

Live Streaming Liability and Real-Time Harm: Legal Accountability of Platforms Under the Information Technology Act, 2000

Introduction

Digital live-streaming platforms (e.g. YouTube Live, Twitch, Facebook Live) pose novel challenges for India's intermediary liability law. The Information Technology Act, 2000 ("IT Act") and subordinate rules provide *conditional* immunity ("safe harbour") to intermediaries, subject to stringent due diligence and takedown obligations. However, these provisions were designed for asynchronously uploaded content and struggle to address the instantaneous nature of live-streamed harms (e.g. sudden incitement of violence, live sexual abuse, or real-time harassment). In *Shreya Singhal v. Union of India*, the Supreme Court struck down the broad Section 66A and interpreted Section 79 narrowly, requiring formal government or court notice before platforms lose immunity.¹² This rule-driven, notice-and-takedown model is inherently ill-suited to live-streaming, where harmful content can spread and vanish before any official order is issued. This article examines the existing legal framework, notably Section 79 and the 2021 Intermediary Guidelines, analyses why it fails to effectively curb real-time harms. It also explores judicial interpretations and international analogues, and suggests reform directions (e.g. a duty-of-care approach or specific live-streaming obligations) to fill the accountability gap.

Legal Framework under the IT Act and 2021 Rules

Section 79:- Conditional Safe Harbour

Section 79(1) of the IT Act provides that intermediaries (online platforms) "shall not be liable for any third-party information, data, or communication link made available or hosted" on their

¹ Information Technology Act, 2000, No. 21 of 2000, §§ 66A (struck down), 67, 67A, 67B, 67C, 69A, 79 (India).

² The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), dated Feb. 25, 2021 (India).

systems.³ This immunity is conditional on: (a) the intermediary's *passive role* (it must not initiate, select receivers, or modify the transmission)⁴; (b) observing "due diligence" and any government-prescribed guidelines⁵⁶; and (c) no actual knowledge of unlawful content coupled with timely removal upon notice.⁷ Subsection 79(3) clarifies that safe harbor does *not* apply if the intermediary "has conspired, abetted, aided or induced" the illegal act, or if upon receiving *actual knowledge* (via government or court notice) of unlawful content, it fails to "expeditiously remove" it.⁸ In practice, this means platforms enjoy broad immunity unless they actively participate in content or ignore official takedown orders.

Scholars emphasize that Section 79's conditions mirror global safe-harbor models, but with a uniquely Indian twist: compliance with government rules is a prerequisite to immunity. As Kakkar, Mohan and Devadasan explain, "Section 79 of the IT Act offers intermediaries conditional legal immunity (or 'safe harbor') for unlawful UGC on their networks. One condition for safe harbor ... is compliance with the Intermediary Guidelines".⁹¹⁰ In short, Section 79 shields platforms that act as passive conduits and follow the law; it strips immunity if the platform "aids, abets or induces" wrongdoing or has actual knowledge of illegal content and does nothing.¹¹

Due Diligence Requirements (IT Rules 2021)

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules 2021") set out extensive due-diligence obligations for all intermediaries. These include (inter alia): prohibiting specified categories of illegal or harmful content in user agreements; a 36-hour takedown window (72 hours in some cases) upon receiving a lawful order;

³ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁴ *MySpace Inc. v. Super Cassettes Indus. Ltd.* (Delhi HC, Dec. 23, 2016).

⁵ J. M. Kakkar, S. Mohan & V. Devadasan, *Safe Harbor and Content Moderation Regulation in India*, in B. Chakravorti (ed.), *Defeating Disinformation* (Cambridge Univ. Press 2024) (App. 5.1, pp. 145–68).

⁶ Government of India, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India (2021).

⁷ Advay Vora, *Challenge to IT Rules 2023: Supreme Court stays union government's notification establishing a fact check unit*, Supreme Court Observer (Mar. 21, 2024).

⁸ Advay Vora, *Challenge to IT Rules 2023: Supreme Court stays union government's notification establishing a fact check unit*, Supreme Court Observer (Mar. 21, 2024).

⁹ *Measures on the Administration of Internet Live-Streaming Services*, Art. 8, 11 (Promulgated by Cyberspace Admin., Nov. 4, 2016) (China), translated version, ChinaLawTranslate.

¹⁰ Jhalak Mrignayani Kakkar, Shashank Mohan & Vasudev Devadasan, *Safe Harbor and Content Moderation Regulation in India*, in Cambridge University Press eBooks 60 (2025).

¹¹ Advay Vora, *Challenge to IT Rules 2023: Supreme Court stays union government's notification establishing a fact check unit*, Supreme Court Observer (Mar. 21, 2024).

maintenance of a grievance redressal mechanism with an officer; and a requirement to cooperate with law enforcement.¹²¹³¹⁴ Significant Social Media Intermediaries (SSMIs, e.g. Facebook, Twitter) – defined as platforms with over 5 million Indian users – face *heightened* duties, such as appointing a Chief Compliance Officer (CCO), Resident Grievance Officer, and nodal law-enforcement contact (all in India)¹⁵¹⁶. SSMIs must also publish monthly compliance reports (including proactive takedowns) and enable identification of the “first originator” of information for law enforcement.¹⁷¹⁸

If a platform fails any of these rules, it loses safe-harbour protection. Indeed, the Rules explicitly state that non-compliance with the Guidelines renders Section 79 immunity inapplicable. For example, Rule 4(1)(a) makes the CCO “liable in any proceedings ... where he fails to ensure that [the] intermediary observes due diligence”.¹⁹²⁰ In short, the 2021 Rules condition safe harbour on elaborate proactive measures and reporting. Kakkar *et al.* note that Indian law thus ties immunity to stringent *pre*-conditions, turning obligations like compliance reporting and content-classification into prerequisites for protection.²¹²²

The Real-Time Harm Challenge

Live Streaming’s Unique Risks

Live streaming differs fundamentally from pre-recorded content. When someone streams violent, obscene, or harassing content in real time, harm to viewers or targets occurs *simultaneously* with

¹² Communications Decency Act, 47 U.S.C. § 230 (1998).

¹³ Regulation (EU) 2022/2065, *Digital Services Act* (May 19, 2022), O.J. (L 277) 1 (EU).

¹⁴ Government of India, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India (2021).

¹⁵ Online Safety Act 2023 (UK), c. 40.

¹⁶ Government of India, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India (2021).

¹⁷ Communications Decency Act, 47 U.S.C. § 230 (1998).

¹⁸ Government of India, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India (2021).

¹⁹ Online Safety Act 2023 (UK), c. 40.

²⁰ Government of India, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India (2021).

²¹ *Measures on the Administration of Internet Live-Streaming Services*, Art. 8, 11 (Promulgated by Cyberspace Admin., Nov. 4, 2016) (China), translated version, ChinaLawTranslate.

²² Jhalak Mrignayani Kakkar, Shashank Mohan & Vasudev Devadasan, Safe Harbor and Content Moderation Regulation in India, in Cambridge University Press eBooks 60 (2025).

dissemination. Categories of real-time harms include live broadcasting of violence or self-harm, incitement of riots, real-time dissemination of defamation or doxxing, or real-time sexual exploitation (including child abuse) witnessed live by others. Because the content is not pre-moderated or stored prior to viewing, traditional moderation is too late to prevent harm.

India's intermediary regime is oriented around *post*-event actions. The notice-and-takedown model assumes unlawful content remains accessible until a platform is notified by a court or government. Yet under *Shreya Singhal*, "actual knowledge" of illegal content requires an official order, not mere user complaints.²³ Live-streamed content may be over before any such order is issued; there is no time for a court injunction while a live video plays. Moreover, live streams may not be archived, so evidence for a post-hoc takedown or prosecution can vanish. The result is a legal "knowledge paradox": an intermediary that *proactively monitors* and removes live content as it appears risks establishing "actual knowledge" of other concurrent illegal streams, potentially exposing itself to liability. Meanwhile, a passive platform with no monitoring remains in safe harbour. Commentators warn this perverse incentive structure deters platforms from conducting real-time moderation, since "providers who intervene may inadvertently forfeit immunity."²⁴²⁵

Algorithmic Promotion and Passive Hosting

Adding to the complexity, modern platforms often algorithmically curate which live streams to feature. If a platform's recommendation engine amplifies a harmful live stream (e.g. by making it trending), the line between passive host and active publisher blurs. Under Section 79(2)(b), immunity requires that the intermediary *not* select or modify content.²⁶ But algorithmic promotion could be viewed as "selection." Indian courts have hinted that algorithmic amplification may undermine safe harbor protection. While the law has not fully defined this yet, globally regulators are eyeing such issues (e.g. the EU DSA imposes transparency requirements on recommendation algorithms). For now, platforms that curate or monetize live streams risk being treated less like neutral conduits and more like content providers, potentially triggering full liability.

²³ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), dated Feb. 25, 2021 (India).

²⁴ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), dated Feb. 25, 2021 (India).

²⁵ Advay Vora, *Challenge to IT Rules 2023: Supreme Court stays union government's notification establishing a fact check unit*, Supreme Court Observer (Mar. 21, 2024).

²⁶ *MySpace Inc. v. Super Cassettes Indus. Ltd.* (Delhi HC, Dec. 23, 2016).

Judicial and Enforcement Developments

Shreya Singhal (2015)

This landmark Supreme Court decision both expanded free speech and narrowed intermediary liability. It struck down Section 66A (penalizing “offensive” messages) as an overbroad chill on expression,²⁷ and interpreted Section 79 to require “actual knowledge” via court or government order before an intermediary can be compelled to remove content.²⁸ For live streaming, *Singhal* essentially guarantees that platforms *cannot* be made liable for content absent formal notice. In practice, this means harmful live content remains online until some authority intercedes – an outcome that works poorly for instantaneous harms. The Court explicitly protected platforms from user-driven censorship, holding that platforms lose immunity only when *officially notified* of illegality.²⁹

MySpace v. Super Cassettes (Delhi HC 2016)

In this copyright infringement case, the Delhi High Court held that merely having the capability to monitor content does not strip safe harbor. MySpace (social network) was held to retain immunity under Section 79 because it only removed copyrighted music after receiving specific takedown notices. The Court emphasized that platforms need not proactively police all content; liability requires actual knowledge of specific infringing material. By analogy, this suggests that live-streaming sites using AI or staff to scan broadcasts would not automatically lose immunity simply by doing so. However, the Court also warned that intermediaries “cannot bury their heads in the sand” if given notice. For live streaming, MySpace implies platforms must act quickly once notified (albeit retroactively).

Ongoing Challenges

The 2021 Rules themselves have been subject to litigation. In early 2024 a constitution bench of the Supreme Court stayed a rule requiring platforms to remove content flagged “fake or false” by a government fact-check unit (Rule 3(1)(b)(v)). The court found the rule raised serious free-speech

²⁷ Information Technology Act, 2000, No. 21 of 2000, §§ 66A (struck down), 67, 67A, 67B, 67C, 69A, 79 (India).

²⁸ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), dated Feb. 25, 2021 (India).

²⁹ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), dated Feb. 25, 2021 (India).

concerns, noting no social media companies had challenged it “presumably because they feared losing safe-harbour protections”. This episode underscores the chill-factor: fear of losing immunity can drive compliance even with legally questionable orders. Additionally, the Delhi and Kerala High Courts have struck down parts of the Rules for procedural infirmities (e.g. requiring traceability orders without safeguard), and the constitutionality of CCO liability has been questioned, but those issues (though noteworthy) extend beyond live-streaming per se.

Global and Comparative Context

India’s approach lies between the U.S. “immunity-first” model and the EU’s risk-based duty model. In the U.S., Section 230 of the Communications Decency Act (47 U.S.C. §230) grants nearly blanket immunity to platforms for any third-party content, live or not. Platforms there can rarely be held liable for user content unless they co-create it. The Indian model is more conditional: platforms only get safe harbor if they meet due diligence (akin to a European style). The EU’s Digital Services Act (Reg. 2022/2065) goes even further – it imposes affirmative obligations on Very Large Online Platforms (VLOPs) to assess and mitigate systemic risks, including mandatory real-time monitoring of live streams for terrorist or child abuse content. Under the DSA, VLOPs must deploy detection tools for identified risks, much like the Chinese regulatory ethos. The UK’s Online Safety Act 2023 likewise introduces broad duties for platforms (though it is not yet fully in force). By contrast, India’s law, even after 2021, lacks any explicit real-time prevention duty. Platforms are only required to “act upon” content after notice, not to pre-screen or interrupt streams proactively.

International Live-Streaming Rules

Notably, China’s regulations explicitly mandate real-time control. The “Measures on Internet Live-Streaming” (2016) require platforms to have staff and tech to review content, segment streams by user scale, and crucially to possess “technical capacity to instantaneously cut off internet livestreams”. Chinese live-streaming providers must also supervise chat (“barrage”) in real time. This model treats live-streaming platforms as active conduits with joint responsibility – a sharp contrast to the Indian passive-conduit approach. While India has not adopted such strict real-time rules, these examples highlight how other regimes impose immediate takedown obligations that India’s notice-based system lacks.

Gaps and Reform Directions

The key deficiency in Indian law is the lack of any *real-time takedown duty*. The 36-hour removal period is meaningless if content disappears in minutes. Intermediaries have no statutory obligation to interrupt an ongoing live broadcast of obvious illegality (violence, harassment, etc.). This gap may be partly addressed by emergent tech (AI moderation) but not by current law. Indeed, deploying AI scanning may increase liability paradoxically, so platforms may hesitate to self-police.

Other gaps include definitional ambiguities. User-generated live streams do not clearly fall under the “online curated content” category of the Rules. The “online curated content” framework presumes editorial control and age-rating – features absent from unfiltered live chats. Thus, general OTT rules (age bands, parental controls) technically apply only to professionally curated content, leaving grassroots live streaming in a regulatory no-man’s land.

The law also lacks a broad “duty of care” concept (unlike the EU DSA or the forthcoming Digital India Act proposals). India still relies on secondary (post-hoc) liability rules. Critics argue a more proactive framework is needed, where platforms must assess and mitigate foreseeable risks – especially for large-scale, live events. Legislative proposals (like the withdrawn Broadcasting Services Bill or the draft Digital India Act) hint at future requirements for pre-listing of banned content and regulated licensing of live services.

Finally, the personal liability of CCOs (under Rule 4(1)(a)) is a problematic feature. Holding an individual officer criminally liable for failure to prevent a live-streamed crime (which they might not even know about until after the fact) raises constitutional issues of fair notice and realistic accountability. Some commentators suggest this provision should be repealed or narrowed, to avoid chilling effects on innovation and management.

Conclusion

India’s intermediary liability regime – Section 79 of the IT Act and the 2021 Guidelines – has evolved in response to digital challenges, but it remains ill-tailored to the instantaneous nature of live-streamed harm. Safe harbor is strictly conditional and has been progressively narrowed, placing heavy compliance burdens on platforms. Yet by design these burdens are still oriented

toward offline or post-publication content. The *notice-trigger* model established in *Shreya Singhal* means platforms are rarely deemed culpable for user content absent official notice, which in turn makes *prevention* of real-time harm legally unrewarded. In practice, this creates perverse incentives that may leave dangerous live broadcasts largely unchecked. The clearest exception is child safety: CSAM streaming breaches both Sections 67B and mandatory 24-hour takedown rules, exposing platforms to direct liability.

Going forward, reformers advocate clearer categories of harmful live content and specific statutory duties to interrupt egregious streams in progress. India’s draft Digital India Act (if enacted) and renewed Broadcasting legislation may fill some gaps, potentially adopting a limited duty-of-care or licensing approach for live content. In parallel, platform design choices – such as AI moderation, human review teams, and safer recommendation algorithms – will determine practical accountability. As things stand, the law permits a wide margin of platform inaction during live events. Any effective strategy must realign legal obligations with technological realities: bridging the “time gap” between a livestream’s appearance and official intervention. Until then, victims of real-time online harms will face an uphill battle for redress under India’s current framework.

References:

1. Information Technology Act, 2000, No. 21 of 2000, §§ 66A (struck down), 67, 67A, 67B, 67C, 69A, 79 (India).
2. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), dated Feb. 25, 2021 (India).
3. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
4. *MySpace Inc. v. Super Cassettes Indus. Ltd.* (Delhi HC, Dec. 23, 2016).
5. J. M. Kakkar, S. Mohan & V. Devadasan, *Safe Harbor and Content Moderation Regulation in India*, in B. Chakravorti (ed.), *Defeating Disinformation* (Cambridge Univ. Press 2024) (App. 5.1, pp. 145–68).
6. Advay Vora, *Challenge to IT Rules 2023: Supreme Court stays union government’s notification establishing a fact check unit*, Supreme Court Observer (Mar. 21, 2024).

7. *Measures on the Administration of Internet Live-Streaming Services*, Art. 8, 11 (Promulgated by Cyberspace Admin., Nov. 4, 2016) (China), translated version, ChinaLawTranslate.
8. Communications Decency Act, 47 U.S.C. § 230 (1998).
9. Regulation (EU) 2022/2065, *Digital Services Act* (May 19, 2022), O.J. (L 277) 1 (EU).
10. Online Safety Act 2023 (UK), c. 40.