GNI Statement on India's Draft IT Amendment Rules 2026: Concerns on Privacy, Free Expression, and Executive Overreach

The Global Network Initiative (GNI) expresses deep concern regarding the Draft Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Second Amendment Rules, 2026, published by India's Ministry of Electronics and Information Technology on 30 March 2026. While presented as "clarificatory and procedural," the proposed amendments introduce substantive changes that risk expanding censorship, undermining privacy protections, and eroding due process in India's digital ecosystem.

In addition, several GNI members have raised concerns about the far-reaching implications of these amendments. Taken together, the amendments could significantly reshape the balance between state authority, platform responsibility, and Indian users in ways that would negatively impact freedom of speech, privacy and access to information. GNI calls on the Government of India to withdraw or substantially revise the proposed amendments to ensure alignment with India's constitutional protections, international commitments, and international human rights standards.

The Regulatory Context

The Information Technology Act, 2000 is the parent statute governing India's intermediary liability regime. Section 79 of the Act provides intermediaries, including social media platforms, search engines, and internet service providers, with protection from civil and criminal liability for content posted by their users, commonly referred to as "safe harbour." This protection is conditional – intermediaries must observe due diligence as prescribed by the legislation and prescribed under Shreya Singhal v Union of India.

The conditions for safe harbour are elaborated in the 2021 IT Rules. GNI had previously commented on the overbroad application and lack of definitional clarity of the rules in 2021. The rules are organised into several parts.Part II sets out due diligence obligations for intermediaries. Part III prescribes a separate Code of Ethics for digital news publishers and over-the-top (OTT) platforms, administered by the Ministry of Information and Broadcasting through a three-tier grievance mechanism culminating in an Inter-Departmental Committee (IDC). The Draft Amendments make targeted but consequential changes to both parts of this framework. These changes, taken together, significantly expand executive authority over platforms and their users while weakening existing legal safeguards and oversight mechanisms.

The Risks of Expanding Data Retention

The amendments to Rules 3(1)(g) and 3(1)(h) introduce mandatory data retention obligations that require intermediaries to retain user data for a minimum period of 180 days, irrespective of whether the purpose for which such data was collected has been fulfilled. This approach appears to conflict with the core principles of India's Digital Personal Data Protection Act, 2023, including purpose limitation and the right to erasure.

Extending data retention obligations without clear necessity and proportionality raises significant risks, as the prolonged storage of large volumes of personal data increases exposure to breaches, misuse, and unauthorised access, particularly for sensitive information. Without adequate legal safeguards and transparency requirements, such measures risk undermining trust in digital services. Data retention

frameworks should therefore be grounded in clear, lawful purposes and incorporate principles of necessity, proportionality, and data minimisation, alongside robust safeguards to protect user rights.

Executive Overreach and Intermediary Liability

The proposed insertion of Rule 3(4) raises serious concerns about the expansion of executive authority over intermediaries. It requires platforms to comply with a wide range of executive instruments as a condition for retaining safe harbour protections under the Information Technology Act.

Under the current framework, Section 79 of the Information Technology Act provides intermediaries with conditional immunity from liability for third-party content, thereby allowing for the development of vibrant, user-generated content ecosystems.

As recognized by the Supreme Court in Shreya Singhal v. Union of India, this framework is intended to balance the need for content regulation with the protection of free expression. Intermediaries are only required to act upon '*actual knowledge from a court order or on being notified by the appropriate government or its agencies*'. This ensures that content removal and platform obligations arise from accountable, challengeable legal instruments rather than informal executive preferences.

The proposed amendment, by contrast, would extend the compliance obligation to clarifications, advisories, orders, directions, standard operating procedures, codes of practice or guidelines to remove or disable access. These are instruments that carry no independent legal authority, are not subject to the same scrutiny as statutory laws, and can be issued without parliamentary sanction. In effect, this collapses the distinction between a lawful order and an administrative preference, incentivizing platforms to treat the latter with the same deference as the former to avoid losing safe harbour protections. This may, in turn lead to over-censorship and create a chilling effect on online expression, particularly for speech that is critical of authorities or relates to sensitive or controversial issues.

Further, the lack of a clear requirement for transparency, independent oversight, or meaningful parliamentary scrutiny creates the potential for opaque and ad hoc decision-making processes that bypass established democratic safeguards. As seen in other contexts and noted in GNI's content regulation and policy brief, opaque regulatory processes can undermine both rights protections and regulatory legitimacy.

Extending Content Regulation Rules to Users

The amendments to Rule 8 and Rule 14 significantly broaden the scope of content regulation by extending the Code of Ethics and the authority of the Inter-Departmental Committee to intermediaries and users who share news and current affairs content, even if they are not themselves recognized publishers.

This expansion would bring ordinary users within the ambit of state-controlled content regulation mechanisms, thereby increasing the range of tools available for content restriction and raising serious concerns for freedom of expression and access to information. Without clear safeguards, due process protections, and transparency requirements, these mechanisms may be used to restrict lawful speech and limit democratic participation online in ways that are otherwise protected against under the current legal regime.

Grave Implications for Freedom of Expression, Privacy and Human Rights

Taken together, the Draft Amendments signal a shift toward increased centralization of authority over digital platforms and online content. Measures that expand data retention, broaden executive discretion, and extend regulatory frameworks to users risk undermining fundamental rights and creating an environment of uncertainty for platforms and users alike.

The regulatory choices made by MeitY have implications not only for hundreds of millions of users in India, but also for global norms around platform governance, intermediary liability, and the relationship between states and digital expression, a phenomenon that some have called the Delhi effect.

GNI has consistently emphasized that digital governance frameworks must be grounded in principles of legality, necessity, proportionality, transparency, and accountability. As governments around the world develop new regulatory approaches, these principles are essential to ensuring that efforts to address legitimate policy concerns do not come at the expense of fundamental rights.

GNI calls on the Government of India to:

- Withdraw or substantially revise the proposed amendments to ensure alignment with India's constitutional protections, international commitments, and international human rights standards;
- Ensure that any data retention requirements are clearly defined, necessary, proportionate, and consistent with principles of purpose limitation and data minimization;
- Maintain clear, transparent, and legally grounded processes for content restriction, ensuring that user-generated content is not subject to disproportionate or indirect regulatory mechanisms;
- Engage in open, inclusive, and meaningful consultation with civil society, industry, and technical experts in the development of digital policy frameworks.

GNI remains ready to engage constructively and offer support toward building a digital ecosystem that respects fundamental rights.

About the Global Network Initiative

GNI is the leading multistakeholder forum for accountability, shared learning, and collective advocacy on government and company policies and practices at the intersection of technology and human rights. Over the last several years, GNI has reviewed, commented on, and helped shape a range of "online safety" bills, data protection laws, and intermediary liability laws across several jurisdictions. Our human rights analysis and recommendations for policymakers can be found in the Content Regulation & Human Rights Policy Brief, which uses international human rights principles to analyze a wide range of legislative efforts and provides proactive guidance on how to address online safety and digital regulations in a rights-protective manner