPYRIGHT PIRACY ON GLOBAL OTT PLATFORMS

MACHARLA RANADEVI

V BA.LLB (hons) – B section

Vels Institute of Science, Technology & Advanced Studies (VISTAS)

V.SWATI

Assistant professor of law

Vels Institute of Science, Technology & Advanced Studies (VISTAS)

ABSTRACT

The rapid expansion of Over-the-Top (OTT) streaming platforms has transformed the global entertainment ecosystem by enabling on-demand access to digital content across borders. However, this growth has simultaneously intensified the problem of copyright piracy, which remains one of the most persistent threats to the creative industries. This research examines the complex interplay between legal frameworks and technological mechanisms in combating copyright piracy on global OTT platforms, highlighting the limitations and gaps that persist despite ongoing regulatory and technical interventions. From a legal perspective, the transnational nature of OTT services creates jurisdictional challenges, as copyright laws vary significantly across countries.

While international agreements such as the Berne Convention and the TRIPS Agreement attempt to harmonize protection standards, enforcement remains fragmented and inconsistent. OTT platforms often operate across multiple legal regimes, making it difficult to identify applicable law and hold infringers accountable. Additionally, safe harbor provisions protecting intermediaries frequently limit platform liability, further complicating enforcement against piracy networks that exploit digital ecosystems. On the technological front, OTT providers employ a range of anti-piracy tools, including digital rights management (DRM), watermarking, encryption protocols, and artificial intelligence-based monitoring systems. Despite these advancements, piracy continues to evolve through techniques such as screen recording, credential sharing, illegal streaming websites, and decentralized peer-to-peer networks. The adaptability of piracy technologies often outpaces preventive mechanisms, exposing the reactive rather than proactive nature of current solutions. The study further explores how socio-economic factors, accessibility issues, and consumer behavior contribute to the persistence of piracy. In many regions, high subscription costs and limited content availability encourage users to resort to unauthorized sources. Thus, piracy cannot be addressed solely through enforcement; it requires a balanced approach that integrates affordability, accessibility, and user awareness. This research concludes that effective mitigation of OTT piracy requires a hybrid strategy combining stronger international legal harmonization with advanced adaptive technologies and consumer-centric policies. A coordinated global response is essential to protect intellectual property rights while ensuring equitable access to digital content.

Keywords : OTT Platforms; Copyright Piracy; Digital Rights Management; International Copyright Law; Streaming Services; Cyber Enforcement

INTRODUCTION

The proliferation of Over-the-Top (OTT) streaming platforms has fundamentally reconfigured the global architecture of audiovisual content distribution. By enabling instantaneous, on-demand access to films, web series, and digital entertainment across jurisdictional boundaries, platforms such as Netflix, Amazon Prime Video, and Disney+ Hotstar have disrupted traditional models of broadcast and theatrical exhibition. This technological shift, while expanding consumer access and transforming creative economies, has simultaneously intensified the problem of copyright piracy in ways that existing legal frameworks were not originally designed to address. At the centre of copyright law lies the normative objective of protecting original creative expression and ensuring that authors and rights holders receive adequate recognition and economic reward for their works.

However, the emergence of OTT ecosystems has exposed significant structural limitations in the enforcement of these rights. Unlike traditional infringement, which was largely territorially confined and physically traceable, piracy in the OTT environment operates through decentralised, borderless, and technologically sophisticated networks that enable rapid duplication and redistribution of copyrighted content across multiple platforms and jurisdictions. The legal regimes governing copyright protection, including the Copyright Act 1957 in India, the Digital Millennium Copyright Act (DMCA) in the United States, and the EU Copyright Directive, were largely conceptualised in an analogue or early digital context. Although successive amendments and judicial interpretations have sought to modernise these frameworks, they continue to exhibit foundational constraints when applied to streaming-based piracy. In particular, issues relating to intermediary liability, jurisdictional enforcement, and cross-border infringement remain inadequately resolved, resulting in a fragmented global enforcement landscape. Compounding these legal challenges is the technological sophistication of modern piracy mechanisms. Illicit streaming websites, peer-to-peer file sharing networks, modified IPTV services, and credential-sharing practices have evolved in parallel with legitimate OTT technologies. Despite the deployment of anti-piracy tools such as digital rights management systems, encryption protocols, watermarking technologies, and artificial intelligence-based monitoring systems, piracy continues to adapt at a pace that often outstrips enforcement capabilities. This creates a persistent asymmetry between enforcement mechanisms and infringement techniques. Furthermore, the persistence of OTT piracy cannot be understood solely through a doctrinal or technological lens. Socio-economic factors, including pricing disparities, regional content restrictions, and unequal access to subscription-based services, contribute significantly to consumer engagement with pirated content. This introduces an additional layer of complexity, wherein piracy is not merely a legal violation but also a market-driven phenomenon influenced by accessibility and affordability considerations.

In light of these intersecting dimensions, this paper seeks to undertake a doctrinal and comparative analysis of the legal and technological challenges associated with combating copyright piracy on global OTT platforms. It focuses particularly on the Indian legal framework while situating it within broader comparative perspectives drawn from the United States, the European Union, and other relevant jurisdictions. The study further evaluates the effectiveness of existing enforcement mechanisms, including judicial interventions such as dynamic injunctions and “John Doe” orders, alongside technological countermeasures employed by industry stakeholders. The central argument advanced in this paper is that current regulatory responses remain largely reactive, fragmented, and insufficiently harmonised at the international level. While legal systems continue to rely on intermediary liability doctrines and post-infringement enforcement strategies, technological realities of OTT piracy demand more proactive, integrated, and adaptive regulatory approaches. Accordingly, the paper contends that a recalibration of both legal doctrine and enforcement architecture is necessary to address the evolving nature of digital piracy in the OTT ecosystem. By engaging with statutory frameworks, judicial developments, and technological enforcement mechanisms, this research aims to contribute to the ongoing discourse on the adequacy of intellectual property law in the digital streaming era. It ultimately argues that effective anti-piracy strategy must be situated at the intersection of law, technology, and policy, rather than within any single domain in isolation.

CONCEPTUAL FRAMEWORK OF COPYRIGHT

The legal protection of copyright in audiovisual works is grounded in the broader principle that intellectual creations constitute property interests deserving of statutory recognition and enforcement. In doctrinal terms, copyright law operates as a calibrated balance between the rights of creators and the public interest in access to information and culture. This equilibrium is particularly delicate in the context of digital dissemination, where reproduction and distribution occur at negligible marginal cost and at unprecedented speed. The conceptual foundation of copyright protection in India is embodied in the Copyright Act 1957, which grants exclusive rights to authors and rights holders over reproduction, adaptation, communication to the public, and distribution of their works. These rights are reinforced by India's obligations under international instruments such as the Berne Convention for the Protection of Literary and Artistic Works and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), both of which emphasise minimum standards of protection and national enforcement mechanisms. However, the conceptual integrity of these rights is increasingly tested in the OTT environment, where “communication to the public” is mediated through complex digital infrastructures rather than linear broadcasting systems. The legal characterisation of streaming, caching, transcoding, and content delivery network (CDN) distribution raises unresolved doctrinal questions regarding the locus of infringement and the attribution of liability across multiple intermediaries.

A central tension emerges between the classical “author-centric” model of copyright and the platform-driven architecture of modern content dissemination. OTT services do not merely host content; they actively curate, recommend, compress, and transmit works through algorithmically governed systems. This hybrid role complicates traditional classifications of intermediaries as passive conduits, thereby blurring the boundaries

of secondary liability. In addition, the doctrine of intermediary liability codified in India under Section 79 of the Information Technology Act 2000 introduces a “safe harbour” framework conditioned upon the observance of due diligence and expeditious takedown upon actual knowledge of infringement. While this regime was designed to facilitate the growth of digital platforms, its application in the context of OTT piracy enforcement reveals significant limitations, particularly in relation to proactive monitoring obligations and cross-border enforcement coordination. Judicial innovation has attempted to bridge some of these gaps. Indian courts have increasingly resorted to dynamic injunctions and “John Doe” (Ashok Kumar) orders to address large-scale, anonymous, and rapidly evolving piracy networks. These remedies enable rights holders to secure pre-emptive or adaptive blocking of infringing websites without initiating separate proceedings for each instance of infringement.

Nevertheless, their effectiveness remains contingent upon cooperation from internet service providers and the technical feasibility of enforcement. At a broader theoretical level, the persistence of OTT piracy also reflects a structural mismatch between territorially bounded legal systems and inherently borderless digital infrastructures. Copyright law continues to operate within a jurisdictional paradigm, whereas OTT platforms function within a transnational ecosystem governed by private contractual arrangements, global distribution networks, and decentralised hosting architectures. This disjunction produces enforcement asymmetries that are difficult to resolve through unilateral legal reforms.

Consequently, any meaningful doctrinal analysis must situate copyright enforcement within an integrated framework that accounts for statutory law, judicial interpretation, platform governance, and technological design. It is at this intersection that the contemporary challenges of OTT piracy become most visible, requiring a reassessment of traditional legal categories and enforcement strategies.

EVOLUTION OF OTT PLATFORMS AND THE DIGITAL PIRACY ECOSYSTEM

The emergence of Over-the-Top (OTT) platforms represents a structural transformation in the delivery, consumption, and monetisation of audiovisual content. Unlike traditional broadcasting systems, which rely on scheduled programming and geographically limited transmission infrastructures, OTT platforms operate through internet-based distribution models that enable on-demand, user-specific access to content. This shift has been driven by advancements in broadband penetration, cloud computing, mobile device accessibility, and adaptive streaming technologies, all of which have collectively lowered barriers to high-quality media consumption. In the Indian context, the growth of OTT services has been particularly pronounced following increased internet accessibility and data affordability. Platforms such as Netflix, Amazon Prime Video, Disney+ Hotstar, and regional services have contributed to a rapidly expanding digital entertainment market. This expansion has also encouraged original content production tailored to diverse linguistic and cultural audiences, thereby altering traditional content creation ecosystems that were previously dominated by theatrical and television distribution channels. However, the same technological features that facilitate the scalability and efficiency of OTT platforms also render them highly vulnerable to unauthorised reproduction and redistribution. The digitisation of audiovisual content enables perfect replication without degradation in quality, while encrypted streams can be intercepted, recorded, and redistributed with relative ease. As a result,

piracy in the OTT environment is no longer confined to physical copying or rudimentary file-sharing but has evolved into a sophisticated, multi-layered ecosystem. This ecosystem comprises several distinct but interconnected modalities. The first involves illicit streaming websites that host or embed copyrighted content without authorisation, often monetised through advertising networks. The second consists of peer-to-peer (P2P) file-sharing networks, which decentralise distribution and make enforcement more complex by dispersing infringing copies across multiple nodes. The third includes modified Internet Protocol Television (IPTV) services, which aggregate pirated content into subscription-based packages that mimic legitimate OTT offerings. A further emerging practice is credential sharing and account resale, wherein legitimate subscriptions are unlawfully accessed and distributed among multiple users beyond permitted contractual limits. The adaptability of these piracy mechanisms is closely linked to the architecture of digital distribution itself. Content Delivery Networks (CDNs), encryption protocols, and adaptive bitrate streaming technologies, while designed to enhance performance and security, also introduce multiple points of vulnerability that can be exploited through screen capture tools, stream ripping software, and server-side breaches. Moreover, the global and decentralised nature of internet infrastructure ensures that infringing content can be hosted, mirrored, or proxied across multiple jurisdictions within seconds, significantly complicating enforcement efforts.

The evolution of OTT piracy is also shaped by the increasing professionalisation of piracy networks. Unlike earlier forms of casual infringement, contemporary piracy operations often exhibit commercial characteristics, including organised content acquisition, systematic distribution, and revenue generation through subscription models or advertising arbitrage. In some instances, these networks operate with technical sophistication comparable to legitimate digital enterprises, employing automated scraping tools, encrypted communication channels, and distributed hosting solutions to evade detection. From a legal standpoint, this transformation challenges the traditional enforcement paradigms of copyright law, which were designed around identifiable infringers and territorially confined acts of infringement. The anonymity of digital actors, combined with the fluidity of online content dissemination, undermines the effectiveness of individual enforcement actions and necessitates broader, system-level regulatory responses.

Furthermore, the economic incentives underlying OTT piracy cannot be ignored. The availability of premium content at no cost, or at significantly reduced prices, creates a parallel consumption economy that competes directly with legitimate subscription-based models. This is particularly relevant in price-sensitive markets such as India, where disparities in income levels and subscription affordability contribute to sustained demand for pirated content. Consequently, piracy functions not merely as a legal infringement but also as a market substitute shaped by accessibility constraints.

The evolution of the piracy ecosystem thus reflects a convergence of technological capability, economic rationality, and regulatory limitation. As OTT platforms continue to expand their global footprint, the corresponding piracy infrastructure is likely to become even more adaptive, further intensifying the need for coordinated legal, technological, and policy-based responses.

EVALUATING THE LEGAL AND REGULATORY MECHANISMS CONTROLLING OTT PIRACY

The regulation of copyright piracy in the OTT ecosystem operates through a layered statutory architecture that combines substantive copyright protection with information technology regulation and intermediary governance. In the Indian context, this framework is primarily constituted by the Copyright Act 1957, the Information Technology Act 2000, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021. When read together, these instruments reflect an attempt to adapt traditional copyright doctrine to a rapidly evolving digital distribution environment, albeit with inherent structural limitations.

The Copyright Act 1957: Substantive Protection and Its Limits

The Copyright Act 1957 forms the cornerstone of copyright protection in India. Section 14 of the Act defines the bundle of exclusive rights granted to copyright holders, including the rights to reproduce the work, issue copies to the public, communicate the work to the public, and make adaptations. In the context of OTT platforms, the right to “communicate to the public” becomes particularly significant, as streaming services operate through continuous digital transmission of content over the internet. Section 51 of the Act sets out the contours of infringement, providing that copyright is infringed when any act is done without authorisation that violates the exclusive rights of the copyright holder. OTT piracy typically falls within this provision, particularly where content is streamed, downloaded, or redistributed without licence.

However, the Act was originally drafted in an analogue era and has undergone only incremental amendments, leaving it conceptually strained when applied to borderless digital dissemination. A key limitation of the Copyright Act lies in its reliance on identifiable infringers and territorially anchored acts of infringement. OTT piracy, by contrast, is frequently anonymous, decentralised, and hosted across multiple jurisdictions. This creates significant evidentiary and enforcement challenges, particularly when infringing servers are located outside India or routed through anonymised networks.

The Information Technology Act 2000: Intermediary Liability and Safe Harbour

The Information Technology Act 2000 introduces a parallel regulatory structure governing digital intermediaries. Section 79 of the Act provides a “safe harbour” to intermediaries, exempting them from liability for third-party content provided they observe due diligence and comply with prescribed takedown obligations upon receiving actual knowledge of unlawful material.

In the OTT piracy context, this provision is crucial because many infringing activities occur through platforms that host, index, or facilitate access to pirated content. However, the interpretation of “actual knowledge” has been a subject of significant judicial scrutiny. Courts have generally held that intermediaries are not required to engage in proactive monitoring, thereby reinforcing a reactive enforcement model. This safe harbour regime, while essential for enabling the growth of digital platforms, has also been criticised for creating enforcement gaps. Illicit streaming websites and piracy networks often exploit intermediary

infrastructure, domain registrars, and hosting services, thereby complicating attribution of liability. The result is a legal environment in which enforcement is largely complaint-driven and post-facto in nature.

The Intermediary Guidelines Rules 2021: Strengthening Due Diligence

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 represent a significant regulatory development aimed at enhancing accountability in the digital ecosystem. These Rules impose additional due diligence obligations on intermediaries, including the requirement to remove unlawful content within specified timeframes and to establish grievance redressal mechanisms. For OTT platforms classified as “publishers of online curated content,” the Rules introduce a tiered self-regulatory structure. While primarily aimed at content regulation and digital media governance, these provisions indirectly impact piracy enforcement by formalising compliance expectations for platforms operating in India. However, the effectiveness of the Rules in combating piracy remains limited. They primarily govern legitimate intermediaries rather than rogue piracy networks operating outside regulatory jurisdiction. Moreover, enforcement depends heavily on platform cooperation and state capacity, both of which vary significantly in practice.

Judicially Developed Enforcement Mechanisms

Given the statutory limitations, Indian courts have played a proactive role in developing enforcement tools tailored to digital piracy. One of the most significant innovations is the use of dynamic injunctions, which allow copyright holders to extend existing injunctions to mirror or proxy websites that emerge after the initial court order.

This mechanism has been particularly relevant in addressing “hydra-headed” piracy networks that rapidly change domain names to evade blocking orders. Additionally, courts have frequently issued “John Doe” or “Ashok Kumar” orders, enabling rights holders to seek injunctive relief against unknown defendants.

These orders are particularly useful in cases of large-scale piracy where the identities of infringers are not easily ascertainable at the time of filing. Cases such as *UTV Software Communications Ltd v 1337x.to* illustrate the judiciary’s willingness to adopt expansive interpretations of injunctive relief to address digital piracy. In such decisions, courts have recognised that traditional enforcement mechanisms are inadequate in the face of technologically sophisticated infringement networks, thereby justifying broader blocking and takedown powers. Despite these innovations, judicial remedies remain dependent on effective implementation by internet service providers and administrative authorities. This creates a structural gap between legal orders and practical enforcement outcomes.

Comparative Regulatory Frameworks

A comparative analysis highlights divergent regulatory philosophies across jurisdictions. In the United States, the Digital Millennium Copyright Act (DMCA) establishes a notice-and-takedown regime that shields intermediaries from liability if they promptly remove infringing content upon notification. While

this system has been effective in facilitating rapid content removal, it has also been criticised for enabling over-removal and placing enforcement burdens on rights holders.

The European Union, through the Copyright Directive in the Digital Single Market, has moved towards a more platform-responsibility-centric model. Article 17 of the Directive, in particular, imposes obligations on content-sharing platforms to obtain authorisation from rights holders or ensure unavailability of infringing content. This represents a shift from passive intermediary liability to a more proactive monitoring framework. The United Kingdom similarly employs a combination of site-blocking injunctions and cooperative regulatory mechanisms involving internet service providers, reflecting a hybrid enforcement model that balances judicial oversight with administrative execution.

Synthesis and Structural Limitations

Across all jurisdictions, a common tension emerges between facilitating digital innovation and ensuring effective copyright enforcement. India's statutory framework reflects a transitional model, where traditional copyright principles coexist with emerging digital governance rules. However, the system remains largely reactive, relying on post-infringement remedies rather than preventive enforcement mechanisms.

The fragmentation between copyright law, intermediary liability regimes, and judicial innovation results in an enforcement architecture that is neither fully centralised nor fully harmonised. In the context of OTT piracy, this fragmentation is particularly pronounced due to the transnational and technologically adaptive nature of infringement networks. As a result, while the statutory framework provides a foundational structure for copyright protection, its effectiveness in addressing OTT piracy is significantly constrained by jurisdictional limitations, technological asymmetry, and enforcement dependency on intermediaries.

JUDICIAL RESPONSE TO OTT PIRACY IN INDIA

The Indian judiciary has played a central and increasingly interventionist role in addressing copyright piracy in the OTT ecosystem. This judicial activism has emerged primarily as a response to the inadequacy of statutory enforcement mechanisms in dealing with rapidly evolving, anonymous, and transnational piracy networks. Courts have therefore developed flexible equitable remedies that extend beyond traditional infringement relief, with a particular focus on ensuring that injunctions remain effective in a dynamic digital environment.

Expansion of Injunctive Relief in Digital Copyright Infringement

Traditional copyright litigation is grounded in static notions of infringement, where the identity of the infringer and the locus of infringement are clearly ascertainable. However, OTT piracy disrupts these assumptions due to the fluid and decentralised nature of online infringement networks. In response, Indian courts have expanded the scope of injunctive relief to accommodate the realities of digital piracy. A key development in this regard is the judicial acceptance of broad, preventive injunctions that target not only specific infringing websites but also future or mirror domains that may emerge to evade enforcement. This marks a departure from conventional injunction principles, which typically require specificity of parties and

acts. The courts have justified this expansion on the basis that piracy networks operate through “hydra-headed” structures, wherein blocking one domain often results in the immediate emergence of multiple alternative domains hosting identical infringing content. As a result, static injunctions are rendered ineffective almost immediately after issuance.

Dynamic Injunctions and Evolving Enforcement Models

One of the most significant judicial innovations in Indian copyright jurisprudence is the development of dynamic injunctions. These injunctions allow rights holders to extend existing court orders to cover newly identified mirror, redirect, or proxy websites without initiating fresh litigation. This approach was notably developed and refined by the Delhi High Court in a series of copyright enforcement cases involving large-scale online piracy platforms. The rationale underpinning dynamic injunctions is that requiring separate proceedings for each infringing domain would impose disproportionate burdens on rights holders and render enforcement practically ineffective. Dynamic injunctions therefore represent a shift towards an adaptive enforcement model, where judicial orders are designed to evolve in tandem with infringing conduct. However, this approach also raises doctrinal concerns regarding procedural fairness, scope of judicial discretion, and potential over-blocking of legitimate content.

“John Doe” / “Ashok Kumar” Orders and Anonymous Infringement

Another important judicial mechanism employed in OTT piracy enforcement is the use of “John Doe” or “Ashok Kumar” orders. These orders enable copyright holders to obtain injunctions against unknown defendants where there is credible evidence of large-scale infringement but the identities of perpetrators remain undisclosed. In the context of OTT piracy, such orders are particularly significant because infringing websites, streaming services, and distribution networks often operate anonymously or through concealed ownership structures. Courts have recognised that requiring prior identification of defendants would effectively defeat the purpose of enforcement in such cases. These orders typically empower copyright holders to notify internet service providers and intermediaries to block access to infringing content. While this mechanism enhances enforcement efficiency, it also places substantial reliance on intermediaries to interpret and implement judicial directives accurately.

Landmark Jurisprudence on Online Piracy

Indian courts have developed a growing body of jurisprudence addressing digital copyright infringement. A leading case in this area is *UTV Software Communications Ltd v 1337x.to*, where the Delhi High Court examined the phenomenon of large-scale online piracy of films and web series.

In this decision, the Court recognised that traditional enforcement mechanisms were insufficient to address the scale and speed of online infringement. It acknowledged the existence of structurally organised piracy networks and endorsed the use of broad injunctive relief, including blocking of domain names facilitating access to infringing content.

Similarly, in a series of decisions involving film producers and OTT content distributors, courts have consistently emphasised the need to balance copyright protection with the technical realities of internet architecture. This has resulted in an increasing reliance on intermediary-directed injunctions rather than direct enforcement against individual infringers.

Collectively, these decisions reflect a judicial willingness to adapt copyright enforcement principles to the realities of digital distribution, even where such adaptation requires stretching traditional doctrinal boundaries.

Role of Intermediaries in Judicial Enforcement

A defining feature of OTT piracy litigation is the central role played by intermediaries such as internet service providers, domain registrars, and hosting services. Judicial orders frequently require these intermediaries to block access to infringing websites or disable access to specific URLs. This enforcement model effectively transforms intermediaries into quasi-enforcement agents. While this approach enhances practical effectiveness, it also raises concerns regarding the delegation of judicial functions to private entities. Intermediaries are often required to interpret complex legal orders and implement technical blocking measures, sometimes under time-sensitive conditions. Moreover, the global nature of internet infrastructure means that blocked content can often reappear through alternative domains or VPN-based access, limiting the long-term effectiveness of such measures.

Critical Evaluation of Judicial Approach

While the Indian judiciary has demonstrated considerable innovation in addressing OTT piracy, its approach remains fundamentally reactive. Judicial remedies are typically invoked after infringement has already occurred, and their effectiveness depends heavily on the speed and cooperation of intermediaries and enforcement agencies.

Furthermore, the expansion of injunctive relief raises important questions regarding proportionality, over-blocking, and due process. Broad blocking orders, while effective against infringing content, may inadvertently restrict access to legitimate information or services hosted on shared infrastructure. There is also an inherent structural limitation in relying on judicial intervention to manage what is essentially a systemic technological problem. Courts are institutionally designed to resolve disputes, not to regulate evolving digital ecosystems. As a result, judicial innovation, while necessary, cannot substitute for comprehensive legislative and policy reform.

Synthesis

The judicial response to OTT piracy in India reflects a pragmatic adaptation of traditional legal principles to a rapidly evolving digital environment. Through dynamic injunctions, “John Doe” orders, and expansive interpretations of injunctive relief, courts have sought to bridge the gap between static legal doctrine and dynamic technological infringement. However, this approach also underscores the inherent limitations of adjudicatory systems in addressing large-scale, transnational digital piracy. While judicial intervention

provides essential short-term enforcement tools, long-term effectiveness ultimately depends on coordinated legislative reform, technological cooperation, and international harmonisation of copyright enforcement standards.

TECHNOLOGICAL MEASURES AND INDUSTRY RESPONSE TO OTT PIRACY

Alongside legal and judicial interventions, the response to OTT piracy has increasingly shifted toward technological enforcement mechanisms deployed by rights holders and platform providers. These measures reflect an acknowledgement that copyright enforcement in the digital environment cannot rely solely on ex post legal remedies, but must instead incorporate preventive and real-time strategies embedded within the architecture of content distribution itself. However, while technological tools have enhanced the capacity to detect and mitigate infringement, they remain inherently limited by the adaptability and decentralised nature of piracy networks.

Digital Rights Management (DRM) Systems

Digital Rights Management (DRM) technologies constitute one of the most widely adopted mechanisms for controlling access to copyrighted content on OTT platforms. DRM systems function by encrypting audiovisual content and restricting playback to authorised devices and licensed applications. Platforms such as Netflix and Amazon Prime Video employ sophisticated DRM frameworks integrated with device authentication protocols to ensure that content cannot be easily copied or redistributed. In principle, DRM operates as a preventive legal-technical hybrid, translating contractual licensing restrictions into enforceable technological constraints. However, DRM systems are not infallible. Screen recording tools, analogue capture methods, and software-based circumvention techniques continue to undermine their effectiveness. Moreover, once encrypted content is decrypted for legitimate viewing, it remains vulnerable to interception and redistribution through external recording mechanisms.

Watermarking and Forensic Tracking Technologies

Watermarking technologies provide an additional layer of protection by embedding identifiable markers within audiovisual content. These markers may be visible or invisible and are designed to trace the origin of leaked content. In the context of OTT platforms, forensic watermarking is particularly useful for identifying the source of piracy, especially in cases where pre-release content is leaked from internal distribution channels or screening copies. Forensic watermarking enables rights holders to trace pirated copies back to specific accounts, devices, or distribution nodes. This facilitates targeted enforcement actions and strengthens evidentiary support in legal proceedings. However, watermarking is primarily a post-infringement detection tool rather than a preventive mechanism, meaning that it does not eliminate piracy but rather assists in attribution after leakage has occurred.

Artificial Intelligence and Automated Content Recognition

Artificial Intelligence (AI) has become a central component of modern anti-piracy strategies. Machine learning algorithms are increasingly deployed to detect infringing content across websites, social media platforms, and file-sharing networks. These systems operate by scanning digital environments for audio-visual matches, identifying patterns associated with pirated uploads, and triggering automated takedown requests. Platforms such as YouTube's Content ID system exemplify the potential of large-scale automated copyright enforcement. Similar systems are being adapted for OTT ecosystems to monitor unauthorised redistribution of premium content. AI-based detection significantly reduces the time lag between infringement and enforcement action, thereby improving response efficiency. Nevertheless, AI systems are not without limitations. They are often dependent on training datasets, which may not capture all variations of pirated content, particularly those altered through compression, cropping, or re-encoding. Additionally, automated systems may generate false positives, raising concerns regarding over-enforcement and wrongful takedowns of legitimate content.

Content Delivery Networks (CDNs) and Infrastructure-Level Protection

OTT platforms rely heavily on Content Delivery Networks (CDNs) to ensure efficient and scalable distribution of content across geographically dispersed users. CDNs function by caching content at multiple edge servers, thereby reducing latency and improving streaming quality. From an enforcement perspective, CDNs also play a role in restricting unauthorised access and monitoring abnormal traffic patterns indicative of piracy. Some CDN providers collaborate with rights holders to implement access controls and block requests originating from known piracy sources. However, because CDNs are designed primarily for performance optimization rather than rights enforcement, their ability to prevent piracy is inherently limited. In many cases, piracy networks exploit CDN inefficiencies or bypass restrictions through proxy servers and mirror sites.

Encryption Protocols and Secure Streaming Architectures

Encryption remains a foundational element of OTT content protection. Streaming services employ advanced encryption standards to secure data transmission between servers and end-user devices. Protocols such as HTTPS-based streaming and secure token authentication are widely used to prevent unauthorised interception of content streams. Despite these safeguards, encryption does not eliminate piracy at the point of consumption. Once content is decrypted for viewing, it becomes susceptible to capture through external recording devices or software. This structural limitation highlights the inherent asymmetry between secure transmission and insecure consumption environments.

Industry Cooperation and Anti-Piracy Coalitions

In addition to technological measures, the OTT industry has increasingly adopted cooperative enforcement strategies. Rights holders, production studios, and streaming platforms often collaborate through anti-piracy coalitions and monitoring agencies that track infringing websites and coordinate takedown requests across jurisdictions. These coalitions operate on the basis of shared intelligence databases, domain tracking systems, and automated enforcement pipelines. Such collaboration enhances enforcement efficiency by pooling resources and standardising response mechanisms. However, the effectiveness of these initiatives is constrained by jurisdictional fragmentation and the ease with which piracy networks can migrate across hosting providers and domain registrars.

Critical Evaluation of Technological Enforcement

While technological measures have significantly strengthened the enforcement capabilities of OTT platforms, they do not provide a definitive solution to piracy. Instead, they function as adaptive mitigation tools that delay, detect, or deter infringement rather than eliminate it. A key structural limitation lies in the reactive nature of most technological systems. DRM, watermarking, and AI detection primarily respond to piracy after content has been accessed or leaked, rather than preventing initial unauthorised access. Moreover, piracy networks continuously evolve to circumvent technological safeguards, resulting in a persistent cycle of innovation and counter-innovation. There is also a broader concern regarding the centralisation of enforcement power within private technology companies. As OTT platforms increasingly rely on proprietary technological systems to regulate access and enforce copyright, questions arise regarding transparency, accountability, and due process in automated enforcement decisions.

Synthesis

Technological enforcement mechanisms constitute an essential but inherently limited component of the global anti-piracy framework. While DRM, watermarking, AI-based detection, and secure streaming architectures have collectively enhanced the resilience of OTT platforms, they have not eliminated the structural vulnerabilities that enable piracy. The persistence of OTT piracy despite these measures underscores a fundamental reality: technological solutions alone cannot resolve what is simultaneously a legal, economic, and transnational governance problem. Effective enforcement therefore requires an integrated approach that combines technological innovation with robust legal frameworks and coordinated international policy responses.

Additionally, the evolving nature of digital piracy—characterised by decentralised distribution networks, encrypted communication channels, and the rapid emergence of mirror and proxy sites—continues to outpace purely technological countermeasures. Piracy ecosystems increasingly operate across jurisdictions with weak enforcement regimes, complicating detection and takedown efforts even when advanced technologies are deployed. Moreover, the cost and complexity of implementing sophisticated anti-piracy tools often place

smaller OTT platforms at a disadvantage, creating uneven protection across the industry. User behaviour also plays a critical role; high subscription costs, fragmented content availability, and delayed regional releases frequently incentivise consumers to resort to unauthorised sources. These realities highlight the necessity of complementing technological enforcement with accessible pricing models, timely content distribution, stronger cross-border cooperation, and public awareness initiatives aimed at reducing demand for pirated content.

CRITICAL ANALYSIS: STRUCTURAL GAPS IN THE REGULATION OF OTT PIRACY

The preceding discussion reveals that neither statutory frameworks, judicial interventions, nor technological measures operate in isolation or provide a comprehensive solution to OTT piracy. Rather, the enforcement landscape is characterised by fragmentation across legal doctrine, institutional capacity, and technological design. This section critically evaluates these structural deficiencies and situates them within a broader law–technology–economy interface.

The Reactive Nature of Copyright Enforcement

A fundamental limitation in the current regulatory regime is its overwhelmingly reactive orientation. Across jurisdictions, enforcement mechanisms are typically triggered only after infringement has occurred, whether through notice-and-takedown systems, judicial injunctions, or intermediary compliance obligations. This post hoc structure is particularly ill-suited to the OTT environment, where infringing content can be duplicated, redistributed, and monetised within minutes of release. Even dynamic injunctions and automated detection systems do not alter this foundational characteristic. They merely accelerate response time without addressing the initial vulnerability of content at the point of release. As a result, enforcement remains structurally dependent on damage containment rather than prevention.

Jurisdictional Fragmentation and Enforcement Asymmetry

OTT piracy is inherently transnational, yet copyright enforcement remains largely territorial. This mismatch produces significant jurisdictional friction. Infringing websites may be hosted in one jurisdiction, registered in another, and accessed globally through decentralised networks. Consequently, enforcement actions initiated in one legal system often have limited practical effect beyond its territorial boundaries. This fragmentation creates enforcement asymmetry between rights holders and piracy operators. While rights holders are often bound by strict legal procedures and evidentiary thresholds, piracy networks exploit jurisdictional gaps, shifting infrastructure rapidly across borders to avoid sustained enforcement. The absence of a harmonised global enforcement mechanism further exacerbates this imbalance.

Safe Harbour Doctrine and Structural Immunity

The intermediary liability framework, particularly the safe harbour provisions under Section 79 of the Information Technology Act 2000 and analogous international regimes, plays a dual role in the digital ecosystem. While it enables the functioning of online platforms by shielding them from excessive liability, it also creates structural constraints on enforcement against piracy. By limiting liability to cases of actual knowledge and requiring due diligence rather than proactive monitoring, safe harbour provisions effectively place intermediaries in a reactive compliance position. In the context of OTT piracy, this means that large-scale infringing activity can persist until specifically reported and acted upon, thereby allowing significant temporal windows for dissemination and monetisation of pirated content. This doctrinal design reflects an intentional policy choice to balance innovation and liability. However, in practice, it has contributed to enforcement gaps that piracy networks systematically exploit.

Economic Drivers of Piracy and Market Substitution

A purely legal or technological analysis of OTT piracy is incomplete without addressing its underlying economic drivers. Piracy is not solely a function of legal non-compliance but also reflects market conditions, including pricing structures, content availability, and regional access disparities. In many jurisdictions, particularly price-sensitive markets, subscription-based OTT services may be perceived as economically inaccessible relative to average consumer income. Additionally, content licensing restrictions often result in fragmented availability across platforms, requiring users to subscribe to multiple services to access desired content. This creates a structural incentive for consumers to turn to pirated alternatives that offer consolidated and cost-free access. From an economic perspective, piracy therefore functions as a parallel distribution system that partially satisfies unmet demand in the legitimate market. This does not legally justify infringement but does explain its persistence despite enforcement efforts.

Technological Arms Race Between Enforcement and Infringement

The relationship between anti-piracy technologies and piracy networks is best characterised as an ongoing arms race. Each advancement in enforcement technology whether DRM enhancement, watermarking sophistication, or AI-based detection is met with corresponding countermeasures such as screen capture bypass tools, encoding obfuscation, domain mirroring, and encrypted distribution channels. This cyclical dynamic indicates that technological enforcement is inherently non-final. It can raise the cost and complexity of piracy but cannot eliminate it entirely. As piracy networks become more organised and technologically sophisticated, enforcement mechanisms must continuously evolve, resulting in escalating operational costs for rights holders and platforms.

Institutional Limitations of Judicial Enforcement

While courts have played an innovative role in expanding injunctive relief, they are institutionally limited in their capacity to manage ongoing technological systems. Judicial orders are episodic and case-specific, whereas OTT piracy is continuous and adaptive. This creates a structural mismatch between adjudicatory processes and the temporal dynamics of digital infringement. Moreover, enforcement of judicial orders depends heavily on intermediaries and administrative agencies, which may vary in technical capability and responsiveness. This dependency introduces variability in enforcement outcomes and undermines uniform application of legal protections.

Synthesis: A Systemic Enforcement Deficit

The cumulative effect of these factors is a systemic enforcement deficit in the regulation of OTT piracy. This deficit is not attributable to any single legal or technological failure but arises from the interaction of multiple structural constraints: territorial law in a borderless digital environment, reactive enforcement mechanisms in a real-time distribution system, and fragmented institutional responsibility across public and private actors. As a result, current anti-piracy frameworks operate in a state of continuous partial effectiveness. They reduce but do not eliminate infringement, and they respond to but do not structurally prevent piracy. This reinforces the conclusion that OTT piracy is not merely a problem of enforcement insufficiency but of regulatory design mismatch.

POLICY RECOMMENDATIONS AND REFORM FRAMEWORK

The persistence of OTT piracy despite layered statutory protections, judicial innovation, and technological enforcement demonstrates that the current regulatory architecture is primarily corrective rather than preventive. Accordingly, a meaningful response requires structural reform that operates simultaneously at the levels of legislation, institutional design, technological governance, economic policy, and international coordination. This section proposes an integrated reform framework aimed at addressing the systemic deficiencies identified in the preceding analysis.

Legislative and Doctrinal Reforms

At the statutory level, the most pressing requirement is the clarification and modernisation of copyright provisions to explicitly account for digital streaming environments. While the Copyright Act 1957 already recognises “communication to the public,” the provision does not fully capture the technological specificity of OTT transmission, including transient streaming, adaptive bitrate delivery, and cloud-based distribution. A targeted amendment could introduce an explicit statutory definition of “digital streaming infringement,” thereby reducing interpretive ambiguity and enhancing enforcement consistency. Additionally, clearer codification of liability standards for entities facilitating access to infringing content particularly indexing platforms and rogue streaming services would reduce reliance on expansive judicial interpretation. Equally important is the recalibration of intermediary liability under Section 79 of the Information Technology Act

2000. While the safe harbour framework is essential for maintaining innovation in the digital economy, its current formulation is overly dependent on reactive takedown mechanisms. A reformed model could introduce graduated responsibility obligations for high-risk intermediaries, particularly those operating in content distribution ecosystems, without imposing disproportionate monitoring burdens.

Strengthening Enforcement Architecture

Institutional fragmentation remains one of the most significant barriers to effective piracy enforcement. At present, enforcement responsibilities are distributed across courts, copyright offices, internet service providers, and law enforcement agencies, often without a unified operational framework. A specialised digital copyright enforcement unit could be established to centralise coordination between stakeholders. Such a body would function as a technical and legal intermediary, facilitating rapid execution of court orders, maintaining updated databases of infringing domains, and coordinating with international enforcement counterparts. Further, procedural timelines for takedown compliance and injunction enforcement could be standardised to reduce delays between identification of infringement and execution of blocking measures. Given the speed at which OTT piracy operates, enforcement delays significantly reduce the practical effectiveness of legal remedies.

Technological Governance and Industry Standards

Technological measures must evolve from optional industry practices into standardised compliance requirements for OTT platforms and associated intermediaries. One key reform would be the mandatory adoption of forensic watermarking for all pre-release and high-value content. This would significantly enhance traceability in cases of internal leaks and early-stage piracy. In addition, artificial intelligence-based content recognition systems should be integrated into a shared enforcement infrastructure, enabling real-time detection of infringing content across platforms, hosting services, and social media ecosystems. Importantly, such systems should be subject to transparency and accountability safeguards to prevent over-removal of legitimate content. Content Delivery Networks (CDNs) could also be required to implement enhanced monitoring protocols for abnormal traffic patterns associated with piracy dissemination. However, such obligations must be carefully calibrated to avoid converting infrastructure providers into de facto content regulators.

Economic and Market-Based Interventions

Legal enforcement alone cannot fully address piracy without addressing the underlying demand-side drivers. A significant proportion of OTT piracy is driven by affordability constraints and content fragmentation across multiple subscription platforms. Policy interventions could therefore encourage bundled subscription models or tiered pricing structures that reduce the cumulative cost of accessing multiple platforms. Additionally, expanding the availability of regional content across affordable tiers may reduce reliance on pirated alternatives in price-sensitive markets. Governments may also consider incentivising

legitimate OTT adoption through tax benefits, subsidies for domestic content platforms, or public-private partnerships aimed at expanding digital content accessibility. These measures recognise piracy not merely as a legal violation but as a market substitution phenomenon.

International Coordination and Cross-Border Enforcement

Given the transnational nature of OTT piracy, unilateral enforcement measures are inherently limited. A harmonised international framework for digital copyright enforcement is therefore essential. Such a framework could include a global fast-track takedown protocol for infringing domains, enabling expedited removal of piracy websites across multiple jurisdictions based on a single verified complaint. Additionally, an international registry of repeat infringing domains and hosting providers could improve transparency and enforcement efficiency. Enhanced cooperation between national regulatory authorities, particularly in relation to domain registration, hosting services, and payment intermediaries, would further reduce the operational resilience of piracy networks.

Synthesis of Reform Strategy

The reform measures outlined above reflect the need for a multi-dimensional enforcement strategy that integrates legal, technological, economic, and international dimensions. Importantly, the objective is not to eliminate piracy entirely, an unrealistic goal in digital ecosystems but to significantly reduce its scale, accessibility, and economic viability. A successful reform framework must therefore move beyond reactive enforcement and toward a proactive governance model in which deterrence is embedded within both legal structures and technological infrastructures. This requires sustained coordination between lawmakers, courts, industry stakeholders, and international partners.

CONCLUSION

The analysis undertaken in this paper demonstrates that OTT piracy represents a structurally complex phenomenon that cannot be effectively addressed through isolated legal or technological interventions. While India's statutory framework, judicial innovations, and technological enforcement mechanisms collectively provide a multi-layered response, they remain fundamentally reactive, fragmented, and dependent on post-infringement action. The evolution of OTT platforms has transformed not only the distribution of audiovisual content but also the nature of copyright infringement itself, shifting it toward decentralised, transnational, and technologically adaptive networks. In response, courts have expanded injunctive remedies, intermediaries have strengthened compliance mechanisms, and platforms have deployed increasingly sophisticated technological safeguards. However, these measures operate within structural constraints imposed by territorial jurisdiction, economic incentives, and the inherent adaptability of digital piracy networks. Ultimately, the persistence of OTT piracy reflects a deeper regulatory mismatch between static legal frameworks and dynamic technological ecosystems. Addressing this mismatch requires a shift toward integrated governance models that combine statutory reform, institutional coordination, technological standardisation, and international

cooperation. In conclusion, the effective protection of copyright in the OTT era depends not on the supremacy of any single enforcement mechanism, but on the creation of a coherent, adaptive, and globally coordinated regulatory ecosystem capable of responding to the evolving realities of digital content distribution.

REFERENCES

A. Books (Core doctrinal sources)

1. Lessig L, *Code and Other Laws of Cyberspace* (Basic Books 1999)
2. Landes WM and Posner RA, *The Economic Structure of Intellectual Property Law* (Harvard University Press 2003)
3. Cornish W, Llewelyn D and Aplin T, *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (Sweet & Maxwell 2019)

B. Statutes and International Instruments

4. Copyright Act 1957 (India)
5. Information Technology Act 2000 (India)
6. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India)
7. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) 1994
8. Berne Convention for the Protection of Literary and Artistic Works 1886
9. Digital Millennium Copyright Act 1998 (US)
10. Directive (EU) 2019/790 on Copyright in the Digital Single Market

C. Case Law (India – essential core)

11. *Shreya Singhal v Union of India* (2015) 5 SCC 1
12. *Super Cassettes Industries Ltd v MySpace Inc* 2016 SCC OnLine Del 6382
13. *UTV Software Communications Ltd v 1337x.to* 2019 SCC OnLine Del 8002
14. *Eros International Media Ltd v BSNL* 2016 SCC OnLine Del 6227
15. *Disney Enterprises Inc v Kimcartoon* (Delhi High Court, 2019)

D. Reports / Institutional Publications

16. World Intellectual Property Organization (WIPO), *Copyright and Artificial Intelligence Report* (2021)
17. European Union Intellectual Property Office (EUIPO), *Online Copyright Infringement Report* (latest edition)
18. Organisation for Economic Co-operation and Development (OECD), *Piracy in Digital Markets Report*

E. Technology / Industry Sources

19. Google, *Content ID System Overview* (YouTube Copyright Enforcement Documentation)
20. Netflix Technology Blog, *Digital Rights Management and Content Protection Systems* (industry publication)