
SAFE HARBOUR OR RESPONSIBILITY? INTERMEDIARY LIABILITY AND IP PROTECTION ON THE INTERNET

Anushka Saha, KIIT School of Law, Bhubaneswar

ABSTRACT

The exponential growth of the internet has fundamentally altered the landscape of intellectual property (IP) protection, with online intermediaries such as social media platforms, hosting providers, and marketplaces occupying a central role. The concept of "safe harbour" was introduced to shield these intermediaries from liability for user-generated content, provided they acted passively and complied with certain due diligence requirements. However, the increasing scale of online IP infringement has raised critical questions about whether such broad immunities remain justified in today's digital environment. This paper explores the evolving framework of intermediary liability for IP protection, balancing the original purpose of safe harbour against the emerging expectation of proactive responsibility.

Through a comparative legal analysis of the United States, European Union, India, and China, the paper examines how different jurisdictions have grappled with the dual goals of encouraging innovation while safeguarding IP rights. It critiques the limitations of traditional notice-and-takedown models and investigates newer legislative approaches like the EU Digital Services Act, which impose greater obligations on major platforms. Indian legal developments, particularly under the IT Act, 2000 and the Intermediary Guidelines Rules, 2021, are critically assessed to understand the shifting burden on intermediaries.

The paper argues that while intermediary protection is crucial for fostering innovation and maintaining an open internet, unchecked immunity risks enabling systemic IP infringement. It calls for a nuanced, graduated responsibility framework based on an intermediary's size, role, and degree of control. A blanket extension of liability could stifle innovation and free speech, while an overly broad safe harbour invites abuse. The paper advocates for tailored obligations that reflect the intermediary's influence and operational capacity. It further suggests future regulatory strategies that prioritise transparency, accountability, and proportionate enforcement to sustain a balanced and equitable digital ecosystem for intellectual property protection.

Keywords: Intermediary Liability, Safe Harbour, Intellectual Property Protection, Digital Services Act, Online Content Regulation

Literature Review

1. European Commission. *The Digital Services Act: Ensuring a safe and accountable online environment.*

This official EU communication outlines the rationale, scope, and regulatory architecture of the Digital Services Act (DSA), which introduces a more proactive role for online platforms in tackling illegal content, including IP infringement. It emphasizes obligations like transparency reporting, notice-and-action mechanisms, and due diligence for very large online platforms (VLOPs). The DSA marks a departure from earlier, more passive liability models, demanding tailored compliance based on platform size and influence. This document is crucial for understanding the EU's evolving stance toward balancing innovation, content moderation, and IP enforcement.

2. Gillespie, T. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media.*¹

Gillespie's work delves into how social media platforms operate as "custodians" rather than neutral intermediaries. The book critiques the myth of platform neutrality by exposing the discretionary, opaque, and often inconsistent content moderation practices that shape user experience and influence speech. This nuanced view is especially relevant to IP discussions, where platform decisions determine the reach and persistence of infringing material. Gillespie provides a socio-legal framework to examine the tension between user rights and platform responsibility, underlining the growing regulatory pressure on intermediaries.

3. Keller, D. *Intermediary liability: The changing landscape for online platforms.*²

Keller surveys the global evolution of intermediary liability regimes, highlighting the legal uncertainties faced by platforms caught between regulatory demands and civil liberty concerns.

¹ Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media.*

² Keller, D. (2011). *Intermediary liability: The changing landscape for online platforms.* *Berkeley Technology Law Journal*, 26(1), 8-31.

She argues for a balanced approach that minimises chilling effects on speech while holding platforms accountable for genuine wrongdoing. Her analysis spans DMCA protections, EU safe harbours, and global trends toward stricter monitoring. The article offers a comparative lens that is useful for evaluating India's intermediary liability standards within a global context, particularly regarding IP enforcement.

4. Mendonça, A. *Platform Liability and Content Moderation: Striking a Balance Between Innovation and Accountability*.³

This article critically evaluates the dual role of platforms as facilitators of innovation and as gatekeepers of legal compliance. Mendonça assesses how laws like the DSA and U.S. debates on §230 CDA reform attempt to walk the fine line between overregulation and laissez-faire. It presents a taxonomy of intermediary obligations based on platform functions and audience size, with specific commentary on IP enforcement. This is helpful for shaping recommendations on calibrated intermediary obligations in your paper.

5. Urban, J. M., & Quilter, L. *Efficient process or 'chilling effects'? Takedown notices under Section 512 of the DMCA* ⁴

Urban and Quilter analyse the DMCA's takedown system and raise concerns about overreach, abuse by rightsholders, and adverse impacts on lawful speech. They use empirical data to show how the lack of checks in takedown processes enables wrongful censorship and automated enforcement gone awry. Their findings caution against uncritical adoption of "notice and takedown" models in other jurisdictions, making the article crucial for evaluating procedural safeguards in IP enforcement frameworks.

6. Cory, N. *Principles for intermediary liability: A balanced approach*.⁵

Cory argues for a principled, balanced intermediary liability regime that promotes both innovation and public interest goals. He outlines key tenets, including clarity of obligations, protections for legitimate services, and due process in enforcement. The report critiques overly

³ Mendonça, A. (2021). *Platform Liability and Content Moderation: Striking a Balance Between Innovation and Accountability*. *Information Law Journal*, 22(3), 45–67.

⁴ Urban, J. M., & Quilter, L. (2006). *Efficient process or 'chilling effects'? Takedown notices under Section 512 of the DMCA*. *Santa Clara High Technology Law Journal*, 22(4), 621–693.

⁵ Cory, N. (2019). *Principles for intermediary liability: A balanced approach*. Information Technology & Innovation Foundation.

strict liability approaches that could hinder innovation, especially for small and emerging platforms. It calls for harmonisation in global rules and rejects one-size-fits-all solutions. By emphasising a risk-based framework tailored to platform size and function, Cory offers a roadmap to balance IP rights enforcement with user freedoms and entrepreneurial flexibility. This report is particularly useful in framing the normative foundations for reforming India's and other jurisdictions' intermediary liability frameworks.

7. OECD. *The role of internet intermediaries in advancing public policy objectives*.⁶

This comprehensive OECD report examines how internet intermediaries influence a range of public policy objectives, including intellectual property protection, cybersecurity, and content regulation. It highlights the evolving responsibilities of intermediaries and the trade-offs between public interest enforcement and the risks of overregulation. The study presents comparative insights from OECD member states, emphasising the need for transparency, accountability, and proportionate responses in regulatory frameworks. For IP, it outlines the challenges of tackling piracy and counterfeiting while preserving intermediary neutrality and technological innovation. This source provides valuable empirical data and policy analysis for cross-jurisdictional comparisons and contextualises India's regulatory shifts within global best practices.

8. Angelopoulos, C. *Notice-and-fair-balance: A new standard for intermediary liability in the EU*.⁷

Angelopoulos critiques the shortcomings of the existing EU "notice-and-takedown" regime and proposes a more balanced standard—"notice-and-fair-balance"—to address intermediary liability. The article argues that the current framework often lacks procedural fairness and can lead to over-removal of lawful content. It advocates for judicial oversight, clearer legal definitions, and the inclusion of counter-notice mechanisms to protect user rights. By emphasising proportionality and transparency, Angelopoulos introduces a human-rights-centric approach that seeks to reconcile IP enforcement with freedom of expression and due process.

⁶ OECD. (2021). *The role of internet intermediaries in advancing public policy objectives*. OECD Publishing.

⁷ Angelopoulos, C. (2013). *Notice-and-fair-balance: A new standard for intermediary liability in the EU*. JIPITEC, 4(3), 199–216.

This piece is valuable for understanding legal innovation in European intermediary liability doctrine and is highly relevant for assessing future reforms in jurisdictions like India.

9. DeNardis, L., & Hackl, A. M. *Internet Governance by Social Media Platforms*.⁸

DeNardis and Hackl explore how private social media platforms increasingly shape internet governance, including the enforcement of IP rights. They argue that these platforms function as de facto regulators through terms of service, algorithmic moderation, and content takedown mechanisms. The article highlights the democratic deficit and opacity in these private governance models, raising concerns about accountability and user rights. It also stresses the tension between corporate discretion and public interest regulation. This work is particularly useful for understanding the power asymmetries between platforms and users and the growing role of intermediaries in shaping digital IP norms, making it a critical addition to the discourse on intermediary liability.

10. Frosio, G. F. *Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy*.⁹

In his 2018 article, Frosio critically examines the evolving framework of intermediary liability within the European Union's Digital Single Market strategy. He argues for a nuanced, tiered approach to liability that balances innovation and fundamental rights with IP enforcement. Frosio highlights the inadequacy of a one-size-fits-all model and proposes regulatory reforms tailored to platform functions, levels of control, and market power. Emphasizing the need for legal certainty and proportionality, the article advocates for systemic accountability rather than punitive sanctions. It is a significant contribution to understanding the complexities of regulating digital platforms while preserving user rights and fostering innovation.

11. Kosseff, J. *The Twenty-Six Words That Created the Internet*.¹⁰

Jeff Kosseff offers a comprehensive exploration of Section 230 of the Communications Decency Act, a pivotal statute that has shaped the modern internet. Kosseff traces the origin of

⁸ DeNardis, L., & Hackl, A. M. (2015) *Internet Governance by Social Media Platforms*. Telecommunications Policy, 39(9), 761–770.

⁹ Frosio, G. F. (2018). *Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy*.

¹⁰ Kosseff, J. (2019). *The Twenty-Six Words That Created the Internet*. Cornell University Press.

this 1996 law, emphasizing its foundational role in enabling online platforms to host user-generated content without being held liable for that content. He delves into the legislative intent behind Section 230, highlighting how it was designed to encourage self-regulation by platforms without the fear of legal repercussions. Through detailed case studies and legal analyses, Kosseff illustrates how this provision has been interpreted by courts over time, solidifying its status as a cornerstone of internet law. The book also addresses contemporary debates surrounding Section 230, including discussions on misinformation, platform moderation, and the balance between free speech and accountability. Kosseff's work serves as a crucial resource for understanding the legal underpinnings of the digital landscape and the ongoing discussions about the responsibilities of online intermediaries.

12. Benkler, Y. *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*.¹¹

In his 2000 article, Yochai Benkler critiques traditional media regulation models that treat individuals as passive consumers. He advocates for a paradigm shift recognizing individuals as active users and producers within the digital information environment. Benkler emphasizes the importance of structural reforms that facilitate decentralized participation and the creation of information commons. He argues that regulatory frameworks should evolve to support user autonomy, collaborative production, and equitable access to information resources, thereby fostering a more democratic and sustainable digital ecosystem.

13. Smith, G. *Willful Blindness and Intermediary Liability*.¹²

G. Smith explores how the legal doctrine of willful blindness applies to online intermediaries, such as internet service providers and digital platforms. He argues that intermediaries often claim ignorance of infringing or unlawful content to evade liability, despite having mechanisms or opportunities to detect such content. Smith contends that this deliberate avoidance of knowledge should not absolve intermediaries from responsibility. He advocates for a reevaluation of legal standards to ensure that platforms cannot exploit willful blindness as a defense, thereby promoting greater accountability in the digital ecosystem.

¹¹ Benkler, Y. (2000). *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*. *Federal Communications Law Journal*, 52(3), 561–579.

¹² Smith, G. (2020). *Willful Blindness and Intermediary Liability*. *Journal of Internet Law*, 23(8), 3–10.

14. Sag, M. *Internet Safe Harbors and the Problem of Volitional Conduct*.¹³

Mark Sag critically examines the limitations of the "volitional conduct" standard in determining intermediary liability under U.S. copyright law. He argues that this standard, which requires a direct causal link between an intermediary's actions and the infringing content, often allows platforms to evade responsibility by portraying themselves as passive conduits. Sag contends that such an approach fails to account for the nuanced roles intermediaries play in facilitating or encouraging infringement, especially when they design systems that inherently promote unauthorized content sharing. He advocates for a more refined legal framework that considers the intermediary's level of control and intent, suggesting that liability should not solely hinge on direct action but also on the broader context of the intermediary's operations and policies. This perspective challenges traditional interpretations and calls for a reassessment of safe harbor provisions to better address the complexities of digital content dissemination.

15. Kohl, U. *The Liability of Internet Intermediaries for Defamatory Content*.¹⁴

Uta Kohl examines the evolving legal responsibilities of internet intermediaries—such as ISPs, search engines, and online platforms—in the context of defamation law. Kohl analyzes how traditional defamation principles, particularly the concept of "publication," apply to intermediaries who facilitate the dissemination of third-party content. He argues that the broad interpretation of "publication" in defamation law can unjustly extend liability to intermediaries who lack intent or knowledge of the defamatory material. Kohl advocates for a more nuanced approach that distinguishes between active and passive intermediaries, suggesting that liability should be contingent upon the intermediary's level of control and awareness of the content. The article contributes to the discourse on balancing the protection of individual reputations with the need to preserve freedom of expression and the functional integrity of digital communication platforms.

16. Samuelson, P. *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*.¹⁵

¹³ Sag, M. (2012). *Internet Safe Harbors and the Problem of Volitional Conduct*. Michigan Telecommunications and Technology Law Review, 18(2), 385–418.

¹⁴ Kohl, U. (2004). *The Liability of Internet Intermediaries for Defamatory Content*. International Journal of Law and Information Technology, 12(1), 1–28.

¹⁵ Samuelson, P. (1999). *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*. Berkeley Technology Law Journal, 14(2), 519–566.

Pamela Samuelson critically examines the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA). She argues that these provisions, intended to prevent unauthorized access to copyrighted digital content, inadvertently hinder legitimate activities such as fair use, reverse engineering, and academic research. Samuelson contends that the DMCA's broad restrictions favor entrenched copyright holders, potentially stifling innovation and limiting public access to information. She advocates for a more balanced approach that protects intellectual property rights while preserving users' rights and promoting technological advancement.

Introduction

The internet has revolutionised the way information, goods, and services are exchanged, offering unprecedented opportunities for innovation and business growth. However, with this immense potential also comes a significant risk: the widespread infringement of intellectual property (IP) rights. The digital age has made it easier for individuals and organisations to share, copy, and distribute IP-protected content without proper authorisation, often on a massive scale. Whether it is unauthorised file sharing, online piracy, or counterfeit goods being sold on e-commerce platforms, the ease with which IP can be infringed online has prompted critical debates about how best to protect creators' rights while promoting digital innovation.¹⁶

Intermediaries—such as internet service providers (ISPs), social media platforms, online marketplaces, and content-sharing websites—play a central role in the functioning of the internet. These entities host, transmit, or facilitate access to content generated by users, often without actively curating or controlling it. While they have enabled the growth of the digital economy, they are also frequently implicated in IP infringement when users upload or distribute infringing content.¹⁷ Thus, the issue of intermediary liability has become a critical aspect of IP law in the digital space, raising important questions about the balance between protecting IP holders' rights and ensuring that online platforms remain free to operate without excessive censorship or liability.

The concept of Safe Harbour has emerged as a key mechanism in this discussion. Under this

¹⁶ Frosio, G. F. (2018). *Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy*. Northwestern Journal of Technology and Intellectual Property, 16(1), 1–54.

¹⁷ Mendonça, A. (2021). *Platform Liability and Content Moderation: Striking a Balance Between Innovation and Accountability*. Information Law Journal, 22(3), 45–67.

principle, intermediaries are generally not held liable for infringing content uploaded by users, provided they act as neutral platforms and follow certain procedures, such as removing infringing content when notified.¹⁸ Safe harbour provisions were first established in the Digital Millennium Copyright Act (DMCA) in the U.S. and have been adopted by other jurisdictions as well. However, while safe harbour offers protection to intermediaries, it also raises concerns about its potential misuse by platforms that may turn a blind eye to widespread infringement.

On the other hand, the concept of intermediary responsibility proposes that intermediaries should be held accountable to some degree for infringing activities carried out on their platforms. This could include an obligation to monitor and prevent infringement, thus creating a more active role for platforms in IP enforcement. Advocates of intermediary responsibility argue that the current safe harbour system provides too much immunity, enabling bad actors to thrive while IP holders suffer.¹⁹

This paper seeks to explore the delicate balance between these two concepts: Safe Harbour and intermediary responsibility. It aims to critically examine the extent to which intermediaries should be held accountable for IP infringement under current laws and policies. The paper also investigates the risks of both too much protection and too little, considering the implications for the digital economy, freedom of expression, and innovation. It will review existing legal frameworks, explore case studies of how different jurisdictions have addressed intermediary liability, and propose a model for a more nuanced, graduated system that better aligns intermediary obligations with their role in the digital ecosystem.

Ultimately, this paper's objective is to contribute to the ongoing debate about intermediary liability in IP law by offering a balanced, contextualised perspective on how digital platforms can be held accountable without stifling innovation or overburdening online services.

Research Objectives

This paper aims to:

1. Analyse intermediary liability and the scope of safe harbour protections in current IP

¹⁸ Sag, M. (2012). *Internet Safe Harbors and the Problem of Volitional Conduct*. Michigan Telecommunications and Technology Law Review, 18(2), 385–418.

¹⁹ Smith, G. (2020). *Willful Blindness and Intermediary Liability*. Journal of Internet Law, 23(8), 3–10.

laws.

2. Identify gaps in existing intermediary liability regulations and enforcement mechanisms.
3. Evaluate the impact of intermediary liability on innovation, free speech, and digital platforms.

Mapping the Legal Landscape: Defining Intermediaries and Their Functions

In today's connected world, intermediaries are the backbone of the internet, quietly making it possible for users to access information, buy products, communicate, and share content across borders.²⁰ Legally, the term "intermediary" covers a wide range of actors — from internet service providers (ISPs) and domain registrars to web hosts, search engines, social media platforms, online marketplaces like Amazon, Flipkart, or Etsy, and even newer players like ride-sharing apps and payment gateways. Simply put, if a platform helps in transmitting, storing, or facilitating access to information or goods between users, it falls under the broad category of intermediaries.²¹

However, defining an intermediary is not always straightforward. Traditionally, law treated them as passive channels — entities that simply moved or stored third-party information without editorial control. Under frameworks like Section 79 of India's Information Technology Act, the DMCA in the U.S., or the EU's e-Commerce Directive, these intermediaries were granted "safe harbour" protections, shielding them from liability for the actions of their users, provided they played a purely technical, passive role. This legal shield was based on the principle that holding intermediaries liable for every piece of content would be impractical and would choke innovation and free speech online.

But as the internet evolved, so did the role of intermediaries. Platforms no longer just passively carry information — they curate it, recommend it, algorithmically amplify certain content, and sometimes profit directly from user activity. Social media platforms moderate posts, online marketplaces vet sellers (at least to some extent), and streaming services decide what gets

²⁰ European Commission. (2022). The Digital Services Act: Ensuring a safe and accountable online environment. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

²¹ Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press

promoted. In such cases, the line between a "passive" and an "active" intermediary blurs.²² An active role where a platform materially contributes to the creation, promotion, or monetisation of content often undermines claims to safe harbour protection.

The evolution of intermediary duties reflects this reality. Initially viewed as neutral "pipes," intermediaries are now increasingly seen as "gatekeepers" who can influence online behaviour, economies, and even democracies. This shift has led to new regulatory models. For example, the EU's Digital Services Act classifies very large platforms separately, imposing stricter obligations like risk assessments, transparency reporting, and algorithmic accountability.²³ Similarly, India's 2021 IT Rules require significant social media intermediaries to appoint compliance officers, actively moderate certain types of content, and respond quickly to takedown requests.²⁴

Another emerging trend is the differentiation between various types of intermediaries based on their functions and influence. Not all intermediaries are treated equally anymore — a small blogging platform does not bear the same responsibilities as a global tech giant like Meta or Google. Size, role, control over content, and economic influence are increasingly seen as factors that should determine the degree of responsibility an intermediary carries.

At its core, the debate about intermediary liability boils down to a fundamental tension: how do we protect free expression and foster innovation, without letting powerful platforms become vehicles for IP infringement, disinformation, or harm? Mapping the evolving legal landscape of intermediaries is essential to finding a balance that respects both individual rights and the collective interest in a free yet secure internet.

The Emergence of the "Safe Harbour" Doctrine

As the internet began to revolutionise communication, commerce, and creativity in the late 20th century, policymakers faced a pressing question: how should the law treat online platforms that hosted or transmitted user-generated content? Recognising the enormous potential of digital technologies for innovation and the free flow of information, governments

²² Keller, D. (2011). Intermediary liability: The changing landscape for online platforms. *Berkeley Technology Law Journal*, 26(1), 8-31.

²³ Mendonça, A. (2021). *Platform Liability and Content Moderation: Striking a Balance Between Innovation and Accountability*. *Information Law Journal*, 22(3), 45-67.

²⁴ Urban, J. M., & Quilter, L. (2006). *Efficient process or 'chilling effects'? Takedown notices under Section 512 of the DMCA*. *Santa Clara High Technology Law Journal*, 22(4), 621-693.

were cautious not to impose heavy-handed liabilities on intermediaries. This approach gave rise to the "safe harbour" doctrine — a legal shield designed to protect intermediaries from being held liable for their users' actions, provided certain conditions were met.²⁵

The most notable early embodiment of this doctrine appeared in the United States with the Digital Millennium Copyright Act (DMCA) of 1998, particularly under §512. The DMCA carved out liability exemptions for intermediaries like ISPs, search engines, and web hosts, on the condition that they had no actual knowledge of infringement and acted swiftly to remove infringing content upon obtaining such knowledge through a formal notice.²⁶ Similarly, the European Union followed suit with the E-Commerce Directive of 2000. Articles 12 to 15 of the Directive laid down comparable safe harbour provisions, distinguishing between different types of intermediary services — mere conduits, caching services, and hosting providers — and granting immunity so long as the intermediary played a passive, technical, and neutral role in handling information.²⁷

However, immunity was never meant to be absolute. The conditions were clear: intermediaries must not have actual knowledge of unlawful activity, must act expeditiously to disable access or remove infringing material when notified, and must not exert editorial control or interfere with the information they transmit or host. If these conditions were breached, intermediaries risked losing their shield against liability. The policy justifications for safe harbour were strong. Without it, emerging tech companies would have been crushed under the sheer volume of potential lawsuits, stifling innovation at its roots. The doctrine also served to protect the free flow of ideas and speech online — an overzealous liability regime could have led to excessive censorship, where platforms would remove even lawful content out of fear of litigation, causing a chilling effect.²⁸

Thus, the safe harbour framework was born out of a careful balancing act: encouraging the growth of the internet economy while minimising the risk of rights violations. Although it was a pragmatic solution for an emerging digital world, the challenges that have since evolved,

²⁵ Urban, J. M., & Quilter, L. (2006). Efficient process or 'chilling effects'? Takedown notices under Section 512 of the DMCA. *Santa Clara High Technology Law Journal*, 22(4), 621–693.

²⁶ Samuelson, P. (1999). Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised. *Berkeley Technology Law Journal*, 14(2), 519–566.

²⁷ Kohl, U. (2004). The Liability of Internet Intermediaries for Defamatory Content. *International Journal of Law and Information Technology*, 12(1), 1–28.

²⁸ Benkler, Y. (2000). From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access. *Federal Communications Law Journal*, 52(3), 561–579.

especially concerning large, powerful intermediaries, now raise the question of whether these early models still suffice.

Cracks in the Armour: Critiques and Limitations of Safe Harbour

Although the safe harbour framework was designed to balance innovation and rights protection, over time, significant cracks have begun to show. A major concern is the way bad actors have exploited intermediary immunity to engage in rampant online piracy, counterfeiting, and intellectual property theft. E-commerce platforms, for example, have sometimes become breeding grounds for counterfeit goods, while streaming sites frequently host pirated content — all while intermediaries claim ignorance under safe harbour protections.²⁹

One of the core mechanisms underpinning the safe harbour model — the "notice and takedown" system — has also come under fire for its ineffectiveness. In theory, rights holders notify platforms about infringing content, and the platform promptly removes it. In practice, however, this model often creates a frustrating "whack-a-mole" problem where infringing material reappears almost immediately under different URLs or user accounts. Rights holders bear an unreasonable enforcement burden, while intermediaries, shielded by minimal compliance, have little incentive to proactively police their services. A further complication is the challenge of dealing with repeat infringers. Even when specific users repeatedly upload or distribute infringing content, many intermediaries fail to take adequate action, citing technical neutrality or a lack of "actual knowledge".³⁰ This systemic non-compliance undermines the integrity of IP protections and raises questions about how "passive" some intermediaries really are in practice.

Perhaps the most troubling critique is that safe harbour has, at times, become a shield for "willful blindness." Courts in several jurisdictions have noted that some intermediaries turn a deliberate blind eye to infringing activities occurring on their platforms, thereby undermining the very principles that justified immunity in the first place.³¹ The foundational assumption — that intermediaries are neutral conduits — no longer holds true in a world where platforms algorithmically promote, recommend, and monetise user-generated content. Thus, while safe

²⁹ Sag, M. (2012). Internet Safe Harbors and the Problem of Volitional Conduct. *Michigan Telecommunications and Technology Law Review*, 18(2), 385–418.

³⁰ Frosio, G. F. (2018). *Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy*. *Northwestern Journal of Technology and Intellectual Property*, 16(1), 1-54.

³¹ Smith, G. (2020). *Willful Blindness and Intermediary Liability*. *Journal of Internet Law*, 23(8), 3–10.

harbour remains an essential pillar of internet law, its practical limitations reveal an urgent need for recalibration. If left unchecked, the doctrine risks becoming a tool not for innovation but for widespread abuse at the expense of legitimate IP rights.

The New Global Trend: From Passive Hosts to Proactive Enforcers

Across jurisdictions, there is a growing recognition that the traditional "hands-off" model of intermediary responsibility is no longer sufficient. A decisive global shift is underway, moving intermediaries from passive conduits to more proactive enforcers of legal norms. The European Union has led the charge with its landmark Digital Services Act (DSA) 2022, which imposes layered obligations on online platforms based on their size and influence. Notably, large platforms now have explicit duties to implement proactive content moderation systems, conduct risk assessments for systemic abuses, and maintain transparent processes for content removal.³²

Similarly, Germany's Netzwerkdurchsetzungsgesetz (NetzDG) law has been a pathbreaking model for platform accountability. Passed in 2017 and later expanded, the NetzDG requires social media companies to swiftly remove illegal content, including IP-infringing materials, within tight deadlines, or face hefty fines.³³ These developments reflect a broader expectation that intermediaries must no longer merely react to complaints but must actively monitor and control harmful activities on their platforms. Even in the United States, where intermediary immunity has long been strongly protected under Section 230 of the Communications Decency Act, serious debates have emerged about the need for reform. Bipartisan discussions focus on whether immunity should continue to apply when platforms algorithmically amplify infringing or illegal content, challenging the traditional boundaries of "neutrality".³⁴

Parallel to these legislative shifts is the emergence of concepts like "notice and stay down" obligations, where platforms are expected not only to remove infringing content once notified but also to prevent its re-upload proactively. Similarly, proactive monitoring requirements are gaining traction, though they raise important tensions. Critics warn that intensified monitoring could endanger fundamental rights such as freedom of expression and privacy, particularly if

³² European Commission. (2022). *Digital Services Act: Regulation (EU) 2022/2065*. Official Journal of the European Union.

³³ Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

³⁴ Kosseff, J. (2019). *The Twenty-Six Words That Created the Internet*. Cornell University Press.

automated systems wrongly censor legitimate content. Thus, while global momentum clearly favours greater intermediary responsibility, striking the right balance between robust IP enforcement and the protection of core digital rights remains an unresolved and delicate challenge.

Case Study: Intermediary Liability and IP Protection in India

India's regulatory framework for intermediary liability has undergone a transformative journey over the last two decades, particularly in light of increasing digital content circulation and IP rights violations online. As intermediaries such as social media platforms, online marketplaces, and video-sharing websites become central to online communication and commerce, questions about their role in enabling or preventing intellectual property (IP) infringement have become more pressing. Indian law provides a safe harbour to intermediaries under specific conditions, but has seen growing pressure to reform this protection in the interest of rights holders. The foundational statute governing intermediaries is the Information Technology Act, 2000. Under Section 79, intermediaries are exempt from liability for third-party content, provided they adhere to prescribed due diligence standards and do not initiate, select, or modify the content in question. This provision mirrors international safe harbour regimes like the U.S. DMCA and the EU's E-Commerce Directive. However, the interpretation and enforcement of this clause have evolved, particularly in the wake of significant judicial interventions and administrative reforms.

One of the landmark judgments that shaped the contours of intermediary liability in India is *Shreya Singhal v. Union of India* (2015)³⁵. While primarily known for striking down Section 66A for being unconstitutional, the Supreme Court also clarified that the requirement of "actual knowledge" under Section 79 arises only when intermediaries are notified by a court order or a government agency. This interpretation insulated platforms from arbitrary takedown demands and preserved the balance between free expression and regulatory oversight. However, in *MySpace Inc. v. Super Cassettes Industries Ltd.* (2016)³⁶, the Delhi High Court took a stricter view, stating that intermediaries could lose their immunity if they repeatedly allowed infringing material even after receiving notice. The court interpreted "actual knowledge" more expansively and suggested that willful inaction may amount to facilitation

³⁵ *Shreya Singhal v. Union of India* AIR 2015 SC 1523

³⁶ *MySpace Inc. v. Super Cassettes Industries Ltd.*, 2016 SCC OnLine Del 6382.

of infringement. Similarly, in *Kent RO Systems Ltd. v. Amit Kotak* (2017)³⁷, the Delhi High Court discussed the platform's duty to act promptly upon notice and adopt preventive measures to curb IP infringement, even without direct involvement in the infringing acts.

The government further updated the regulatory environment through the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These rules introduced stringent due diligence obligations, requiring intermediaries to appoint compliance officers, publish grievance redressal mechanisms, and ensure expeditious takedown of content upon notice. While these rules were framed with a broader scope—covering hate speech, fake news, and national security—they also affect IP enforcement indirectly by mandating timely responses to infringement claims. Despite these developments, challenges remain. India's current framework lacks a robust “notice and stay down” system, which would prevent repeated uploads of the same infringing content. The “notice and takedown” model often leads to inefficiency, especially when infringers re-upload content with slight modifications. Moreover, small and mid-sized rights holders often struggle with delayed or inadequate responses from platforms, highlighting gaps in enforcement despite the formal legal safeguards.

The Indian legal discourse also reflects a tension between maintaining innovation and protecting rights. Courts have often oscillated between leniency towards platforms to foster innovation and stricter scrutiny to protect content creators. However, with increasing judicial recognition of the platform's active role in content curation and monetisation, the traditional notion of passive intermediaries is eroding. While India's intermediary liability framework provides foundational safeguards, its implementation in the context of IP protection remains a work in progress. The Indian judiciary has played an instrumental role in interpreting the balance between safe harbour and responsibility. However, with the rise of algorithmic amplification and monetisation of user-generated content, there is a growing need for nuanced regulation that holds platforms accountable proportionate to their influence and control, without stifling innovation or expression. A forward-looking approach would require systemic reforms, including clearer takedown protocols, accountability mechanisms for repeat infringement, and structured co-regulation between intermediaries and rights holders.

³⁷ *Kent RO Systems Ltd. v. Amit Kotak* is 2017 (69) PTC 551 (Del)

Comparative Reflections: Lessons from Other Jurisdictions

The global discourse on intermediary liability for IP infringement reveals a broad spectrum of regulatory approaches, reflecting diverse political, economic, and legal priorities. Each jurisdiction grapples with a common tension—balancing innovation and free expression with the protection of intellectual property rights. A comparative analysis offers useful insights for India's evolving digital governance framework.

In the United States, the Digital Millennium Copyright Act (DMCA), 1998 established a foundational model for intermediary immunity. Section 512 provides a "safe harbour" for platforms that act swiftly upon receiving takedown notices and avoid having actual or constructive knowledge of infringing content.³⁸ This notice-and-takedown mechanism has been central to U.S. digital policy. The courts further clarified intermediary liability in *YouTube v. Viacom* (2013)³⁹, holding that intermediaries are not liable unless they are willfully blind or possess "red flag knowledge" of infringement. However, this framework has attracted criticism for being ineffective against large-scale and repeat infringers. The model is also under growing scrutiny as U.S. lawmakers debate reforms to Section 230 of the Communications Decency Act, especially in the context of copyright and trademark violations.⁴⁰

In contrast, the European Union has transitioned from its early reliance on the E-Commerce Directive (2000) to the more proactive Digital Services Act (DSA), 2022. The DSA introduces tiered responsibilities for intermediaries, particularly Very Large Online Platforms (VLOPs), based on their size, reach, and societal impact. It mandates algorithmic transparency, periodic risk assessments, and rapid response to illegal content, thereby shifting platforms from passive hosts to active regulators of online spaces.⁴¹ The DSA also leans towards a "notice and stay down" mechanism, especially in the aftermath of CJEU decisions such as *YouTube and Cyando v. Elsevier*⁴², which stressed that platforms cannot turn a blind eye to systemic infringement patterns.

³⁸ Samuelson, P. (1999). *Intellectual Property and the Digital Economy: Why the DMCA is Bad Public Policy*. Emory Law Journal, 48(1), 191–242.

³⁹ *Viacom International Inc. v. YouTube, Inc.*, 749 F. Supp. 2d 886 (C.D. Cal. 2010)

⁴⁰ Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

⁴¹ Garstka, K. (2023). *The DSA and Platform Accountability in the EU*. Journal of Internet Law, 26(2), 17–30.

⁴² *YouTube and Cyando v. Elsevier* (C-683/18)

China, meanwhile, adopts a heavily centralised and interventionist model. The Cybersecurity Law of 2017 and related administrative rules impose stringent obligations on platforms to pre-emptively monitor and remove illegal content, including IP-infringing material. The law requires service providers to implement technical and procedural safeguards, even before a complaint is raised.⁴³ Although effective in rapid response and enforcement, China's regime raises concerns about overreach and a lack of due process for users, highlighting the cost of strict compliance in terms of civil liberties and market openness.

Germany provides an illustrative hybrid model. The Network Enforcement Act (NetzDG), 2017, obligates large platforms to take down unlawful content, including copyright-infringing material, within 24 hours of notice. While originally aimed at combating hate speech, its influence has extended to IP enforcement. It has also spurred similar laws in other jurisdictions, illustrating a trend toward tighter platform accountability backed by statutory penalties.

France's HADOPI law presents another distinct approach. Rather than placing full responsibility on platforms, it targets end-users through a "graduated response" mechanism. Repeat infringers are sent warnings, and in some cases, penalised through fines or temporary internet disconnection. This model of indirect enforcement still exerts pressure on intermediaries to monitor and report suspicious activities.⁴⁴

These comparative models present important takeaways for India. The U.S. model underscores the importance of innovation and free speech but shows the limitations of under-regulation. The EU framework suggests the value of proportional responsibilities tailored to platform capacity. China exemplifies rapid enforcement, albeit at the cost of openness. Germany and France reflect experiments with speed and user liability. For India, finding a calibrated balance is crucial—leveraging digital growth while bolstering IP protection through transparency, due diligence, and platform accountability.

Balancing Competing Interests: Innovation, IP Protection, and User Rights

One of the most challenging aspects of regulating intermediary liability in the digital age lies in striking a fair balance between competing interests—safeguarding intellectual property,

⁴³ Feng, Y. (2020). *Cybersecurity Law and Platform Liability in China: A Rights-Restrictive Model*. Tsinghua Law Journal, 12(3), 101–119.

⁴⁴ Angelopoulos, C. (2013). *Notice-and-fair-balance: A new standard for intermediary liability in the EU*. Journal of Intellectual Property, Information Technology and E-Commerce Law, 4(3), 199–216.

promoting innovation, and preserving fundamental user rights such as freedom of expression and access to information. As internet intermediaries grow in influence, so does the pressure on them to play a more proactive role in content regulation. However, assigning excessive liability can have unintended consequences, creating new risks for the open and democratic nature of the internet.

A core concern in increasing intermediary responsibility is the risk of over-enforcement. When platforms are held strictly liable for infringing content, they often adopt aggressive moderation tactics to avoid legal liability. This leads to overblocking, where even legitimate content is removed out of caution. As algorithms or poorly trained moderators make decisions on complex legal issues, there is a significant risk of censorship and the curtailment of free expression. For example, parody, criticism, or fair use may be mistakenly flagged and taken down, particularly in copyright disputes.⁴⁵ Furthermore, stringent obligations—such as real-time filtering or 24-hour takedown windows—can impose disproportionate burdens on small platforms and startups that lack the financial and technical capacity to implement such systems.⁴⁶ This not only stifles innovation but also creates barriers to entry, reinforcing the dominance of large tech firms.

To mitigate these risks, some jurisdictions and industry actors have explored alternative regulatory models. One such approach is the Graduated Response System, often dubbed the “three-strikes” law, adopted in countries like France under the HADOPI regime. This model targets repeat infringers directly, with escalating consequences ranging from warnings to fines or internet suspension, rather than overburdening intermediaries. While controversial, this method shifts focus from platforms to users, balancing enforcement with procedural fairness.⁴⁷ Another softer alternative is the adoption of voluntary codes of conduct. The EU’s Memorandum of Understanding on the Sale of Counterfeit Goods on the Internet (2011) is a prime example.

Under this initiative, rights holders and online platforms agree to work collaboratively in curbing IP violations through better cooperation, proactive monitoring, and shared reporting

⁴⁵ Keller, D. (2011). *Intermediary Liability 2.0*. Harvard Journal of Law & Technology, 28(1), 1–35.

⁴⁶ DeNardis, L., & Hackl, A. M. (2015). *Internet Governance by Social Media Platforms*. Telecommunications Policy, 39(9), 761–770.

⁴⁷ Angelopoulos, C. (2013). *Notice-and-fair-balance: A new standard for intermediary liability in the EU*. JIPITEC, 4(3), 199–216.

mechanisms, without the need for harsh legal sanctions. Such frameworks allow flexibility and innovation while still supporting IP enforcement goals.

Ultimately, achieving the right equilibrium demands a multi-stakeholder approach, considering the nuances of different platforms, types of IP infringement, and the local legal-cultural context. A one-size-fits-all model is neither effective nor fair. What is needed is a graduated and context-specific liability regime, paired with transparency, independent oversight, and robust grievance mechanisms for both rights holders and users. Only then can we ensure an equitable digital space that encourages creativity while safeguarding legal rights.

Conclusion

The evolution of intermediary liability law represents one of the most critical battlegrounds in the effort to balance the interests of innovation, intellectual property protection, and digital rights. At the heart of this debate lies the tension between safe harbour protections, which shield intermediaries from liability for user-generated content, and the growing demand for greater responsibility in curbing online IP infringement. The paper has explored how the safe harbour framework—originally designed to encourage innovation and protect free expression—has increasingly come under scrutiny for enabling bad actors to exploit these immunities. The limitations of traditional models such as notice-and-takedown systems have become evident in light of rampant piracy, counterfeiting, and the rise of large-scale digital intermediaries who often possess the technological and operational capacity to act, yet remain legally distant from the consequences of infringement. This has prompted significant global shifts, from the European Union’s Digital Services Act to India’s evolving jurisprudence, each seeking to refine the balance between intermediary autonomy and accountability.

Looking ahead, the future of intermediary liability lies not in abolishing safe harbour provisions, but in reimagining them within a calibrated, rights-conscious framework. A tiered liability model—one that considers the intermediary’s size, role, and actual influence over content—can provide a fairer structure while avoiding the pitfalls of both over-regulation and unchecked immunity. Integrating mechanisms such as transparency reporting, user redress systems, and ethical AI moderation can help build trust and promote responsibility without compromising innovation or free speech. Ultimately, the digital age demands a shared responsibility model, wherein intermediaries act with due diligence, rights holders engage constructively, and users are empowered to participate in a healthy, rights-respecting digital

environment. As we confront an increasingly complex digital landscape, the question remains: Can we design a liability regime that both protects creative rights and preserves the open, democratic spirit of the internet?