Page 1014 - 1023 **DOI:** *https://doij.org/10.10000/IJLMH.1112144*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

Intermediary or Accomplice: Balancing intermediary liability and cybercrime mitigation in India

ANWESHA MISHRA*

ABSTRACT

The advent of internet has led to an expansion in the ambit of 'crimes' and 'offenders'. The perpetrators are now become capable of unethical conduct via non-physical mediums i.e. the internet space. Although a necessity, the cyber space has also become a breeding ground for online offenders and like-minded persons. Internet intermediaries like the Internet Service Providers (ISPs), network operators, social networking sites, etc. serve as a medium for the growing cyber offences. This paper explores the fine line between an intermediary acting as a neutral conduit and an accomplice in criminal activity. It revolves around the analysis of cyber-crimes, the liabilities of intermediaries and the provisions for safe harbour for such intermediaries under the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules . As platforms have evolved from passive hosts to algorithmic curators, the traditional "safe harbour" protection available to them has been under close scrutiny of the Judiciary. The landmark Avnish Baja and Shreya Singhal cases are just a couple of the many examples where the Courts have undertaken to illustrate the role and liability of these platforms. The real issue is: do we hold these platforms responsible for what their users do, or would it discourage the intermediaries thereby end up killing creativity and silencing their right to speak freely? This paper further examines the technical and ethical challenges of cyber-crime mitigation. Ultimately, the research argues for a balanced regulatory approach. We can't expect the internet intermediaries to be mere bystanders nor can we expect them to always keep a check over the endless cyber space.

I. INTRODUCTION

Between 2017 and 2019, several incidents of mob lynching were reported across India, triggered by rumours circulated on WhatsApp about child kidnappers operating in local areas[1]. These messages, often accompanied by disturbing videos or fabricated claims, were forwarded rapidly

* Author is a Guest Faculty of Law at Madhusudan Law University, Cuttack, Odisha, India.

[1] Balla Satish, *How whatsapp helped turn an Indian village into a lynch mob,* BBC News (2018), https://www.bbc.com/news/world-asia-india-44856910 (last visited May 21, 2026).

 [ISSN 2581-5369]

across groups, creating panic and outrage. In multiple cases, innocent individuals were attacked or killed based on these false rumours. The issue that arose here was- whether WhatsApp acted merely as a platform or should it be made liable along with the offenders in order to secure the platform from further misuse?

The confusion lies in this grey area:

- If WhatsApp is treated purely as a passive intermediary, harmful misuse goes unchecked.
- If it is treated as an active publisher, it becomes technically and ethically difficult to monitor private communications

Human communication has shifted to the cyber space, interacting with one another via online platforms. From financial transactions to shopping, everything is now on-line and so are the cyber offenders. Numerous cyber offences have been recognised by various Indian legislations like the IT Act, 2000[2], BNS, 2023[3], etc. The said enactments also hold liable the internet intermediaries for the commission of such offences but the grey area still remains unresolved as to what is the extent of liability that can be prescribed upon such intermediaries so as to not discourage or unfairly penalize them.

The intermediaries are passages through which large amount of data gets transferred from one device to another every second. The intermediaries are inclusive of various categories of mediums like Internet Service Providers (ISPs), search engines, social media platforms, e-commerce marketplaces and payment gateways. ISPs facilitate connectivity, enabling users to access the internet. Social media platforms host user-generated content and enable communication at an unprecedented scale. E-commerce platforms provide marketplaces where buyers and sellers interact, often without ever meeting physically. Each of these intermediaries functions as a digital gatekeeper managing access to information and shaping the contours of online engagement. In the age of AI, especially, the line has started dissolving as to when their activity is solely that of a third-party and when it merges with the cybercrime. Defining, in a practical sense, the ambit under the doctrine of safe harbour[4] could heavily impact foreign investments as well. In times like such, it becomes difficult to harmonize accountability and uplifting of innovation.

[2] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India)
[3] The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India)
[4] Information Technology Act, 2000, Sec 79, No. 21, Acts of Parliament, 2000 (India)

 [ISSN 2581-5369]

This paper entails the study of the liability presently pressed upon intermediaries, understanding the cloak of "safe harbour" and its exceptions, the various judicial pronouncements portraying the Intermediaries as conduits and as accomplice, and addressing of the yet undercover issues regarding intermediary liability.

II. ROLE OF INTERMEDIARIES IN INDIA

Sec 2(1)(w) of the IT Act, 2000 defines the term "intermediary" as "intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes"[5]. The following could be treated as intermediaries in accordance with the above definition:

- Internet access and service providers (ISPs);
- Data processing and web hosting providers, including domain name registration;
- Internet search engines and portals;
- E-commerce intermediaries, where the platforms do not themselves take title to the goods;
- Internet payment systems; and
- Participative networking platforms, like publishing and broadcasting platforms. [6]

Intermediary Liability

Digital intermediaries can find themselves legally liable across a broad spectrum of issues, from civil wrongs and crimes to trademark and copyright infringements. Legislations around the globe handle the challenge of policing third-party content through two distinct strategies: the horizontal approach and the non-horizontal approach. The horizontal approach relies on a single, uniform legal framework to govern all intermediary liability. In contrast, the non-horizontal approach, adopted in countries like India, addresses different legal violations separately through their own specific statutes and penalties.[7]

[5] Information Technology Act, 2000, Sec 2(1)(w), No. 21, Acts of Parliament, 2000 (India)
[6] Ms. Karine Perset, *The Economic and Social Role of Internet Intermediaries*, OECD(2010)
[7] eGyanKosh, https://egyankosh.ac.in/bitstream/123456789/96306/3/Unit-6.pdf (last visited 21st May, 2026)

 [ISSN 2581-5369]

Modern internet and telecommunications technologies enable the widespread dissemination of illicit content and facilitates several other cyber offences while veiling the offenders behind the screen. Thereby, it is important to understand the liability that attaches to such intermediaries that aid in harbouring these cyber offenders. Liability is linked to many different kinds of content, and the issues it raises may be different depending on the type of content. A few examples are discussed as under-

- Hosting defamatory and libelous content- In the landmark case of Cubby Inc v CompuServe (1991)[8], the US District Court distinguished the role of intermediaries as 'publishers' and 'distributors'. The court distinguished that a 'publisher' is one who edits content and is liable; and a 'distributor' is one who merely hosts/transmits content without reviewing it. It was held that CompuServe acted as a mere distributor and thereby not guilty of libel.

- Trademark infringements- The landmark judgment of Christian Louboutin SAS v. Nakul Bajaj & Ors. (2018)[9] by the hon'ble Delhi High Court established that e-commerce platforms are not passive intermediaries if they engage in activities like curation, storage, or facilitating the sale of counterfeit products. Such platforms lose their immunity and are liable for trademark infringement if they do not exercise due diligence.

- Misrepresentation- The intermediary stands guilty in cases of misrepresentation through the cyberspace hosted by him, especially in cases where such malfeasance should have been known to him or when he gains any profit out of it. Protection is lost if the intermediary actively participates, induces, or conspires in the illegal act, or fails to take down content upon receiving actual knowledge of its unlawful nature.

- Violating content-blocking orders: The platforms are obligated to block public access to a certain kind of content if the same is ordered by the Central Government under Sec 69A of the IT Act, 2000[10].

- Copyright infringing material- The Hon'ble Court in M/s Shri Krishna International v. Google India Pvt. Ltd.[11] judgment has held that the defendants had infringed the plaintiffs' copyright by making available the plaintiffs' films and other audiovisual

[8] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).
[9] Christian Louboutin SAS v. Nakul Bajaj & Ors., AIRONLINE 2018 DEL 1962
[10] Information Technology Act, 2000, Sec 69A, No. 21, Acts of Parliament, 2000 (India)
[11] M/s Shree Krishna International v. Google India Pvt. Ltd. & Ors., Dist. Ct. Gurugram, Judgment dated Sept. 27, 2019 (India)

 [ISSN 2581-5369]

works on their website. The Court further observed that, despite having full knowledge of the titles of the infringing content, the defendants failed to remove such content. The Court ruled that the defendants could not claim immunity under the safe harbour doctrine, since they had engaged in modification of the video content through the insertion of advertisements and had failed to take down the content even after they had notice of the same.

- Dissemination of Illegal and harmful content- The cyber space has enables easy distribution of materials which can be labelled as pornographic, racist, or terrorist. The intermediaries. Their responsibility has shifted from passive hosting to active content moderation, largely driven by "notice-and-take-down" legal frameworks that require swift removal of pornographic, racist, or terrorist material upon receiving actual knowledge of its unlawfulness.
- Failure to comply with data retention provisions- Rule 3(1)(d) of the IT Rules, 2021[12] requires digital intermediaries and platforms to give government agencies the access to information. This rule applies to any official agency tracking down cyber threats, protecting the public, or running a legal investigation.

III. SCOPE OF SEC 79 OF THE IT ACT, 2000

The protection of "safe harbour" under Sec 79 of the IT Act is only conditional to the intermediary function that falls under the ambit of "third-party activity". The conditions for application of Sec 79 of the Act are as under :

- The intermediary functions merely as a technical facilitator and limits its role to the transmission, hosting, or temporary storage of data that is wholly generated by third parties.
- The intermediary does not originate or initiate the transmission.
- The intermediary does not determine or choose the recipient of the transmission.
- The intermediary neither selects nor alters the information contained in the transmission.
- The intermediary exercises due diligence and complies with the guidelines prescribed by the Central Government or any authority authorised by it. [13]

[12] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India)

[13] Information Technology Act, 2000, Sec 79(2), No. 21, Acts of Parliament, 2000 (India)

 [ISSN 2581-5369]

An intermediary loses its legal immunity if it helps, conspires, or is induced—through threats or rewards—to commit an illegal act. The protection of "safe harbour" is also revoked if the platform gains actual knowledge of the unlawful material but fails to take it down quickly, or if it tampers with any digital evidence in the process. In cyber security matters, the malicious intent of the intermediary does not mandatorily need to be proved. Intermediaries cannot simply claim they were unaware of the harmful content. To claim exemption from the liability, they must prove that they did not start the transmission, choose the recipients, modify the data, or in any way aid or abet the commission of the offence. The sententia legis behind such exemption is to encourage the free flow of online information, recognizing that over-regulating platforms would cripple technological innovation and digital communication.

IV. THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021[14]

The Intermediaries Guidelines Rules lay down the requirements that intermediaries must follow to be eligible for the safe harbour protection available under Section 79 of the Information Technology Act, 2000. Rule 3[15] describes the procedures to be followed by intermediaries to claim that they'd maintained "due diligence". Intermediaries must:

- Publish their user agreement, privacy policy, terms of service, and community guidelines prominently on their website and app, ensuring users consent to these terms.
- Not host, store, or publish information that violates Indian laws, including content that threatens India's sovereignty, integrity, security, or public order, or is defamatory, obscene, or infringing on intellectual property rights.
- Within 36 hours of receiving a Court order or Government notice, the host shall remove or disable access to the unlawful contents.
- Retain records of such actions for 180 days.
- Appoint a Grievance Officer and Nodal Contact Person for Significant Social Media Intermediaries (SSMIs like Instagram or Facebook), publish their details, and resolve complaints within specified timelines.
- Not host content that impersonates another person or deceives users about its source.

[14] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India)
[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3, G.S.R. 139(E) (India)

 [ISSN 2581-5369]

V. INTERMEDIARY: AS MERE CONDUIT VS AN ACCOMPLICE AND IT'S GREY AREAS

Indian intermediary liability law has evolved through an ongoing effort to balance free expression and innovation with the need to protect people from online harm and hold digital platforms accountable. Courts no longer treat intermediaries as either fully immune or automatically responsible for all user activity. Instead, they assess liability based on how much control, knowledge, participation, and compliance an intermediary demonstrates in a given situation.

The shift in interpretation became visible in Avnish Bajaj v. State (NCT of Delhi)[16], widely known as the Bazee.com case. After a user uploaded and sold an obscene MMS clip through the platform, authorities prosecuted the CEO on the basis that the platform had effectively published the content. Although Bazee.com removed the listing and cooperated with investigators, the case pushed courts to recognise that intermediaries cannot pre-screen all user activity in the same way traditional publishers operate. The outcome influenced later amendments to Section 79 and strengthened safe harbour and notice-and-takedown mechanisms.

Courts reinforced this approach in MySpace v. Super Cassettes[17]. The court held that hosting user-generated content alone does not amount to copyright infringement when the platform acts passively and responds appropriately after receiving notice. Rather than encouraging blanket censorship, the decision supported reactive moderation over prior restraint.

The Supreme Court expanded these protections in Shreya Singhal v. Union of India (2015)[18]. Section 66A[19] of the IT Act was struck down as being violative of Art 19(1)(a). The Court also clarified that intermediaries lose safe harbour only if they ignore valid court orders or lawful government directions requiring removal of unlawful content. Informal complaints alone do not create liability. This interpretation narrowed the meaning of "actual knowledge" and reduced pressure on platforms to become private censors.

Together, these decisions shaped the "mere conduit" doctrine. Intermediaries retain protection when they remain neutral, comply with due diligence obligations, and act on legally valid takedown requests.

[16] Avnish Bajaj v. State (NCT of Delhi) (2005)
[17] Super Cassettes Industries Ltd. v. MySpace Inc. is cited as 2016 SCC OnLine Del 6356.
[18] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1
[19] Information Technology Act, 2000, Sec 66A, No. 21, Acts of Parliament, 2000 (India)

 [ISSN 2581-5369]

Safe harbour, however, has clear limits. Courts withdraw protection once intermediaries move beyond passive facilitation and begin participating in, promoting, endorsing, or negligently ignoring unlawful conduct.

This principle appeared in Google India Pvt. Ltd. v. M/s Visaka Industries (2019)[20], where defamatory material remained online despite notice. The court observed that a platform capable of removing unlawful content but choosing not to intervene may attract publisher-like liability. The decision confirmed that safe harbour depends on responsible action.

The Delhi High Court developed this principle further in Christian Louboutin SAS v. Nakul Bajaj & Ors. (2018)[21]. Darveys.com actively marketed products and created the impression of authenticity while benefiting commercially from listings. The platform's intrinsic involvement in the selection and display of supposedly authentic materials led to it being devoid of the safeguard under Sec 79.

These cases show that intermediaries may become accomplices and attract a strict liability when they promote unlawful content, profit from user activity, create an appearance of endorsement, ignore lawful takedown obligations, or exercise editorial and algorithmic influence over visibility.

Despite legal progress and the IT Rules, 2021, several unresolved issues continue to create opportunities for cyber offenders.

One major issue involves traceability and end-to-end encryption[22]. Rule 4(2)[23] of the IT Rules talks about retaining originator traceability. It requires the SSMIs to identify the first originator of information under lawful orders. Platforms argue that traceability weakens encryption and threatens privacy. Courts and policymakers continue to debate whether such requirements conflict with constitutional privacy protections under Article 21. This uncertainty may enable anonymous misinformation, cybercrime, and illegal content distribution.

Another emerging issue concerns AI-driven curation and algorithmic liability. Current law does not clearly determine whether recommendation systems transform intermediaries into active participants. Modern platforms recommend content, personalise feeds, amplify posts, and generate summaries. Because the legal position remains unclear, malicious actors may

[20] Google India Pvt. Ltd. v. M/s Visaka Industries, 2019 SCC OnLine SC 1587
[21] Christian Louboutin SAS v. Nakul Bajaj & Ors., AIRONLINE 2018 DEL 1962
[22] Gumati, M. R, *Digital Sovereignty or Regulatory Overreach? The Case of Indonesia's Platform Registration Policy*, Competition and Regulation in Network Industries, 25(4), 131–146 (2024).
[23] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule No. 4(2), G.S.R. 139(E) (India)

 [ISSN 2581-5369]

manipulate recommendation systems to spread disinformation, scams, synthetic media, and coordinated influence campaigns.

Dark web intermediaries also present major challenges. Hidden services often support cybercrime ecosystems through anonymous infrastructure, illicit marketplaces, and criminal networks. Existing rules focus primarily on visible commercial platforms and offer limited guidance on assigning liability to hidden infrastructure operators.

A further concern involves the absence of tiered liability standards. Indian law still groups many intermediaries together despite major differences in their roles and influence. Internet service providers generally act as passive access providers, while hosting providers and search engines perform technical storage and indexing functions. Social media platforms influence visibility through algorithms, e-commerce platforms combine commercial and intermediary roles, and payment gateways may facilitate transactions. Without differentiated standards, enforcement remains inconsistent and vulnerable to misuse.

VI. CONCLUSION AND SUGGESTIONS

In conclusion, intermediary liability must be governed through a balanced framework that protects cyberspace without undermining innovation, privacy, and freedom of expression. Under Section 79 of the Information Technology Act, 2000 and the Intermediary Guidelines, safe harbour protection remains conditional and depends on the intermediary's role, degree of control over content, and compliance with due diligence obligations. Judicial developments show that immunity cannot extend to platforms that actively facilitate or tolerate unlawful conduct. At the same time, emerging challenges such as AI-generated content, encrypted communication, dark web activities, and cross-border cybercrime have exposed gaps in the current legal framework.

To address the above discussed concerns, Indian legislations should adopt a proportionate and risk-based approach to intermediary liability. This includes introducing a tiered liability where the passive intermediaries could be protected under Sec79 and active platforms could be exempted. The classification would be based on platform involvement, clarifying the meaning of "active participation" in AI-driven systems. Thereby strengthening content reporting mechanisms, and ensuring traceability only through lawful and proportionate processes. Greater transparency, algorithmic accountability, differentiated compliance obligations, and a co-regulatory model involving the State, intermediaries, and independent oversight bodies can further improve accountability without encouraging overregulation. Ultimately, an effective intermediary liability regime must strike a balance between responsibility and innovation. At

 [ISSN 2581-5369]

the same time, it must ensure the protection of freedom of speech and expression[24] within the evolving digital ecosystem.

*****

[24] Indian Const. Art 19(1)(a)

 [ISSN 2581-5369]