

**CUTS Comments on the Draft Amendments to Information
Technology (Intermediary Guidelines and Digital Media
Ethics Code) Rules, 2021**

Submitted by: CUTS International
Consumer Unity & Trust Society
www.cuts-international.org
May 2026

Prepared by: Sohom Banerjee, Senior Research Associate, CUTS International
(Consumer Unity & Trust Society)



Executive Summary

CUTS International welcomes the Ministry of Electronics and Information Technology's (MeitY) continued efforts to strengthen India's digital governance framework through the proposed amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The proposed amendments reflect a timely and important attempt to improve accountability, enforceability, and responsiveness within India's rapidly evolving digital ecosystem. At a time when online platforms play an increasingly central role in public discourse, commerce, and access to information, strengthening intermediary due diligence and grievance redressal mechanisms is both necessary and legitimate.

At the same time, regulatory expansion in the digital ecosystem must be accompanied by legal clarity, procedural safeguards, and proportional implementation. A well-calibrated intermediary liability framework should preserve the foundational principles of safe harbour under Section 79 of the Information Technology Act, 2000, while ensuring that compliance obligations remain predictable, transparent, and operationally practicable across platforms of varying scale and capacity.

In this context, CUTS has undertaken a legal, constitutional, and practical analysis of the proposed amendments and respectfully submits the following key observations and recommendations:

1. Need for Greater Clarity on Data Retention Obligations

The proposed clarification that retention obligations operate "without prejudice to other applicable laws" is a welcome step. However, intermediaries operating across multiple regulatory domains may face practical uncertainty where different frameworks prescribe varying retention standards. For instance, while the IT Rules prescribe a baseline retention period, sector-specific frameworks may require significantly longer retention durations, whereas the Digital Personal Data Protection Act, 2023 emphasises data minimisation principles.

CUTS recommends greater harmonisation and clearer guidance regarding the application of retention requirements across different categories of data to prevent excessive retention practices, reduce compliance burdens, and align intermediary obligations with emerging data protection principles.

2. Distinguishing Binding Directions from Advisory Instruments

The proposal to strengthen intermediary compliance with clarifications, advisories, SOPs, and directions issued by the Ministry may improve enforcement effectiveness and reduce ambiguity in compliance obligations. However, the increasing reliance on subsidiary instruments also raises concerns regarding regulatory certainty and the potential expansion of executive discretion beyond legislative intent.

CUTS recommends that:

- A clear hierarchy between binding and non-binding instruments be articulated;

- Binding directions be accompanied by transparent publication, reasoned justification, stakeholder consultation, and ex-ante cost–benefit assessments;
- Subsidiary instruments be limited to clarifying existing rules or prescribing procedural requirements ancillary to duly notified regulations; and
- Such instruments be subjected to parliamentary oversight consistent with delegated legislation practices.

These safeguards would strengthen accountability while preserving regulatory predictability for intermediaries, creators, entrepreneurs, and end users.

3. Preserving the Distinction Between Intermediaries and Publishers

The proposed expansion of Part III to intermediaries hosting news and current affairs content generated by non-publisher users reflects the changing realities of digital content dissemination. However, the absence of explicit legal safeguards may create a risk of indirect expansion of publisher-like liability onto intermediaries.

CUTS recommends that the Rules explicitly preserve the distinction between passive hosting and editorial control. Intermediaries should not be treated as publishers solely by virtue of hosting, transmitting, recommending, or facilitating access to third-party content unless they exercise demonstrable editorial control or material influence over such content.

Maintaining this distinction is critical to preserving the safe harbour framework under Section 79 of the IT Act and preventing unintended chilling effects on lawful expression and access to information.

4. Strengthening Procedural Safeguards for the Inter-Departmental Committee

The proposal to expand the powers of the Inter-Departmental Committee may improve responsiveness in addressing harmful content. However, broader powers should be accompanied by robust procedural safeguards to ensure fairness, transparency, and accountability.

CUTS recommends:

- Clearly defined thresholds and triggers for Ministry-referred or suo motu cases;
- Transparent and documented decision-making processes;
- Disclosure of relevant material to affected parties;
- Meaningful opportunities to be heard; and
- Reasoned and proportionate decisions subject to challenge or review mechanisms.

5. Balancing Accountability with Innovation and Inclusion

While stronger oversight may be necessary to address misinformation, user harm, and platform accountability concerns, regulatory expansion should not inadvertently increase compliance burdens for startups, emerging platforms, and smaller intermediaries. Excessive or unclear

compliance obligations may increase operational costs, encourage over-cautious content moderation, and undermine innovation, competition, and digital inclusion.

CUTS therefore recommends proportional compliance frameworks and periodic ex-ante and ex-post Regulatory Impact Assessments (RIAs) to evaluate the real-world effects of the amendments on users, platforms, and market dynamics.

The proposed amendments represent a constructive step toward strengthening India's digital governance architecture. Going forward, regulatory implementation should remain guided by the constitutional principles of legitimacy, necessity, and proportionality, as articulated in Justice K.S. Puttaswamy v. Union of India, ensuring that interventions remain lawful, transparent, evidence-based, and minimally intrusive.

CUTS remains committed to supporting MeitY through evidence-based research, stakeholder consultations, Regulatory Impact Assessments, and policy monitoring initiatives aimed at ensuring that India's digital governance framework continues to promote accountability, innovation, user trust, and inclusive digital growth.

1. Introduction

CUTS International would like to appreciate the Ministry of Electronics and Information Technology (MeitY) for its continued efforts to strengthen India's digital governance framework in a manner that seeks to balance openness, safety, trust, and accountability in the online ecosystem. The consultative approach adopted by the Ministry, as reflected in this stakeholder engagement process, is particularly commendable and aligns with global best practices in participatory policymaking.

The proposed amendments, which aim to enhance clarity, improve enforceability, and strengthen oversight mechanisms, are timely given the increasing complexity of digital platforms and the growing societal reliance on intermediary services. While technology platforms have made progress in strengthening user safety, significant gaps persist in grievance redressal systems, particularly in their ability to respond swiftly and contextually to emerging harms. Research indicates that harmful or dangerous speech can spread rapidly through influential accounts, amplifying its impact well before corrective action is taken.¹ These challenges underscore the need to enhance grievance mechanisms, so they are not only more responsive and transparent but also better attuned to India's complex socio-cultural landscape. MeitY's efforts to refine the compliance framework are therefore commendable as a constructive step toward ensuring accountability while safeguarding the interests of millions of digital Nagariks.

At the same time, the mechanisms adopted to advance platform accountability should provide regulatory clarity and predictability for intermediaries. A well-calibrated framework grounded in clear statutory authority and transparent processes can help ensure that compliance expectations are both consistent and practicable across the ecosystem. In this regard, it is important that due diligence obligations remain closely aligned with the structure and intent of the IT Act, particularly in relation to the scope of intermediary liability and safe harbour protections. Clarity in how such obligations are triggered, communicated, and enforced can reduce uncertainty and support more effective implementation by platforms of varying sizes and capacities. Ensuring that regulatory instruments are accessible, well-defined, and proportionate will further strengthen trust in the compliance framework. This, in turn, can enable intermediaries to respond more confidently and efficiently to emerging harms, while continuing to support innovation and the growth of India's digital ecosystem. Upon a detailed legal, constitutional, and practical analysis of the Draft Amendment Rules, we find that several proposed provisions raise concerns which have been discussed below.

CUTS looks forward to MeitY considering its suggestions and contributing to efforts that empower consumers and shape a regulatory framework that maximises benefits and minimises harms for citizens.

We would be glad to present our submission in person before MeitY.

¹Insights Into Incitement: A Computational Perspective on Dangerous Speech on Twitter in India, available at: <https://arxiv.org/abs/2111.03906>

2. On Retention Obligations and Legal Clarity (Draft Amendment Rule 3(1)(g) and 3(1)(h))

The clarification that data retention obligations under Rule 3 are “without prejudice to other applicable laws” is a welcome step, as it seeks to avoid interpretational conflicts and situates the Rules within India’s broader legal framework.

At the same time, the use of the phrase “without prejudice to any other law”, while a standard savings clause, may inadvertently create an open-ended compliance environment in practice, particularly for intermediaries operating across multiple regulatory domains with differing retention requirements.

For instance, while Rule 3 prescribes retention of certain categories of data for a minimum period of 180 days, sector-specific frameworks, such as financial regulations, may require retention of transactional or KYC-related data for significantly longer durations (e.g., five to ten years). At the same time, the Digital Personal Data Protection Act, 2023 emphasises the principle of data minimisation, requiring that personal data be retained only for as long as necessary for the specified purpose.

While sector-specific laws may prevail within their respective domains, operational challenges arise in multi-service or multi-functional platform environments where different categories of data such as user-generated content, platform logs, and account-level or transactional data are subject to overlapping regulatory expectations. In the absence of explicit guidance on how these obligations apply across different data layers within a single platform, intermediaries may face uncertainty in determining the appropriate retention standard for each category of data.

For example, a platform facilitating payments may be required to retain KYC or transactional data for longer durations under financial regulations, while simultaneously complying with the 180-day retention requirement under the IT Rules for content-related data, and the data minimisation principle under the Digital Personal Data Protection Act, 2023. Without clear guidance distinguishing the applicability of these obligations across data types, intermediaries, particularly smaller platforms, may adopt a risk-averse approach by aligning with the most stringent retention requirement across frameworks, even where such retention may not be necessary for all categories of data.

Such an approach, while rational from a compliance perspective, may lead to unintended outcomes, including increased compliance burdens, higher storage costs, and a tendency toward excessive data retention. This may not be fully aligned with data minimisation principles and could elevate risks relating to data security, data breaches, and broader consumer welfare.

In this context, a more harmonised and bounded approach to data retention obligations would be beneficial. Greater clarity on the application of retention requirements across different data categories, as well as guidance on precedence and coordination across regulatory frameworks, would help ensure legal certainty while aligning with emerging data protection principles.

CUTS therefore suggests that:

- Efforts may be made toward harmonisation of retention requirements across applicable laws and regulatory frameworks; or
- At a minimum, the Ministry may consider issuing clear guidance notes or compliance frameworks to help intermediaries, especially SMBs, navigate overlapping obligations in an efficient and predictable manner.

Such measures would help reduce compliance friction while preserving regulatory objectives and strengthening alignment with data protection principles.

Suggested Amendment:

“...subject to applicable data protection principles, including data minimisation under the Digital Personal Data Protection Act, 2023, unless retention is specifically extended pursuant to a lawful order issued by a competent authority for a defined purpose and duration.”

3. On Strengthening Compliance with Ministry Directions (Draft Amendment Rule 3(4))

The proposal to explicitly mandate compliance by intermediaries with clarifications, advisories, directions, SOPs, and guidelines issued by the Ministry is a significant step toward improving regulatory certainty and operational clarity. In several cases, large digital intermediaries have exhibited delays in complying with content takedown obligations, as evidenced by the 2025–26 Parliamentary Committee report on cyber safety. The report noted that while over 1.41 lakh URLs were forwarded to platforms for removal through the Sahyog portal, there were documented instances of delayed compliance. The persistence of these delays, despite a formal regulatory mechanism and significant volumes of flagged unlawful content, highlights a gap between legal obligations and timely enforcement.² From a governance standpoint, this helps reduce ambiguity that platforms often face in interpreting compliance obligations.

However, from a balanced regulatory perspective, it is important to ensure that such instruments, particularly advisories and guidelines, are clearly distinguished from binding legal directions. The design of such mechanisms must ensure that they operate within a predictable and legally grounded framework. The safe harbour regime under Section 79 of the IT Act has been carefully structured as a conditional immunity, with liability typically arising only when intermediaries fail to act upon clearly defined legal triggers.

Without such distinction, there is a risk that non-statutory instruments may effectively acquire binding force, potentially expanding executive discretion beyond legislative intent. This could have broader implications for regulatory predictability and ease of doing business, particularly for smaller intermediaries and emerging platforms. In turn, increased compliance uncertainty and costs are likely to be passed on downstream to small entrepreneurs, creators, and end users who rely on these platforms for access, livelihoods, and digital participation.

² [No platform’s ever lost safe harbour despite cases of delayed compliance with takedown notices—House panel | ThePrint](#)

CUTS would therefore suggest that:

- A clear hierarchy of regulatory instruments be articulated (e.g., binding vs non-binding);
- Any binding direction issued by the Ministry should be accompanied by transparent publication, clear reasoning, proportionality standards, stakeholder consultation, and an ex-ante cost–benefit assessment. Such procedural safeguards are necessary to ensure regulatory predictability, accountability, and proportionality in implementation.
- Further, the use of subsidiary instruments, such as clarifications, advisories, directions, SOPs, and guidelines, should only be limited to:
 - (a) clarifying ambiguities within existing regulations; and
 - (b) laying down procedural requirements that are ancillary to notified rules.
- To strengthen legal robustness and institutional accountability, such instruments should also be formally laid before Parliament, like delegated legislation practices. This approach, as seen in frameworks such as the Securities Markets Code, can help ensure democratic oversight and reduce the risk of legal challenges.

This would enhance both legal certainty for intermediaries and accountability in regulatory action.

Suggested Amendments:

(c) compliance with any clarification, advisory, order, direction, standard operating procedure, code of practice or guideline issued under clause (a) shall form part of the due diligence obligations of the intermediary under section 79 of the Act to the extent that such instrument clarifies existing statutory obligations or procedural requirements ancillary to notified rules, consistent with the procedure prescribed under Section 87(3) of the Act.

Provided that such clarification, advisory, order, direction, standard operating procedure, code of practice or guideline issued shall not automatically vitiate the protections under Section 79 of the Act absent a violation of a formal rule or binding legal order.

Provided further that all such instruments shall be laid before each House of Parliament in a manner consistent with the procedure for delegated legislation.

4. On Expanding Scope of Digital Media Oversight (Part III - Draft Amendment Rule 8(1))

CUTS notes and appreciates the clarification provided by senior officials from MeitY and MIB during the stakeholder consultation held on April 7, 2026³, that intermediaries would not be held liable for news and current affairs content generated or uploaded by users who are not publishers within the meaning of the Rules. The clarification that the proposed amendment is intended to facilitate communication and dissemination, rather than impose publisher-like liability on

³ Edition 25: 'No liability intended for intermediaries under Part III,' govt to industry

intermediaries for third-party user content, is a welcome step that addresses concerns relating to indirect expansion of intermediary liability.

We also acknowledge that extending the applicability of Part III to intermediaries hosting news and current affairs content generated by non-publisher users reflects an attempt to address the evolving nature of digital content dissemination, where platforms increasingly function as important vectors for the discovery, amplification, and circulation of news content.

While this reflects an important recognition of platform realities, it also raises significant considerations regarding:

- The blurring of roles between intermediaries and publishers; and
- The potential indirect expansion of content liability onto intermediaries.

The principle of regulatory certainty requires that the Government's stated intent be explicitly reflected in the text of the Rules. In the absence of express statutory clarification, there remains a risk of interpretational expansion that could indirectly subject intermediaries to publisher-like obligations for third-party content. This, in turn, may incentivise over-cautious content moderation practices and increase legal uncertainty for intermediaries, creators, and users relying on digital platforms for lawful expression and access to information.

Accordingly, CUTS recommends that the proposed amendment be refined to clearly distinguish between passive hosting functions performed by intermediaries and editorial functions performed by publishers.

In this regard:

- The insertion of clause (b) relating to "users who are not publishers" should be reconsidered, with greater focus placed on circumstances involving algorithmic amplification, active content curation, or demonstrable editorial intervention by intermediaries.
- The Rules should explicitly preserve the distinction between passive hosting and editorial control to ensure that intermediaries are not indirectly subjected to publisher-like obligations solely by virtue of hosting, transmitting, recommending, or facilitating access to third-party content.
- Intermediaries should not be treated as publishers unless they exercise demonstrable editorial control or material influence over the creation, selection, modification, or presentation of the content in question.

Suggested Amendment:

"For the removal of doubts, an intermediary hosting, transmitting, recommending, or facilitating access to news and current affairs content generated by users who are not publishers shall not be deemed to be a publisher under these Rules solely by virtue of such hosting, transmission, recommendation, or facilitation, unless the intermediary exercises demonstrable editorial control or material influence over the creation, selection, modification, or presentation of such content."

5. On Strengthening the Inter-Departmental Committee (Draft Amendment Rule 14(2))

The proposal to expand the scope of the Inter-Departmental Committee to consider matters beyond complaints, including suo motu or Ministry-referred cases, enhances the responsiveness of the regulatory framework.

However, given the expanded mandate, it becomes equally important to ensure that:

- The Committee operates with procedural safeguards, including transparency in proceedings.

To ensure robustness and credibility of the expanded mandate of the Inter-Departmental Committee, it would be important that:

- Clearly defined processes and thresholds are established for initiating reviews, including cases taken up suo motu or referred by the Ministry.
- Such processes and triggers are formally recorded and documented, ensuring consistency and auditability.
- The material forming the basis of any proposed action is disclosed for review by the concerned parties, subject to reasonable safeguards.
- Affected parties are provided a meaningful opportunity to be heard, including access to relevant information; and
- Decisions are reasoned, proportionate, and recorded in writing, with provision for an effective mechanism to challenge or appeal such decisions.

Strengthening these procedural aspects would reinforce due process and institutional credibility.

Suggested Amendments:

“(b) referred to it by the Ministry subject to clearly defined thresholds and documented triggers for such referrals.

Provided that matters referred directly by the Ministry shall be limited to instances where the content poses an imminent threat to public order, sovereignty, or user safety, or where there is a demonstrable and systemic failure of the Level I and Level II grievance redressal mechanisms to address consumer complaints.

Provided further that the affected parties are provided a meaningful opportunity to be heard and decisions, consistent with existing procedural safeguards in the IT Rules under Rule 4(1)(a), Rule 3(1)(d)(ii), and Rule 6(1).”

6. On Balancing Oversight with Innovation and Market Dynamics

From a broader policy perspective, the amendments indicate a shift toward greater regulatory oversight and enforceability, which is understandable given concerns around misinformation, user harm, and platform accountability.

At the same time, it is important that regulatory expansion does not inadvertently:

- Increase compliance uncertainty for emerging platforms and startups, the cost of which is likely to be passed on to users, thereby potentially undermining digital inclusion and access gains, particularly for price-sensitive segments, or
- Lead to over-cautious content moderation (chilling effect) due to risk-averse platform behaviour.

CUTS would therefore suggest that:

- The Ministry should consider proportional compliance frameworks, especially for smaller intermediaries.
- Periodic ex-ante and ex-post Regulatory Impact Assessments (RIA) be undertaken to evaluate both the anticipated and real-world effects of the amendments, ensuring that regulatory objectives are met without unintended consequences.

7. Concluding Observation

Overall, the proposed amendments represent a progressive attempt to strengthen India's digital governance architecture, particularly by enhancing clarity and enforceability of intermediary obligations.

Going forward, the key policy challenge will lie in ensuring that:

- Regulatory authority is exercised in a manner consistent with the constitutional principles of legitimacy, necessity, and proportionality, as articulated by the Supreme Court in Justice K.S. Puttaswamy v. Union of India, ensuring that regulatory interventions are lawful, evidence-based, minimally intrusive, transparent, and aligned with clearly defined public interest objectives.
- Safe harbour principles are preserved, and
- The framework continues to support innovation, competition, user rights, access, and inclusion, alongside accountability, ensuring that regulatory objectives do not come at the cost of broader digital ecosystem development.

CUTS remains committed to supporting the Ministry in refining this framework and would be happy to engage further on specific aspects of implementation and impact.

8. Potential Role of CUTS International:

1. **Regulatory Impact Assessment (RIA):** CUTS can undertake independent RIAs to evaluate the economic, compliance, and consumer welfare implications of the proposed amendments, ensuring that regulatory objectives are achieved without unintended market distortions.
2. **Pan-India Evidence-Based Studies:** Leveraging its field presence, CUTS can conduct large-scale, multi-state studies to assess how intermediary compliance measures impact user behaviour, platform practices, and digital inclusion across diverse regions.
3. **Stakeholder Consultations & Capacity Building:** CUTS can facilitate multi-stakeholder dialogues (industry, government, civil society) and design capacity-building programmes for intermediaries, especially MSMEs and emerging platforms, to enhance compliance readiness.
4. **Policy Monitoring & Feedback Loop:** CUTS can support MeitY through continuous policy monitoring, enabling early identification of harms, risks, and systemic stress, while documenting implementation challenges (e.g., over-compliance, chilling effects) and providing timely, evidence-based policy recommendations.