



AI, OTT Platforms and Child Online Safety: A Comparative Study of Regulatory Standards of Various Countries

¹Rahul Deo, ²Dr. Gawaraja Suthar

¹Ph.D. Research Scholar & ²Assistant Professor

^{1/2}Department of Law, Apex University, Jaipur

ABSTRACT

Artificial intelligence increasingly shapes children's experiences of online entertainment through personalised recommendations, advertising, content moderation and interactive features. These functions raise regulatory questions that extend beyond the age classification of individual programs. This article presents a qualitative comparative review of selected regulatory instruments in India, the United Kingdom, the United States and Australia, alongside the European Union's supranational framework. It examines content safeguards, children's personal data, age assurance, algorithmic accountability and platform responsibility. The comparison identifies different regulatory emphases: classification and emerging data safeguards in India; complementary media, platform and AI rules in the European Union; design standards and risk-based safety duties in the United Kingdom; parental consent and data governance under United States federal children's privacy rules; and account restrictions combined with broader safety codes in Australia. The article argues for an integrated approach that addresses both program suitability and the systems through which content reaches children. Its conclusions concern regulatory design rather than measured effectiveness in reducing harm.

Keywords: Artificial intelligence; OTT platforms; child online safety; comparative regulation; age assurance; data protection; recommender systems; parental consent; digital rights; safety by design.

1. INTRODUCTION

Internet-delivered entertainment creates opportunities for children to learn, discover cultural material and access accessible media. However, the same environment can expose them to unsuitable content and intrusive data practices. AI adds another dimension because a child's experience may depend on automated decisions about what to recommend, promote, suppress or generate. UNICEF's Guidance on AI and Children identifies privacy, safety, fairness, transparency and children's participation as central requirements for responsible AI. It also addresses emerging concerns involving AI companions and AI-generated child sexual abuse material.¹

A useful comparison must distinguish the technology used to deliver a service from its legal classification. "Over-the-top" broadly describes delivery over internet infrastructure, but this article uses "curated OTT" principally for on-demand catalogues selected by a provider. Social video platforms, user-upload services and standalone AI chatbots are considered



separately where their features create related risks. A subscription streaming catalogue does not automatically fall within every obligation imposed on a social media platform.²

The article therefore asks three questions: how do selected jurisdictions distribute responsibility for children's safety; how far do their rules address AI-mediated experiences; and which principles could strengthen regulation of curated OTT services without unnecessarily restricting children's access to information?

2. METHODOLOGY AND SCOPE

The study uses doctrinal and comparative policy analysis. Its sources are legislation, official commencement notifications, regulator publications and UNICEF guidance, checked for this article on 6 October 2026. The jurisdictions were selected purposively to illustrate different approaches rather than to represent all countries. The European Union is included as a supranational regulatory framework, not described as an individual country.

The comparison considers five dimensions: content classification and access; personal-data protection; age assurance and parental involvement; AI and recommender-system accountability; and institutional enforcement. Binding legal provisions are distinguished from interpretative guidance and policy recommendations. The discussion of the United States focuses on the federal COPPA framework and does not attempt a comprehensive survey of state legislation. No interviews, platform experiments or outcome measurements were conducted; accordingly, the article does not rank countries by demonstrated safety performance.

3. WHY AI CHANGES THE OTT SAFETY QUESTION

Content classification answers whether a programme is suitable for an age group. Algorithmic governance asks a different question: why was that programme, trailer or advertisement selected for this viewer? A service may correctly classify its catalogue yet still need to examine how recommendations, previews and profile-switching affect children's exposure.

For example, a hypothetical family account might contain a carefully restricted child profile while allowing easy movement into an adult profile. Another service might respect an age filter but continually promote further viewing through autoplay. These examples illustrate why catalogue controls, interface design and recommendation systems should be assessed together; they are not allegations about particular providers.

AI can also support protection through classification assistance and detection of potentially harmful material. Nevertheless, automated decisions require evaluation and routes for correction. Regulatory attention should therefore cover both harmful uses of AI and the reliability of AI deployed as a safety measure. The appropriate safeguards depend on the actual service: risks from open user interaction differ from those of a closed editorial catalogue.

4. INDIA: CONTENT CLASSIFICATION AND EMERGING DATA SAFEGUARDS

India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 distinguish publishers of online curated content from intermediaries. The curated-content framework specifies five classifications: U, U/A 7+, U/A 13+, U/A 16+ and



A. It provides for prominent ratings and content descriptors, access controls including parental locks for U/A 13+ and higher content, and reliable age verification for A-rated material. These provisions directly address the suitability and accessibility of OTT catalogues.²

A separate layer is established by the Digital Personal Data Protection Act, 2023. It defines a child as an individual below eighteen. Section 9 provides for verifiable parental consent, prohibits processing likely to harm a child's well-being, and restricts tracking, behavioural monitoring and targeted advertising directed at children. These provisions are subject to statutory exemption mechanisms; parental consent is not a blanket authorisation for otherwise prohibited processing.³

The timing is essential. The November 2025 commencement notification places section 9 within the group commencing eighteen months after Gazette publication. Thus, at the article's October 2026 cutoff, these substantive child-data duties should be described as enacted but awaiting commencement, rather than fully operational obligations.⁴ The comparative implication is that India's catalogue safeguards and forthcoming data duties address different parts of the same experience. Further operational guidance could explain how child profiles, viewing histories and personalisation should interact, including on shared family accounts.

5. EUROPEAN UNION: COMPLEMENTARY MEDIA, PLATFORM AND AI REGULATION

The Audiovisual Media Services Directive provides a sector-specific foundation. Article 6a requires Member States to ensure that audiovisual services containing material potentially harmful to minors' development are made available in ways that minors will not normally encounter. The Directive also contains distinct provisions for video-sharing platforms. Its relevance to curated OTT therefore arises through audiovisual-service regulation and national implementation.⁵ The Digital Services Act adds obligations for services within its definitions. Article 28 addresses proportionate privacy, safety and security measures on covered online platforms accessible to minors, and restricts profiling-based advertising where the provider knows with reasonable certainty that the recipient is a minor. Article 27 concerns recommender transparency, while very large platforms face additional systemic-risk duties. These provisions cannot simply be applied to every curated catalogue because it operates online.⁶

The Commission's July 2025 guidelines recommend safer recommendation systems, protective defaults, controls on engagement features and safeguards for integrated AI chatbots. They assist assessment of compliance with Article 28(1); following them is voluntary and does not automatically establish legal compliance.⁷ The AI Act contributes a further rule: Article 5(1)(b) prohibits exploitation of age-related vulnerabilities where the specified conditions concerning behavioural distortion and significant harm are met. This is a threshold-based prohibition, not a ban on all personalised recommendations to children.⁸ Taken together, these instruments illustrate how content, distribution and AI conduct can be governed through complementary legal layers.



6. UNITED KINGDOM: DESIGN STANDARDS AND RISK-BASED DUTIES

The UK Information Commissioner's Children's Code sets out fifteen standards for relevant online services likely to be accessed by children. Its themes include children's best interests, impact assessment, high-privacy defaults, data minimisation, profiling and avoidance of nudges that weaken privacy. It is a statutory code explaining the application of data-protection law, rather than a separate general prohibition on children using online services.⁹

Ofcom's Protection of Children Codes address services within the Online Safety Act's user-to-user and search framework. The children's safety duties became applicable from July 2025, with requirements to assess risks and implement protective measures. Providers may follow the Codes or use other effective measures satisfying their legal duties. The framework explicitly considers recommender systems alongside moderation, reporting and age assurance.¹⁰

Curated video-on-demand requires separate attention. Ofcom's ODPS framework addresses editorial programming and restricts children's access to specially restricted material. Consequently, an analysis of a streaming service must determine which legal regime applies rather than assume that all Online Safety Act duties attach to every OTT catalogue.¹¹ The distinctive lesson is the connection between organisational risk assessment and everyday product design. A visible parental-control menu alone cannot establish whether a service has adequately managed the relevant risks.

7. UNITED STATES: FEDERAL PRIVACY PROTECTION AND PARENTAL CONSENT

The Children's Online Privacy Protection Rule applies to covered commercial services directed to children under thirteen and to general-audience services with actual knowledge of relevant collection from children under thirteen. It regulates personal-information practices and provides parental notice, consent and control mechanisms. The under-thirteen threshold identifies COPPA's protection boundary; it is not a universal legal minimum age for internet use.¹²

The FTC's 2025 amendments strengthen restrictions on data monetisation and retention. They require separate verifiable parental consent for covered third-party disclosures, including disclosures supporting targeted advertising, subject to the Rule's exceptions. They also reject indefinite retention and expand the personal-information definition to include biometric identifiers.¹³

For covered streaming and video services, these requirements make the treatment of children's viewing-related identifiers and advertising data an important compliance issue. However, COPPA's privacy purpose should not be confused with a comprehensive programme-classification system or a general federal algorithmic-safety regime for all teenagers. The comparative limitation lies in the scope of this particular instrument, not in an assertion that adolescents lack protection under every other American law.

8. AUSTRALIA: ACCOUNT RESTRICTIONS AND BROADER SAFETY CODES

Australia requires age-restricted social media platforms to take reasonable steps to prevent people under sixteen from creating or retaining accounts, with the obligation operating from



10 December 2025. The regulator's guidance identifies qualifying service features and relevant exclusions. This is an account-based obligation for a defined platform category, not a general prohibition on under-sixteens watching all internet-delivered entertainment.¹⁴

Australia also has broader Online Safety Codes and Standards. The Age-Restricted Material Codes address children's exposure to material such as pornography, high-impact violence and self-harm content across covered service categories. The regulator's 2026 explanation expressly discusses relevant generative-AI systems and companion chatbots. Duties must still be assessed under the applicable code and service definition.¹⁵ Australia therefore demonstrates two distinct regulatory choices: limiting account access for a category of social platforms and requiring protective measures against particular material across a wider ecosystem. Assessments of OTT compliance should identify which layer applies rather than equating the social-media age threshold with an all-purpose streaming restriction.

9. COMPARATIVE FINDINGS

The comparison identifies convergence around greater provider responsibility, but substantial differences in legal triggers and protected activities. Age thresholds are especially easy to misinterpret: India's child-data definition, COPPA's under-thirteen coverage and Australia's social-media account restriction perform different legal functions. They should not be compared as if each were a national "internet access age." A second finding is that content safety and data safety are complementary. A suitable film can be delivered through intrusive profiling, while a privacy-compliant service can still require stronger content controls. Neither a rating label nor a consent form answers every question raised by AI-mediated entertainment. Third, the regulatory unit matters. A hybrid platform may combine editorial catalogues, uploaded clips, advertising and interactive AI. A sound assessment should examine each function and its legal classification. Finally, regulatory ambition is not the same as proven effectiveness. Outcome claims require evidence on harmful exposure, circumvention, exclusion, complaint resolution and privacy consequences.

Jurisdiction	Main emphasis in reviewed instruments	Critical scope distinction
India	OTT ratings/access controls; enacted child-data safeguards awaiting commencement	Programme classifications and section 9 data duties perform different functions.
European Union	Audiovisual safeguards, platform duties and prohibited AI practices	AVMSD, DSA and AI Act have different definitions and triggers.
United Kingdom	Children's privacy by design; risk-based platform safety; ODPS controls	User-to-user/search duties are distinct from curated-programming regulation.
United States	COPPA notice, consent and children's data governance	Federal COPPA focuses on covered processing involving under-thirteens.
Australia	Under-sixteen social-media account	The account restriction is not a

	restrictions and wider safety codes	universal ban on children using OTT.
--	-------------------------------------	--------------------------------------

10. RECOMMENDATIONS

The following proposals are the article's policy recommendations, not statements that identical duties already exist in every jurisdiction.

- First, curated OTT providers should undertake child-impact assessments covering catalogue access, recommendations, trailers, advertisements and movement between profiles. Assessments should be repeated after material changes to AI or interface design.
- Second, age assurance should be proportionate and privacy-preserving. Services should seek the minimum information needed to establish the relevant age band, limit retention and offer accessible correction procedures. Assurance should not become a reason to build additional commercial profiles. This approach is consistent with the Commission's emphasis on effective, non-intrusive and non-discriminatory methods.⁷
- Third, child profiles should provide protective defaults, understandable controls and clear limits on engagement-driven features. Parents should receive usable tools, while children should receive explanations appropriate to their maturity. The Children's Code offers a useful design reference, although local legal requirements must still be considered.⁹
- Fourth, recommendation and moderation systems should undergo documented testing appropriate to their risks. Evaluation should examine whether restricted content appears in previews, whether filters work consistently across languages, and whether mistakes can be challenged through human review.
- Fifth, regulators should coordinate across media, privacy and online-safety responsibilities. Shared reporting formats could reduce duplication while preserving each authority's remit. For India, practical guidance connecting catalogue classification with the coming child-data framework would be particularly valuable.
- Finally, evaluation should include children's experiences and access needs. Safety measures should be judged both by the harm they prevent and by whether they preserve legitimate educational, cultural and social opportunities.

11. CONCLUSION

AI makes child online safety a question of how digital entertainment is organised as well as what it contains. The selected frameworks regulate different parts of that experience: program access, data collection, persuasive design, recommendation systems and platform accountability. Their differences make direct transplantation of a single age threshold or consent mechanism inadequate. An effective approach to curated OTT should combine age-appropriate content access, restrained data use, proportionate assurance and accountable AI design. Clear distinctions between platform categories, binding rules and guidance, and enacted and commenced provisions are essential to credible comparison. Future research should test whether these measures improve children's actual experiences rather than treating legislative adoption alone as evidence of success.

REFERENCES



1. eSafety Commissioner. (2026, March 6). Online safety codes introduce real-world protections for children online. <https://www.esafety.gov.au/newsroom/media-releases/online-safety-codes-introduce-real-world-protections-for-children-online>
2. eSafety Commissioner. (n.d.). Social media age restrictions. <https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions>
3. European Commission. (2025, July 14). Commission publishes guidelines on the protection of minors. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>
4. European Parliament and Council. (2010, as amended). Directive 2010/13/EU (Audiovisual Media Services Directive), articles 6a and 28b. Consolidated version dated 8 February 2025. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A02010L0013-20250208>
5. European Parliament and Council. (2022). Regulation (EU) 2022/2065 (Digital Services Act), articles 27–28 and 34–35. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>
6. European Parliament and Council. (2024, as amended). Regulation (EU) 2024/1689 (Artificial Intelligence Act), article 5(1)(b). <https://eur-lex.europa.eu/eli/reg/2024/1689>
7. Federal Trade Commission. (2025). FTC finalizes changes to children’s privacy rule limiting companies’ ability to monetize kids’ data. <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data>
8. Federal Trade Commission. (n.d.). Complying with COPPA: Frequently asked questions. <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>
9. Government of India. (2021). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Part III and Appendix: Code of Ethics, online curated content. <https://www.mib.gov.in/sites/default/files/2024-02/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf>
10. Government of India. (2023). Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), sections 2(f) and 9. <https://www.meity.gov.in/static/uploads/2024/06/2bflf0e9f04e6fb4f8fef35e82c42aa5.pdf>
11. Information Commissioner’s Office. (n.d.). Age appropriate design: A code of practice for online services. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/>
12. Ministry of Electronics and Information Technology. (2025, November 13). Notification G.S.R. 843(E): Commencement of provisions of the Digital Personal Data Protection Act, 2023. Gazette of India.



International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

<https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf>

13. Ofcom. (2025, April 24; updated July 30). Statement: Protecting children from harms online. <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-children-from-harms-online>
14. Ofcom. (n.d.). Guide to video on demand. <https://www.ofcom.org.uk/tv-radio-and-on-demand/video-on-demand/video-on-demand>
15. UNICEF Innocenti. (2025). Guidance on AI and children, version 3.0. <https://www.unicef.org/innocenti/reports/policy-guidance-ai-children>