Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 420-433 | ISSN:1505-4683

Laws and Regulations on OTT Platforms in the age of Artificial Intelligence: A Comparative Study of India's IT Rules with US and Australia

Narmada Singh Rana[1], Dr. Priya A Sondhi[2], Dr. Shreya[3]
[1]Research Scholar, School of Law, Sushant University, Gurugram, Haryana- 122003, India
[2]Professor and Dean, School of Law, Sushant University, Gurugram, Haryana- 122003, India
[3]Assistant Professor, School of Law, Sushant University, Gurugram, Haryana- 122003, India

ABSTRACT

The rapid integration of artificial intelligence (AI) into Over-The-Top (OTT) platforms has severely transformed how digital content is delivered, curated, and moderated. Recommendation algorithms, automated content classification, deepfake detection systems, and the AI driven age-gating mechanisms increasingly shape the interaction between platforms and users at an unprecedented scale. The regulatory frameworks governing these platforms across major jurisdictions, including India, the United States and Australia, remain fragmented, reactive, and largely unequipped to address the diverse challenges posed by AI powered content ecosystems. The author will undertake a comparative legal analysis of the regulatory approaches adopted by India, the United States, and Australia in governing AI powered OTT platforms. In India, the analysis examines the Information Technology Act, 2000, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, including the three-tier grievance redressal mechanism and self-regulatory framework, as well as the implications of the Digital Personal Data Protection Act, 2023 for algorithmic profiling. For the United States, the paper evaluates Section 230 of the Communications Decency Act, First Amendment constraints on algorithmic content curation, FTC enforcement actions on algorithmic transparency, and emerging state-level content moderation legislation. Australia's framework is assessed through the Online Safety Act 2021, the powers of the e-Safety Commissioner, Basic Online Safety Expectations (BOSE), age verification mandates, and proposed AI governance initiatives. The comparative analysis is focused and structured around key dimensions i.e. self-regulation versus co-regulation versus state regulation models, intermediary liability and safe harbour provisions, content takedown mechanisms and due process standards, algorithmic transparency and explainability requirements and data protection regimes governing user profiling. The paper further examines AI-specific regulatory concerns, identifies key regulatory gaps across all the three jurisdictions and proposes a set of recommendations for a harmonised governance framework.

Keywords: *OTT Platforms, Artificial Intelligence, Information Technology, IT Rules 2021, Algorithmic Regulation, Content Moderation, Digital content.*

1. Introduction

1.1 Background and Context

The production, distribution, and consumption of audio-visual material have been completely transformed by the widespread use of Over-The-Top (OTT) platforms. Now serving billions of users globally, well-known platforms like Netflix, Amazon Prime, Disney+, and several other regional counterparts use advanced artificial intelligence technologies to improve user engagement, automate moderation, and customise content discovery. OTT platforms work as technology intermediates, content producers, and data processors in an uncertain regulatory landscape, in contrast to traditional broadcasting, which operates within well-established legal paradigms. Artificial intelligence pipelines shape the digital material that these OTT platforms deliver end-to-end, and the amount and velocity of this content have become the main focus of algorithmic regulation in many significant jurisdictions.

A new level of complexity has been added by the incorporation of AI into these platforms. To optimise interaction metrics, recommendation

engines frequently highlight information that is sensational or divisive. Every day, millions of judgements regarding whether content stays available are made by automated content moderation algorithms, often without human oversight. While AI-driven age-gating mechanisms aim to limit minors' access to inappropriate information, deepfake detection technologies try to counteract synthetic media. Each of these roles brings up important issues regarding accountability, culpability, freedom of speech, and the suitability of current legal systems.

1.2 Research Objectives

The study seeks to achieve the following objectives:

1. To study and compare the legal frameworks regulating AI-powered OTT platforms in India, United States and Australia.
2. For examination of AI based Technologies used by OTT platforms, which includes recommendation algorithms, automated content moderation, deepfake detection, and age verification mechanisms.
3. To analyse the effectiveness of existing laws in addressing issues relating to platform accountability, intermediary liability, online safety, child protection and freedom of expression in AI driven digital environments.
4. To identify the regulatory gaps and emerging legal challenges in the governance of AI-powered OTT platforms and suggest suitable policy recommendations for a balanced regulatory framework.

1.3 Aim of the Study

The study aims to evaluate how well current frameworks handle AI specific issues, pinpoint the advantages, disadvantages, and gaps in each jurisdiction's strategy, and make suggestions for a more standardised governance model.

1.4 Research Questions

1. How do India, United States and Australia regulate AI powered OTT platforms within their respective legal systems?
2. To what extent do existing legal frameworks address AI related concerns such as algorithmic recommendation systems, automated moderation, deepfake content and child safety?
3. How effective are the present intermediary liability and platform accountability frameworks in balancing freedom of expression, user rights and online safety?
4. What are the major legal and regulatory gaps in the governance of AI powered OTT platforms and what reforms are necessary to address emerging technological challenges?

1.4 Research Methodology

The study adopts a doctrinal and comparative legal methodology. The doctrinal approach is used to examine and interpret court rulings, subordinate legislation, primary legislation, principle legislative instruments and regulatory guidance in each of three jurisdictions. The analysis is up to date as of social media taking into account the latest modifications to India's IT Rules (including the 2025 and 2026 amendments),[1] advancements in US Section 230 jurisprudence, such as the Take It Down Act[2], and Australia's adoption of the Social Media Minimum Age framework[3] and Phase 2 e-Safety industry codes. The comparative method is employed to analyse and compare the regulatory approached adopted in India, United States and Australia.

2. Artificial Intelligence on OTT Platforms: Technological Landscape

2.1 Recommendation Algorithms and Content Personalisation

At the core of every major OTT platform, lies a recommendation engine, an AI system that analyses user behaviour, preferences, viewing history, and demographic data to curate personalised content feeds. These algorithms employ collaborative filtering, content-based filtering, and increasingly, deep learning models to predict user preferences with remarkable accuracy.[4] While this personalisation enhances user experience, it also creates filter bubbles, amplifies engagement-

[1] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), effective Feb. 20, 2026 (India) [hereinafter IT Amendment Rules 2026].

[2] Take It Down Act, Pub. L. No. 119-12, 139 Stat. 251 (2025).

[3] Online Safety Amendment (social media Minimum Age) Act 2024 (Cth) (Austl.), effective Dec. 10, 2025.

[4] Carlos A. Gomez-Uribe & Neil Hunt, The Netflix Recommender System: Algorithms, Business Value, and Innovation, 6 ACM Transactions on Management Information Systems 1, 4–7 (2015).

maximising content regardless of its societal impact, and raises fundamental questions about algorithmic accountability.[5] The scale of this Artificial Intelligence deployment is illustrated in Figure 1 below, which captures the parallel rise of the global OTT Platforms subscriber base and the share of platforms integrating AI driven recommendation and Content Moderation pipelines.

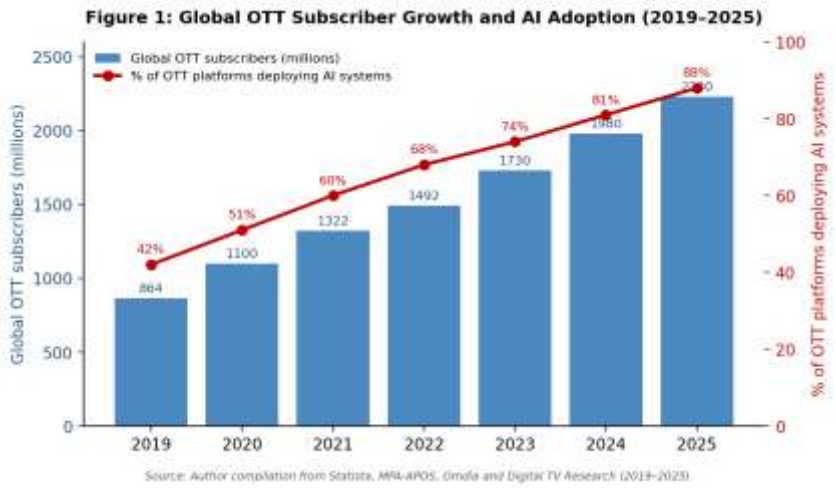

Figure 1: Global OTT Platforms subscriber base and the share deploying Artificial Intelligence systems (2019–2025). Source: Author compilation from Statista, MPA-APOS, Omdia and Digital TV Research.

The opacity of these systems described as 'black boxes'[6] means that neither users nor regulators can fully understand why specific content is promoted or suppressed. This lack of transparency has significant implications for regulatory frameworks that were designed for an era of human editorial decision making.

2.2 Automated Content Moderation and Classification

OTT platforms deploy AI powered content moderation systems to classify content by age appropriateness, detect policy violations, and flag potentially illegal material. These systems process vast volumes of content at speeds impossible for human moderators. However, automated moderation carries inherent risks: false positives result in the suppression of lawful speech, while false negatives allow harmful content to remain accessible. Cultural and linguistic biases embedded in training data further compound these challenges, particularly for platforms operating across diverse markets like India.

2.3 Deepfake Detection and Artificial Intelligence Generated Synthetic Media

The emergence of generative AI has enabled the creation of increasingly convincing synthetic media like deepfake videos, cloned voices, and fabricated imagery.[7] OTT platforms face dual challenges when preventing the distribution of harmful synthetic content while also deploying AI based detection tools to identify such material. The regulatory response to synthetic media varies significantly across jurisdictions, from India's recently introduced Synthetically Generated Information (SGI) framework[8] to the absence of comprehensive federal legislation in the United States.

[5]Eytan Bakshy, Solomon Messing & Lada A. Adamic, Exposure to Ideologically Diverse News and Opinion on Facebook, 348 Science 1130 (2015) (documenting algorithmic curation's role in shaping cross-cutting content exposure).

[6]See Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (2015).

[7]Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Cal. L. Rev. 1753, 1758–65 (2019).

[8]IT Amendment Rules 2026, supra note 7, r. 2(1)(wa) (defining synthetically generated information as "audio, visual or audio-visual information which is artificially or algorithmically

2.4 AI-Driven Age-Gating and Child Safety Mechanisms

Protecting minors from inappropriate content is a shared regulatory concern across all three jurisdictions. AI systems are increasingly deployed for age verification, parental controls, and content filtering tailored to younger audiences. Australia's world leading social media minimum age requirement of sixteen years, effective December 2025, exemplifies the most aggressive regulatory approach.[9] India's IT Rules mandate self-classification and access restrictions, while the US relies primarily on COPPA[10] and platform self-governance, supplemented by the recently enacted Take It Down Act targeting non-consensual intimate imagery including AI generated content.

3. India's Regulatory Framework

3.1 Information Technology Act, 2000

Evolution and Scope: India's regulation of OTT platforms is rooted in the Information Technology Act, 2000,[11] India's foundational cyber legislation. Originally it was enacted to provide legal recognition for electronic commerce and address cybercrime, the IT Act has been progressively expanded through amendments and subordinate legislation to address the challenges of social media, digital content, and now artificial intelligence. Section 79 of the IT Act establishes the safe harbour framework for intermediaries, exempting them from liability for third-party content provided they observe prescribed due diligence requirements.[12]

3.2 Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 (IT Rules)

The IT Rules 2021, represent the most comprehensive regulatory intervention targeting OTT platforms in India. Part III of the Rules, establishes a Code of Ethics for OTT platforms and digital news media, requiring platforms to self-classify content into age-based categories such as U, U/A 7+, U/A 13+, U/A 16+, and A. It also implements access control mechanisms for restricted content, and display content descriptors.

The Rules have been amended multiple times and most recently in February 2026. In substance, the IT Rules 2021 are India's primary instrument of Algorithmic Regulation for Digital content on OTT Platforms, and they expressly contemplate Artificial Intelligence-driven curation, recommendation and age-gating systems as objects of compliance and oversight.

The 2025 amendment introduced procedural safeguards for content takedowns, mandating senior level authorisation and reasoned intimation specifying the legal basis and exact content identifier.[13] The 2026 amendment represents a paradigm shift, introducing the concept of Synthetically Generated Information into the regulatory lexicon, now subject to mandatory labelling requirements, metadata embedding for traceability, and a drastically reduced takedown timeline of three hours for illegal content and two hours for non-consensual intimate deepfake imagery.[14]

3.3 Three-Tier Grievance Redressal and Self-Regulatory Framework

The IT Rules establish a three-tier grievance redressal mechanism for OTT platforms:[15]

1. Level I requires platforms to appoint a Grievance Officer to address user complaints within fifteen days
2. Level II involves self-regulatory bodies established by content publishers, headed by a retired judge or eminent person; and
3. Level III provides for government oversight through an inter-departmental committee.

---

created/generated/modified/altered using a computer resource").

[9]Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth) (Austl.).

[10]Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.

[11]Information Technology Act, 2000, No. 21, Acts of Parliament (India).

[12]Information Technology Act, 2000, § 79, No. 21, Acts of Parliament (India).

[13]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025, effective Nov. 15, 2025 (India).

[14]IT Amendment Rules 2026, supra note 7, r. 3(1)(d) (mandating removal within three hours for content deemed illegal by court or appropriate government, and two hours for non-consensual intimate deepfake imagery).

[15]IT Rules 2021, supra note 4, rr. 11–14 (establishing the three-tier grievance redressal mechanism).

However, the implementation of this mechanism has been stalled by judicial challenges. The Bombay High Court and Madras High Court have stayed certain provisions, the Kerala High Court has barred coercive action for non-compliance, and approximately fifteen petitions challenging the Rules have been consolidated before the Delhi High Court.[16]

3.4 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection (DPDP) Act, 2023[17] introduces significant implications for AI-driven OTT platforms. The Act regulates the processing of personal data by data fiduciaries, establishes consent-based processing requirements, and provides special protections for children's data.[18] For OTT platforms that rely extensively on algorithmic profiling to personalise content recommendations, the DPDP Act's provisions on purpose limitation, data minimisation, and the obligation to obtain verifiable parental consent for processing children's data represent substantive compliance obligations that intersect directly with AI-powered operations.

3.5 Censorship, Self-Regulation, and Judicial Interventions

A persistent tension in India's OTT regulatory landscape is the debate between censorship and self-regulation. Unlike films, which are subject to certification by the Central Board of Film Certification (CBFC), OTT content operates under a self-classification model. The government has repeatedly expressed dissatisfaction with the efficacy of self-regulation, with the Ministry of Information and Broadcasting banning over thirty OTT applications between July 2025 and February 2026 for distributing obscene content.[19]

Both the Supreme Court and the Delhi High Court have observed that OTT regulation is necessary, and the government has considered expanding the definition of 'obscene digital content' to include material deemed defamatory, containing half-truths, or exhibiting anti-national attitudes, proposals that have raised significant free speech concerns.[20]

4. United States Regulatory Framework

4.1 Section 230 of the Communications Decency Act

Section 230 of the Communications Decency Act, 1996 is the cornerstone of US platform regulation.[21] Its core provision has been credited with enabling the growth of the modern internet. Section 230 simultaneously protects platforms from liability for hosting third-party content and immunises good-faith content moderation decisions.[22] However, Section 230 was enacted in an era that did not contemplate artificial intelligence, algorithmic content curation, or generative AI.[23] As the law marks its thirtieth anniversary, scholars and policymakers are intensely debating whether its protections should extend to AI-generated content and algorithmic amplification.[24] Legislative

[16]See Justice for Rights Found. v. Union of India, W.P. No. 12497/2021 (Bombay H.C.); Digital News Publishers Ass'n v. Union of India (Madras H.C.); see also Internet Freedom Found. v. Union of India (transferred to Delhi H.C.).

[17]Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament (India) [hereinafter DPDP Act].

[18]DPDP Act, supra note 23, § 9 (requiring verifiable parental consent for processing children's data).

[19]Government Blocks OTT Platforms for Streaming Obscene Content, THE HINDU (July 25, 2025), https://www.thehindu.com/news/national/government-blocks-ott-platforms-for-streaming-obscene-content/article70672926.ece.

[20]See Centre Plans Tighter IT Rules to Curb 'Obscene' and Harmful Online Content, Bus. Standard (Nov. 24, 2025). https://www.business-standard.com/industry/news/centre-it-rules-amendments-obscene-digital-content-ott-news-regulation-125112400358_1.html

[21]47 U.S.C. § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

[22]Zeran v. America Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997) (establishing broad Section 230 immunity for distributor liability); see also Reno v. ACLU, 521 U.S. 844, 870 (1997).

[23]See Kadous Sarah, Section 230 and AI-Driven Platforms, The Regulatory Rev. (Jan. 17, 2026) (discussing the thirtieth anniversary of Section 230 and AI challenges).

https://www.theregreview.org/2026/01/17/seminar-section-230-and-ai-driven-platforms/

[24]Graham Ryan, Generative AI and the Future of Section 230, 38 Harv. J.L. & Tech. (2025).

proposals including a House bill to sunset Section 230 by December 31, 2025[25] and the 'No Section 230 Immunity for AI Act'[26] reflect bipartisan frustration with the law's perceived overreach. Courts have yet to definitively rule on whether AI-generated content is covered by Section 230, though legal experts increasingly suggest that platforms whose AI systems actively shape content, rather than passively hosting it, face diminished immunity.[27]

4.2 First Amendment and Algorithmic Content Curation

A distinctive feature of the US regulatory landscape is the First Amendment's application to algorithmic content curation. Federal courts have generally treated platform moderation decisions as protected editorial discretion, analogous to a newspaper's choice of which articles to publish. The Supreme Court's consideration of cases such as Anderson v. TikTok[28] that raises questions about platform liability for harms linked to algorithmic amplification of third-party content, might reshape this understanding. In Moody v. Net Choice and Net Choice v. Paxton (2024), the Supreme Court vacated both lower court decisions and remanded the challenges to Florida's and Texas's social media content-moderation laws, holding that the appellate courts had failed to conduct the analysis required for a facial First Amendment challenge. The Court signalled, however, that a platform's curation of third-party content is generally protected expressive activity, while leaving open the question of whether algorithmic amplification constitutes editorial judgment or something categorically different.[29]

4.3 FTC Enforcement and the Take It Down Act

The Federal Trade Commission has emerged as a key regulator of platform conduct, particularly regarding algorithmic transparency, data practices, and child safety.[30] The Take It Down Act, signed into law by President Trump, represents a significant departure from Section 230's protective framework by imposing liability on platforms that fail to remove non-consensual intimate imagery, including AI-generated content, within 48 hours of a valid takedown request by a victim, with the FTC empowered to enforce compliance against non-compliant platforms.[31] This Act represents the first federal legislation to create platform accountability specifically for AI-generated harmful content.

4.4 State-Level Content Moderation Laws and COPPA

In the absence of comprehensive federal legislation, states have pursued their own regulatory approaches. California and Texas have enacted content moderation laws, though these have faced constitutional challenges. The Children's Online Privacy Protection Act (COPPA) remains the primary federal instrument for child safety online, requiring parental consent for the collection of personal information from children under thirteen. However, COPPA was enacted in 1998 and does not adequately address the sophisticated AI-driven engagement mechanisms that OTT platforms now deploy to capture and retain young users' attention. Scholars have likewise observed that COPPA's notice-and-consent architecture does not constrain recommendation driven engagement, and that meaningful child safety online will require obligations targeted at algorithmic design rather than mere data collection.[32]

5. Australia's Regulatory Framework

[25]See Tech Regulation Digest: Sunsetting Section 230, Milken Inst. (2025) (discussing House bill to sunset Section 230 by 2026).

[26]No Section 230 Immunity for AI Act, S. 1993, 118th Cong. (2024).

[27]See Section 230 in the Era of Generative AI, Am. Action F. (2025) ("Courts haven't addressed this yet, with no rulings to date on whether AI-generated content is covered by Section 230.").

[28]See Anderson v. TikTok, Inc. (pending before the U.S. Supreme Court, raising questions about platform liability for algorithmic amplification).

[29]See Net Choice, LLC v. Paxton, 49 F.4th 439 (5th Cir. 2022); Moody v. Net Choice, LLC, 603 U.S. (2024).

[30]See, e.g., In re Epic Games, Inc., FTC File No. 202-3203 (2022) (enforcement action regarding deceptive practices in data collection).

[31]See The Future of Online Expression and Innovation Depends on Robust Section 230 Protections, Cato Inst. Pol'y Analysis No. 1013 (Feb. 26, 2026).

[32]Max Del Real, Comment, Recommendation Algorithms and Section 230 Immunity, 101 Wash. L. Rev. __ (2025).

5.1 Online Safety Act 2021 and the e-Safety Commissioner

Australia has adopted arguably the most interventionist approach among the three jurisdictions. The Online Safety Act 2021 empowers the e-Safety Commissioner, Australia's independent online safety regulator, to investigate complaints, order content removal, and enforce compliance across all online services available in Australia, regardless of where they are hosted.[33] The e-Safety Commissioner possesses powers to issue removal notices for cyberbullying material, adult cyber abuse, image-based abuse, and illegal or restricted content, backed by substantial civil penalties for non-compliance. This represents a co-regulatory model that combines industry self-governance through registered codes with robust state oversight.

5.2 Industry Codes, BOSE, and Age Verification

The e-Safety Commissioner has registered industry codes in two phases targeting different categories of harmful content.[34] Phase 1 Unlawful Material Codes, effective from late 2025, target the generation, storage, and sharing of illegal content including child sexual exploitation material and pro-terrorism content. Phase 2 Age-Restricted Material Codes, with the final six codes effective from March 2026, protect children from lawful but harmful content including pornography and self-harm material across social media platforms, messaging services, app distribution platforms, and designated internet services. The Basic Online Safety Expectations (BOSE) determination sets baseline safety expectations for all online services, requiring platforms to take reasonable steps to keep Australians safe.[35] In an Australian first, the eSafety Commissioner issued legal notices in October 2025 to four AI companion chatbot companies, requiring them to demonstrate compliance with BOSE and report their child safety measures, signalling regulatory willingness to extend online safety frameworks to AI-native services.[36]

5.3 Social Media Minimum Age and Classification Framework

Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024, effective from December 2025, introduced a mandatory minimum age of sixteen for accounts on age-restricted social media platforms.[37] This world-leading legislation places the compliance burden on platforms rather than users or parents, and applies to major services including Facebook, Instagram, TikTok, Snapchat, Reddit, and YouTube. The legislation interacts with Australia's broader classification framework under the Classification (Publications, Films and Computer Games) Act,[38] which defines content categories that the Online Safety Act uses to regulate streaming services. This represents a uniquely Australian approach that integrates traditional content classification principles with modern platform regulation.

6. Comparative Analysis

6.1 Regulatory Models: Self-Regulation vs. Co-Regulation vs. State Regulation

The three jurisdictions represent distinct points on the regulatory spectrum. India adopts a hybrid model that nominally emphasises self-regulation through its three-tier mechanism but increasingly trends toward direct state intervention, as evidenced by the rapid takedown timelines introduced in the 2026 amendments and the government's outright banning of non-compliant OTT applications.

The United States maintains the most permissive approach, with Section 230 providing broad immunity and limited affirmative regulatory obligations, though this framework is under unprecedented pressure from both legislative proposals and judicial evolution. Australia occupies

[33]Online Safety Act 2021 (Cth), pts. 6–9 (Austl.) (establishing the e-Safety Commissioner's investigation and enforcement powers).

[34]E-Safety Commissioner (Austl.), Online Safety Codes and Standards (Phase 1 Unlawful Material Codes registered June 27, 2025; Phase 2 Age-Restricted Material Codes registered Sept. 9, 2025, effective Mar. 9, 2026).

[35]Basic Online Safety Expectations Determination 2022 (Cth) (Austl.).

[36]Minter Ellison, e-Safety Commissioner Issues Notice to AI Chatbot Providers (Oct. 23, 2025), https://www.minterellison.com/articles/esafety-targets-4-ai-chatbot-firms.

[37]See Online Safety (Age-Restricted Social Media Platforms) Rules 2025 (Cth) (Austl.) (designating Facebook, Instagram, TikTok, Snapchat, Reddit, and YouTube as age-restricted platforms).

[38]Classification (Publications, Films and Computer Games) Act 1995 (Cth) (Austl.).

the co-regulatory middle ground, with industry-developed codes that carry legal force once registered by the e-Safety Commissioner, supplemented by direct enforcement powers. Figure 2 distils these divergent postures into a comparative scorecard across seven regulatory dimensions, making visible the asymmetric maturity of Algorithmic Regulation, statutory AI rules and Content Moderation regimes in India, the United States and Australia.

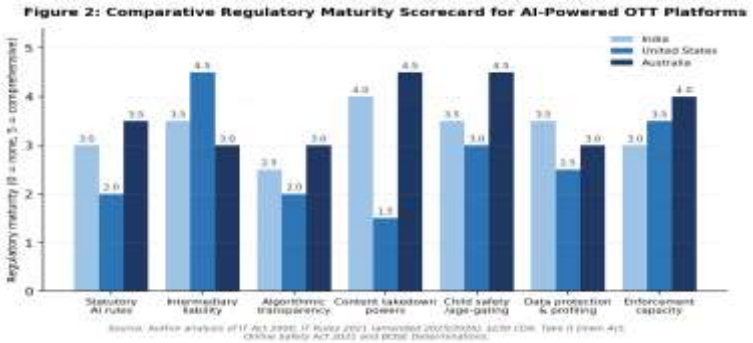

Figure 2: Comparative regulatory maturity scorecard for AI-Powered OTT Platforms across India, the United States and Australia. Source: Author analysis of the Information Technology Act 2000, IT Rules 2021 (as amended in 2025 and 2026), Section 230 CDA, the Take It Down Act, the Online Safety Act 2021 and BOSE Determinations.

6.2 Intermediary Liability and Safe Harbour

Safe harbour provisions differ materially across jurisdictions. India's Section 79 conditions safe harbour on compliance with due diligence obligations under the IT Rules, creating a framework where failure to comply with government-mandated takedown requirements, now within a three-hour window, strips platforms of immunity.[39] The US Section 230 provides the broadest immunity, though its application to AI-generated content and algorithmic amplification remains unsettled. Australia's approach focuses less on blanket immunity and more on affirmative duties, requiring platforms to proactively design safe systems rather than merely respond to complaints.

6.3 Algorithmic Transparency and Data Protection

Algorithmic transparency requirements vary dramatically. India's 2026 amendments mandate labelling of synthetically generated information and metadata embedding for traceability, representing the most prescriptive requirements among the three jurisdictions. The DPDP Act further constrains algorithmic profiling through consent and purpose limitation requirements. The United States lacks any federal algorithmic transparency mandate, though the FTC has taken enforcement action against deceptive algorithmic practices and individual states are developing their own requirements. Australia's BOSE framework requires platforms to take reasonable steps to ensure algorithmic systems do not expose users to harmful content, though specific transparency mandates remain limited.[40]On data protection, the three jurisdictions present a striking asymmetry. India's DPDP Act 2023 and Australia's Privacy Act 1988[41] provide statutory frameworks for data protection, while the United States lacks a comprehensive federal privacy law: a gap that is particularly significant given the data-intensive nature of AI-powered OTT platforms. The regulatory fragmentation created by state-level privacy laws in the US, led by California's Consumer Privacy Act,[42] creates compliance complexity but inconsistent protections.

6.4 Extra-Territorial Jurisdiction and Cross-Border Challenges

[39]Information Technology Act, 2000, § 79(3)(b), No. 21, Acts of Parliament (India) (removing safe harbour protection if an intermediary fails to act after receiving actual knowledge of unlawful content).

[40]Regulation (EU) 2022/2065, on a Single Market for Digital Services (Digital Services Act), arts. 27, 38 & 40, 2022 O.J. (L 277) 1 (imposing algorithmic transparency and data access obligations on very large online platforms).

[41]Privacy Act 1988 (Cth) (Austl.) (currently under reform pursuant to the Attorney-General's Department review).

[42]California Consumer Privacy Act, Cal. Civ. Code 1798.100–1798.199.100 (West 2020).

All three jurisdictions grapple with the challenge of regulating global platforms that transcend national boundaries. India's IT Rules apply to all intermediaries operating in India regardless of where they are incorporated. Australia's Online Safety Act explicitly applies to services available in Australia, regardless of hosting location. The US approach is more nuanced, with Section 230 creating a domestic framework that has limited extra territorial reach but significant indirect influence through the dominance of US headquartered platforms. The absence of harmonised international standards means that platforms face conflicting obligations across jurisdictions, creating opportunities for regulatory arbitrage.

7. AI-Specific Regulatory Issues

7.1 Algorithmic Bias and Legal Accountability

Recommendation algorithms on OTT platforms can perpetuate and amplify biases present in their training data, leading to discriminatory content promotion that disadvantages certain linguistic, cultural, or demographic groups.[43] In India's linguistically diverse market, where OTT platforms serve content in over twenty languages, the risk of algorithmic bias in content recommendation is particularly acute. None of the three jurisdictions has enacted specific legislation addressing algorithmic bias in content recommendation, though general anti-discrimination principles and evolving AI ethics frameworks provide a foundation for future regulatory development. Closing this gap will require dedicated Algorithmic Regulation: rules that require auditability of Artificial Intelligence-driven ranking systems and impose accountability for biased Digital content surfacing on OTT Platforms, going beyond the procedural compliance currently demanded by the IT Rules 2021.

7.2 AI-Generated Content and Platform Liability

The rapid advancement of generative AI has created an urgent regulatory challenge: determining liability for AI-generated harmful content distributed through OTT platforms. India's 2026 amendments address this most directly through the SGI framework, requiring mandatory labelling, user self-declaration, and platform verification of AI generated content.[44] The US Take It Down Act creates narrow liability for AI generated non-consensual intimate imagery. Australia's e-Safety Commissioner has demonstrated willingness to apply existing online safety frameworks to AI services, as evidenced by the legal notices issued to AI companion chatbot providers.[45] However, no jurisdiction has established a comprehensive liability framework for AI generated content on OTT platforms that addresses the full spectrum of potential harms. Scholars have argued for a nuanced, flexible application of existing immunity doctrines to generative AI models, rather than blanket extension or removal of protections.[46]

7.3 Automated Content Moderation: Accuracy, Censorship, and Due Process

The reliance on AI for content moderation creates a tension between efficiency and accuracy, and between safety and free expression. Automated systems lack the contextual understanding necessary to evaluate nuanced content, frequently producing false positives that suppress legitimate speech or false negatives that allow harmful content to persist. India's rapid takedown requirements: three hours for illegal content, two hours for intimate deepfakes,[47] effectively mandate reliance on automated systems, as human review at such speeds is impractical at scale. This raises significant due process concerns, as content may be removed based on algorithmic judgment without meaningful human oversight or adequate appeal mechanisms.

7.4 AI and Children: Personalised Content Risks

[43]See Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism (2018) (discussing how algorithmic systems perpetuate existing social biases).

[44]IT Amendment Rules 2026, supra note 7, r. 3(1)(b)(v) (requiring mandatory labelling and user self-declaration for synthetically generated content).

[45]E-Safety Commissioner, Transparency Reports issued under Basic Online Safety Expectations to Generative AI Providers (Austl. 2024) (notices to providers of AI companion services).

[46]Veronica Arias, A Nuanced Application of Section 230 to Generative AI Models, Penn J. Phil. (2025).

[47]Ministry of Elec. & Info. Tech. (India), Frequently Asked Questions on IT Amendment Rules, 2026 (2026), https://www.meity.gov.in/static/uploads/2025/10/065b6deb585441b5ccdf8be42502a49c.pdf.

The protection of children from AI driven harms on OTT platforms is perhaps the area of greatest regulatory convergence. All three jurisdictions recognise that AI powered personalisation poses unique risks to minors, including exposure to inappropriate content, exploitation of psychological vulnerabilities, and the collection and profiling of children's data. Australia's minimum age requirement represents the most aggressive intervention, while India's self-classification and access control requirements and the US COPPA framework provide less robust protections. The emerging consensus is that platform design choices, not merely content moderation, must be regulated to ensure child safety in AI powered environments.

8. Gaps and Emerging Challenges

Despite significant regulatory activity across all three jurisdictions, critical gaps persist. First, no jurisdiction has enacted AI specific legislation that comprehensively addresses the unique challenges posed by AI powered OTT platforms. Existing frameworks were designed for human-curated content environments and are being retrofitted, with varying degrees of success to address algorithmic decision-making. The absence of a purpose-built Algorithmic Regulation regime is felt most acutely in the governance of Digital content on OTT Platforms, where Artificial Intelligence now mediates discovery, classification and moderation at a scale that the IT Rules 2021, Section 230 and the Online Safety Act 2021 did not originally anticipate.

Second, regulatory arbitrage remains a significant concern. Platforms operating across jurisdictions can exploit differences in regulatory stringency, particularly given the absence of harmonised international standards. The tension between India's increasingly prescriptive approach, the US's permissive framework, and Australia's co-regulatory model creates incentives for forum shopping and compliance minimisation.[48]

Third, the balance between platform accountability and user agency remains unresolved. Overly prescriptive regulations risk creating state driven censorship: as critics have argued regarding India's proposed expansion of 'obscene content' definitions, while insufficient regulation allows platforms to externalise the costs of AI driven harms onto users and society.

Fourth, the rapid pace of AI development consistently outstrips regulatory capacity.[49] By the time jurisdictions develop and implement regulatory responses to specific AI capabilities, the technology has typically evolved beyond the scope of those regulations. The EU AI Act[50] represents one attempt at comprehensive, technology-neutral AI regulation, but its application to OTT specific challenges remains to be tested.

9. Recommendations

The paper proposes the following recommendations for a harmonised governance framework for AI powered OTT platforms. First, jurisdictions should adopt technology neutral regulatory principles that focus on outcomes and harms rather than specific technologies. The OECD AI Principles emphasising transparency, accountability, robustness, and human oversight, provide a suitable foundation that can accommodate evolving AI capabilities without requiring constant legislative amendment.[51]

Second, mandatory algorithmic impact assessments should be required for AI systems that materially influence content discovery and user engagement on OTT platforms. These assessments, analogous to environmental impact assessments in other regulatory domains, would require platforms to evaluate and disclose the potential impacts of their recommendation algorithms on user welfare,

[48]Christopher T. Marsden & Ian Brown, Regulating Code: Good Governance and Better Regulation in the Information Age 35–42 (MIT Press 2013) (analysing cross-jurisdictional regulatory arbitrage in platform regulation).

[49]Gary E. Marchant, The Growing Gap Between Emerging Technologies and the Law, in The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight 19, 23–28 (Gary E. Marchant et al. eds., Springer 2011) (articulating the "pacing problem").

[50]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689).

[51]OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (adopted May 22, 2019, as amended May 3, 2024).

diversity of content exposure, and vulnerable populations. Operationally, such assessments should be embedded as an obligation under the IT Rules 2021 in India and treated as a core pillar of Algorithmic Regulation, so that the Artificial Intelligence systems shaping Digital content on OTT Platforms are subjected to ex ante, evidence-led scrutiny rather than only ex post takedown.

Third, harmonised international standards for AI generated content labelling and provenance tracking should be developed through multilateral cooperation. India's SGI labelling framework and the EU AI Act's transparency requirements offer models that could be adapted for international application, potentially through the OECD, UNESCO,[52] or the G20 Digital Working Group.[53]

Fourth, regulatory frameworks should mandate independent algorithmic audits by qualified third parties, ensuring that platforms' AI systems are periodically assessed for bias, accuracy in content moderation, compliance with legal standards, and effectiveness of child safety measures. Audit results should be reported to relevant regulators and, in summary form, to the public.

Fifth, child safety in AI powered environments should be addressed through a combination of platform design obligations, robust age verification requirements, and restrictions on algorithmic profiling of minors. Australia's approach of placing compliance burdens on platforms rather than users offers a model that balances child protection with practical enforceability.

10. Conclusion

The regulation of AI powered OTT platforms stands at a critical juncture. Instead of the current patchwork of ex post takedown responsibilities, unified regulatory monitoring is now necessary for the delivery, curation, and moderation of digital material on OTT platforms. Although the US, Australia, and India all have different regulatory ideologies and tools to contend with, none of them has created a thorough framework that effectively handles the entire range of hazards unique to AI. India's changing IT regulations show growing regulatory aspirations, but they also raise issues with free speech and implementation. Although historically successful in fostering innovation, the US Section 230 framework is becoming less and less appropriate in the age of algorithmic content moderation and generative artificial intelligence. Although it is still a work in progress, Australia's co-regulatory model, supported by robust enforcement capabilities and proactive child protection measures, presents possibly the most promising pattern.

The US's dedication to free speech principles, Australia's focus on platform design accountability and child safety, and India's specificity on synthetic media regulation are some of the strengths of each jurisdictional model that should be used going forward. The most practical route to governance frameworks that simultaneously safeguard human rights, respond to AI-driven harms, and encourage responsible innovation in the OTT ecosystem is the creation of harmonised international standards based on the OECD AI Principles and influenced by the real-world experiences of these three jurisdictions.

Furthermore, governments and regulatory bodies must enact adaptable, forward-thinking legislation that can address emerging issues in the digital world as AI technology continues to advance quickly. Stronger data security protocols, greater accountability of OTT platforms, and greater openness in algorithmic decision-making will all be crucial to maintaining user safety and public confidence. Regulation should, however, refrain from imposing needless limitations that could impede innovation, creativity, and technical advancement. Therefore, creating a safe, transparent, and responsible AI-driven OTT ecosystem that safeguards both societal interests and individual freedoms in the digital age requires a balanced strategy based on collaboration between governments, tech companies, legal institutions, and international organisations.

REFERENCES

1. Pasquale, Frank. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press. https://www.hup.harvard.edu/books/9780674736061
2. Marsden, Christopher T., & Brown, Ian. (2013). *Regulating Code: Good Governance and Better Regulation in the Information Age*. MIT Press.

[52]UNESCO, Recommendation on the Ethics of Artificial Intelligence, SHS/BIO/PI/2021/1 (adopted Nov. 23, 2021).

[53]See G20 Digital Economy Working Group, G20 AI Principles (2019) (endorsed under Japan's G20 presidency, drawing on the OECD AI Principles).

https://mitpress.mit.edu/9780262525596/principles-and-parameters-in-comparative-grammar/
3. Noble, Safiya Umoja. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York University Press. https://nyupress.org/9781479837243/algorithms-of-oppression/
4. Marchant, Gary E. et al. (2011). *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight*. Springer. https://link.springer.com/book/10.1007/978-94-007-1356-7
5. Gomez-Uribe, Carlos A., & Hunt, Neil. (2015). "The Netflix Recommender System: Algorithms, Business Value, and Innovation." *ACM Transactions on Management Information Systems*, 6(4), 1–19. https://dl.acm.org/doi/10.1145/2843948
6. Bakshy, Eytan, Messing, Solomon, & Adamic, Lada A. (2015). "Exposure to Ideologically Diverse News and Opinion on Facebook." *Science*, 348(6239), 1130–1132. https://www.science.org/doi/10.1126/science.aaa1160
7. Chesney, Robert, & Citron, Danielle Keats. (2019). "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review*, 107(6), 1753–1820. https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security/
8. Ryan, Graham. (2025). "Generative AI and the Future of Section 230." *Harvard Journal of Law & Technology*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5337202
9. Arias, Veronica. (2025). "A Nuanced Application of Section 230 to Generative AI Models." *Penn Journal of Philosophy*. https://repository.upenn.edu/server/api/core/bitstreams/d503357f-c540-4592-9600-0041fe75ec27/content
10. Information Technology Act, 2000 (India). https://www.meity.gov.in/static/uploads/2024/03/IT-Act-Rules_2000_0.pdf
11. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India). https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf
12. Digital Personal Data Protection Act, 2023 (India). https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
13. Communications Decency Act, 47 U.S.C. § 230. https://www.law.cornell.edu/uscode/text/47/230
14. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
15. Online Safety Act 2021 (Cth) (Austl.). https://www.legislation.gov.au/C2021A00076/latest/versions
16. Privacy Act 1988 (Cth) (Austl.). https://www.legislation.gov.au/C2004A03712/latest/versions
17. Reno v American Civil Liberties Union, 521 U.S. 844 (1997). https://supreme.justia.com/cases/federal/us/521/844/
18. Zeran v America Online, Inc., 129 F.3d 327 (4th Cir. 1997). https://law.justia.com/cases/federal/district-courts/FSupp/958/1124/1881560/
19. Moody v NetChoice, LLC, 603 U.S. (2024). https://www.supremecourt.gov/opinions/23pdf/22-277_d18f.pdf
20. NetChoice, LLC v Paxton, 49 F.4th 439 (5th Cir. 2022). https://www.supremecourt.gov/opinions/21pdf/21a720_6536.pdf
21. OECD. (2019). *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
22. UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. https://unesdoc.unesco.org/ark:/48223/pf0000381137
23. G20 Digital Economy Working Group. (2019). *G20 AI Principles*. https://www.caidp.org/resources/g20/
24. E-Safety Commissioner (Australia). (2025). *Online Safety Codes and Standards*. https://www.esafety.gov.au/industry/codes
25. Ministry of Electronics & Information Technology. (2026). *Frequently Asked Questions on IT Amendment Rules, 2026*. Government of India. https://www.meity.gov.in/
26. MinterEllison. (2025). "e-Safety Commissioner Issues Notice to AI Chatbot Providers." https://www.minterellison.com/articles/esafety-targets-4-ai-chatbot-firms
27. "Government Blocks OTT Platforms for Streaming Obscene Content." *The Hindu*. (25 July 2025). https://www.thehindu.com/news/national/government-blocks-ott-platforms-for-streaming-obscene-content/article70672926.ece
28. "Centre Plans Tighter IT Rules to Curb 'Obscene' and Harmful Online Content." *Business Standard*. (24 November 2025). https://www.business-standard.com/industry/news/centre-it-rules-

amendments-obscene-digital-content-ott-news-regulation-125112400358_1.html
29. Kadous, Sarah. (January 17, 2026). "Section 230 and AI-Driven Platforms." *The Regulatory Review*. https://www.theregreview.org/2026/01/17/seminar-section-230-and-ai-driven-platforms/
30. Watson, Allie. "Section 230 in the Era of Generative AI." *American Action Forum*. (2025). https://www.americanactionforum.org/?s=Section+230+in+the+Era+of+Generative+AI
31. "The Future of Online Expression and Innovation Depends on Robust Section 230 Protections." *Cato Institute Policy Analysis No. 1013*. (26 February 2026). https://www.cato.org/policy-analysis/future-online-expression-innovation-depends-robust-section-230-protections