# CONTENT REGULATION AND HUMAN RIGHTS IN THE DIGITAL AGE

## Multistakeholder Roundtable on India's Draft Intermediaries Guidelines Amendments

**26 June 2020 --- 6:00pm IST / 2:30pm CEST / 8:30am EDT / 5:30am PDT**

## Roundtable Report

On June 26, 2020, the Global Network Initiative (GNI) and the Indian Internet Multistakeholder Coalition (India IMSC) hosted a multistakeholder roundtable discussion to examine key provisions of India's Draft Intermediaries Guidelines (Amendment) Rules, 2018 ("the Draft Amendments ") through the lens of international human rights law and principles. This roundtable was part of GNI's on-going consultations on content regulation and human rights.

GNI provided the participants with a draft version of its forthcoming policy brief, "Content Regulation and Human Rights in the Digital Age," which was presented as a framework for considering good policy practice. Though many human rights are impacted by content regulation, controls on communication most directly impact the fundamental rights to freedom of expression and privacy.

A member of the India-based non-profit, Software Freedom Law Center, India, (SFLC.in), which facilitates the India IMSC, delivered opening remarks, and stressed that the onus is on governments to protect safety, security, freedom of speech and human rights. The impact of regulations put in place today will be felt by many generations to come, and as such careful deliberation and collaborative discussion is key. The subsequent discussion of the proposed amendments to the Intermediary Guidelines was organized around three key components of GNI's policy brief: i) legality and legitimacy, ii) proportionality, and iii) privacy.

Content regulation initiatives continue to spread around the world. GNI believes proactive and honest multistakeholder conversations on this topic are key to ensuring that responses to digital harms are legal, proportionate, and fit-for-purpose. GNI looks forward to further consultations on India's draft amendments and other content regulation efforts.

The conversation was held under the Chatham House Rule. Nothing in this report is attributed to any individual, institution, or affiliation, nor does it necessarily reflect GNI's, the India IMSC's, or other participants' positions.

## Table of Contents

# An Introduction to India's Draft Intermediaries Guidelines Rules

In December 2018, India's Ministry of Electronics and Information Technology ("MeitY") released the Draft Intermediaries Guidelines (Amendment) Rules, 2018 ("the Draft Amendments"). The Draft Rules suggested changes in the existing due diligence standards to be observed by Internet intermediaries in India, in order to avail themselves of the protection of safe harbour provisions for user generated content under Sec. 79 of the Information Technology Act, 2000.

There are two key cases that have shaped the intermediary liability law in India. In 2004, a scandal involving the sale of a pornographic clip on Bazee.com and the subsequent arrest of the company's CEO led to the creation of a committee to reevaluate the Information Technology Act. In its final report, the committee recommended that intermediaries must do their 'due diligence' in order to receive immunity, which was accepted by the government. This was the first amendment to section 79 since its inception in 2000. The second was made through the *Shreya Singhal vs. Union of India* (2015) case. In that decision, the Supreme Court 'read down' section 79, and shielded intermediaries from liability unless they failed to act upon a court order or government notice that particular content was illegal.

In 2018, the intermediary liability rules once again opened up for debate, after a Parliamentary discussion on incidents of violence triggered by the misuse of social media platforms. MeitY issued a press note alongside the draft rules, which states that the "misuse of social media by criminals and anti-national elements have brought new challenges to Law Enforcement Agencies." The draft rules say that intermediaries will now have to proactively monitor and filter their users' content through automated tools or other appropriate mechanisms, and be able to trace the originator of questionable content to avoid liability for users' actions. Additionally, intermediaries are required to provide assistance to government agencies — who must clearly state in writing or electronic means the purpose for seeking such information — within 72 hours. Upon notification, an intermediary will have 24 hours to remove or disable unlawful content.

A number of stakeholders have raised concerns about the potential adverse impact of the draft rules on citizens' freedom of expression and privacy in the online space.[1] Article 19 of the Constitution of India guarantees the freedom of speech and expression, as one of its six freedoms. However, Article 19(2) allows the government to impose "reasonable restrictions" on freedom of speech and expression in the interests of the sovereignty and integrity of India, security of the

[1] *See, e.g.,* GNI, Submission on Draft Amendments to Intermediary Guidelines in India, January 2019, https://globalnetworkinitiative.org/gni-submission-draft-amendments-intermediaries-guidelines-act/ ; Centre for Internet Society, "Response to the Draft of The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018," January 31 2019, https://cis-india.org/internet-governance/resources/Intermediary%20Liability%20Rules%202018.pdf

state, and public order, among others.[2] In the context of this legal landscape, there are varying opinions on whether the draft rules meet the international human rights principles of legality, legitimacy, and necessity.

Once the new rules are notified to Parliament, which can be done at any time, they will become final.

## Presentation

### A Human Rights Based Approach to Content Regulation

The roundtable began with an overview of the analytical framework used in GNI's forthcoming policy brief, "Content Regulation and Human Rights in the Digital Age." The brief was developed in response to an increase in governmental efforts around the world that claim to address various forms of harm related to user-generated online content, which GNI refers to broadly as "content regulation." It uses a human-rights based approach to analyze content regulation measures from a dozen countries around the world.

International human rights law reminds us to put individual rights at the center of efforts to improve our shared digital spaces. This is critical because these spaces and services remain primarily devoted to acts of communication. History has repeatedly shown the perils of efforts to govern communication that put majoritarian interests above the rights of individuals, journalists, critics, and dissidents.

The brief demonstrates that the norms and principles articulated in international human rights law provide a universal, time-tested, and robust framework that can help lawmakers find creative and appropriate ways to engage stakeholders, reconcile different interests, and mitigate unintended consequences of content regulation.

The brief examines content regulation efforts for their compatibility with three key principles of international human rights law: legality, legitimacy, and necessity. It also considers proportionality as a component of necessity and extends this analysis to privacy.

#### *Legality*

[2] Article 19(2) of the Constitution states: "Nothing in sub clause (a) of clause ( 1 ) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence."

The principle of legality establishes that restrictions on freedom of expression must be provided by public laws "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly." In other words, laws must clearly define what is prohibited and by reference what is allowed. Those who are in charge of dispensing the law must also have sufficient guidance on "what sorts of expression are properly restricted and what sorts are not." This is particularly important when private entities, and not law enforcement or regulators, are responsible for adjudication. Sufficient guidance ensures that the laws are predictable, consistent, and non-discriminatory. The legality principle is essential for curbing the "chilling effect" of ambiguous content regulation, which can contribute to self-censorship from individuals who fear violating the law and overly aggressive enforcement by intermediaries who fear the consequences of failing to abide by the law.

### *Legitimacy*

The principle of legitimacy holds that laws restricting expression can only be justified to achieve specific, enumerated purposes. These may include respect for the rights or reputations of others or the protection of national security, public order, public health or morals. While international law gives states significant latitude to determine the activities that justify restrictions, that discretion is not unlimited. International courts and authorities have made clear that the right to freedom of expression is broad and encompasses "even expression that may be regarded as deeply offensive."

In addition, numerous consensus United Nations resolutions establish that the same rights that are protected offline must also be protected online. Inconsistencies in the treatment of online and offline speech may be exploited by regimes and actors who do not respect democratic norms. Therefore, it is critical to protect speech equally and consistently, and to resist differentiating approaches to expression across offline and online mediums.

### *Necessity and Proportionality*

The principle of necessity requires states seeking to restrict expression to articulate the threat imposed by a specific type or piece of speech as well as the "direct and immediate" connection between the expression and the threat.

The related principle of proportionality requires that any restrictive law, as well as the actions of administrative and judicial authorities in their application of that law, must be: (i) proportionate to the interest being protected; (ii) appropriate to achieve that protective function; and (iii) the least intrusive instrument among those which might achieve that protective function.

In the content regulation context, the principles of necessity and proportionality should guide lawmakers to think carefully about which types of services are most appropriately positioned to address specific concerns. Shifting liability for illegal content from creators to intermediaries

rarely if ever fits this description. Similarly, punitive sanctions, rigid timelines for content adjudication, and pre-emptive filtering requirements are also likely to run afoul of the necessity and proportionality principles, and as such are likely to prove ineffective or counterproductive. To ensure content regulation efforts are appropriately and narrowly tailored and to guard against unintended consequences, lawmakers should look to proven approaches based on concepts like transparency, due process, and remedy. They should also consider the perspectives of and, where appropriate, provide explicit protections for specific actors such as journalists and vulnerable groups.

#### *Privacy*

Many content regulation efforts lack protections for the fundamental right to privacy and some actively undermine individual privacy. Requirements to proactively monitor, track, or trace content often lack consideration of associated privacy risks. In addition, compelling content hosts to proactively report user-generated content and associated data to law enforcement agencies further undermines this right. Moreover, the explicit prohibition or implicit limitation of the use of anonymity and encryption tools signals a disregard for the importance of privacy and the rights it enables.

Finally, it is worth noting as one participant in the roundtable underscored, that these principles are related but yet divisible. As such, even if a particular rule or application of law passes the legitimacy test, it may nevertheless fail to satisfy the legality analysis, etc.

# Discussion

## Legality and Legitimacy

#### *Agenda prompt:*

*When the draft rules were released in 2018, several concerns were submitted by the participants of this discussion during the consultation period. Some of those key concerns included: Who has the authority to define the particular meaning of a term(s)? Are the goals behind the rules legitimate? Are the rules sufficiently clear? Is there sufficient legal basis for the traceability provision?*

#### *Delegation of Rulemaking Authority*

Given that the nature of communication has evolved since 2011, and more of the population is on social media, the due diligence provision outlined in section 79(2)(c) of the IT Act[3] may well need to be reevaluated. The government is duly empowered to introduce subordinate legislation, as

[3] Section 79(2)(c) of the IT Act states "the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf."

long as it abides by free expression and other principles outlined in Article 19(2) of India's Constitution. The intention behind the rules was to hold companies accountable to the principles stated in Article 19(2) in their decision-making about content on their platforms. While the government has the legal authority to continue evaluating different options, the relevant regulators will consider new input and craft the rules accordingly.

### *Roles and Responsibilities*

In the absence of clearly articulated government rules, it is unclear who should be the ultimate arbiter of what content is illegal and must be removed. Per the precedent established by the Supreme Court of India in *Shreya Singhal vs. Union of India*, content removal requests cannot be made arbitrarily, and an intermediary would be liable to remove content only after receiving "actual knowledge" from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed. For content falling under the scope of Section 69a, all requests are shared with intermediaries 48 hours in advance. A meeting is then convened with the requesting agency, intermediary/website owner, and a committee of five senior government officials, including the Department of Legal Affairs and the Director General for Cyberlaw. Moreover, requests can only be made by certain government agencies, and the intermediary is not necessarily bound to abide by the request.

However, the Draft Amendments allow "the Government or its agency" to issue removal orders that must be processed within 24 hours. Intermediaries can and do take content down for violating their terms of service, but they are not positioned to interpret and adjudicate Indian law. This challenge is particularly acute with respect to, for example, extremist speech, which is not easily defined. The role of the intermediary, and whether they should be responsible for making this type of judgement, is a key issue. If intermediaries are held responsible for such determinations, they are likely to err on the side of removal in order to avoid liability, and this could result in significant restrictions, including on protected speech. In addition, intermediaries may face subtle pressures to curb freedom of expression to avoid government intervention, thereby further obscuring their process from public scrutiny. Should intermediaries act as censors when their mission is to provide a platform for free expression, and debate among users with diverse perspectives?

### *Traceability*

While the Indian government has a commitment to free expression and human rights, it also has a responsibility to ensure that free speech given by the Constitution is not abused. Intermediary liability was initially debated in 2011, because of the spread of fake news and rise in mob violence. Similarly, privacy is not sacrosanct in all situations, particularly when national security is at risk. The traceability provision is designed to address these security concerns, and apparently will only be invoked in exceptional cases. The government is also obligated to share evidence.

Despite this, many concerns remain around the legality and legitimacy of the traceability requirement. As one participant noted, "If a law enforcement agency seeks to violate someone's privacy via traceability, is the individual deemed guilty until proven innocent?" Another participant explained that there is substantial jurisprudence examining the government's arguments about when and how "the misuse of freedoms" can legitimately justify restrictions of those freedoms.

The Supreme Court case, *Puttaswamy v. India (2017)* ruled that the right to privacy is protected as a fundamental constitutional right under Articles 14, 19, and 21 of the Constitution of India. Additionally, what is considered "objectionable" content and therefore sufficient grounds for breaking privacy is still unclear. Furthermore, while the Draft Amendments only envision tracing to be conducted upon government requests, the technical steps required by intermediaries to enable this functionality could substantially weaken the privacy, data protection, and cybersecurity of their users  While the spread of fake news and criminal activity are legitimate concerns, there needs to be more clarity as to how the judicial process and provisions of the legal framework will ensure the protection of fundamental rights.

### *Website Blocking*

The lack of clarity around website blocking has also drawn public scrutiny. Section 69A of the IT Act empowers the government to order that access to certain websites can be blocked. The constitutionality of the procedure under 69A was upheld by the Supreme Court in *Shreya Singhal vs. Union of India*, but this legal precedent for website blocking is still a subject of debate. While remedies under Article 226 permit persons to file writ petitions in state high courts, in practice, critics argue that the website blocking orders and reasons for them are shrouded in secrecy, such that gathering the necessary information to successfully challenge such orders is nearly impossible.

The government has tried to provide sufficient clarity and guidance on website blocking orders. In an interactive process, MeitY will reach out to the website owner, unless the details are not clear or the organization is already banned. It will only block the website under review after discussion with the intermediary and approval by the inter-ministerial Committee for Examination of the Request (for more on the process for handling website blocking requests, see here). The same Committee can and has also ordered the unblocking of some previously blocked sites. MeitY will also disclose when it has blocked a website. However, officials also contend that it is not in the public interest to publicize every blocking order, particularly content that could cause unrest, such as fake news or extremist content.

## Necessity and proportionality

***Agenda Prompt:*** *The proportionality test has come up in the context of the draft rules vis-à-vis automated filtering and the timing for notice and takedowns. Several studies have shown the limits of AI*

*filtering, and how these tools can be a boon to smaller companies with fewer resources. As for timing, companies are given 24 hours notice for content takedown requests, and 72 hours for traceability. Another issue concerns the "fair use" in the copyright context. Are these provisions proportional to the government's aims?*

Where automated content moderation is not technically feasible, companies are seeking out other methods, including identifying content that spreads quickly and subsequently flagging for further review.

The government understands that complete elimination of harmful content is not possible, but sees the use of automated tools favorably, given the scope of content on relevant platforms. The government claims that it intends to prioritize proportionality in practice, and will only impose restrictions in exceptional cases, especially as they apply to large social media companies. The Supreme Court in the case of *Kamlesh Vaswani v. Union of India* [W.P. (Civil) No. 177 of 2013] had directed the Union of India to take positive steps to tackle the issue of CSAM.

On the issue of the timeframe for notice and takedown requests, it was articulated that in certain cases, the government may not want to wait for judicial review. For instance, if content violating a user's privacy or showing violence goes viral, the government may need to act quickly to mitigate harm. While acknowledging there may be some leeway to adjust the time in which companies must comply with takedown requests, the government seems to consider 72 hours a reasonable amount of time for social media companies to provide more information upon request, especially with the consideration that content can go viral quickly. However, as noted in the GNI submission to MeitY on the proposed rules, "most large platforms already act expeditiously in response to clear orders appropriately issued from duly empowered government authorities. There are nevertheless instances when such orders may be incomplete, issued inappropriately, or are overly broad. It is important that companies are allowed to review orders and seek clarity, where appropriate, in order to avoid unnecessarily impacting user rights."

## Privacy

***Agenda Prompt:*** *There is a growing consensus that encryption has benefits for security and anonymity, but less so about how traceability and encryption are related. Does traceability require encryption to be broken? Procedurally, how are requests administered? What steps do governments and companies need to comply with?*

Intermediaries have articulated various views on the traceability provision, which most clearly impacts providers who offer end-to-end encryption and do not have access to the information that would be necessary to carry out tracing as contemplated in the Draft Amendments. One perspective is that it is imperative to stand up for encryption in India, even where that may make certain government priorities more difficult to realize. This position argues that, without strong

encryption, India will put itself at the mercy of actors who wish to disrupt India's growing digital economy. Hostile actors will be able to access sensitive communications and spoil private messaging. Creating back doors can be very harmful, and will set India back in the long term.

With respect to procedural steps, transparency and accountability measures are also essential in support of privacy rights. There need to be standards for transparency reports, particularly around content moderation and notice and takedown measures, so that users have a clear sense of what is happening to their data and content. An oversight board grounded in human rights is another possible measure. Governments should also have a better understanding of transparency reports, and how they function across various company types and sizes.

Civil society is most alarmed by how a lack of transparency can lead to politically-motivated censorship. 'Risk' as a justification for breaking privacy and other rights is a slippery slope, and can be misused down the line. Moreover, how the government chooses to regulate illegal, and therefore punishable, speech online will also shape companies' privacy practices (i.e. a company may feel compelled to trace messaging in order to detect and remove illegal speech, figuring the costs outweigh the benefits). Without the proper legal safeguards, transparency and accountability mechanisms will be insufficient.

## Closing Remarks

Stakeholders' understanding of the Draft Amendments has changed significantly since 2018, and several entities have provided input and impacted the conversation.It is clear that candid engagement with the government is important. Across the world, governments are pushing for various requirements and opportunities to participate in those deliberations in an informed way are key.

There is no one-size fits all solution, but technical feasibility needs to be clarified and articulated in India and globally. There needs to be greater transparency and accountability, and freedom of expression remains a critical element. This applies to governments as much as it does to companies.

GNI and the India IMSC were extremely appreciative of all the views expressed and for the constructive and proactive tenor of the conversation. This roundtable should serve as a reminder that opportunities for further engagement remain available. And, as long as that window has not closed, we encourage all stakeholders to continue these important discussions.

## About the Global Network Initiative

The Global Network Initiative (GNI) was launched in 2008. Our mission is to protect and advance freedom of expression and privacy rights in the information and communications technology (ICT) sector by setting a global standard for responsible decision making and serving as a multistakeholder voice in the face of government restrictions and demands. GNI members include ICT companies, civil society organizations (including human rights and press freedom groups), academics, academic institutions, and investors from around the world. For more information, please visit our website: www.globalnetworkinitiative.org.

## About the Indian Internet Multistakeholder Coalition

The Indian Internet Multistakeholder Coalition (India IMSC) is a coalition of various stakeholder groups and it has been formulated with the idea that there needs to be a collective consisting of technology business, civil society, academia, and investors, for defending freedom of speech and privacy in the digital world and ensuring safety and security in digital technologies.

## Appendix 1: Recommended Reading

How India is using its Information Technology Act to arbitrarily take down online content (Torsha Sakar and Gurshabad Grover, Feb. 2020)

The Future of Intermediary Liability in India (SFLC.in, Jan. 2020)

Wikimedia Foundation expresses deep concerns about India's proposed intermediary liability rules (TechCrunch, Dec. 2019)

Intermediary Liability 2.0: A Shifting Paradigm (SLFC.in, March 2019)

Submission to MeitY on the Draft Amendments to the Intermediary Guidelines (GNI, Jan. 2019)

Response to the Draft of The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 (The Centre for Internet and Society, Jan. 2019)

But what about Section 69A? (Apar Gupta, 2015)

## Appendix 2: Participants

Aditi Agrawal, Medianama
Aditi Chaturvedi, KoanAdvisory
Alex Warofka, Facebook
Aman Taneja, Ikiglaw
Amrita Choudhury, CCAOI
Apar Gupta, IFF
Apurva, SFLC.in
Arjun Jayakumar, ORF
Berges Malu, ShareChat
Devdutta Mukhopadhyay, IFF
Dr. Amitayu Sengupta, IAMAI
Faisal Farooqui, Mouthshut.com
Faiza Rahman, NIPFP
Government Representative
Gurshabad Grover, The Centre for Internet and Society
Jan Gerlach, The Wikimedia Foundation
Jyoti Panday, Internet Governance Project, Researcher
Kushagra Sinha, SFLC.in
Mamta Verma, SFLC.in
Mishi Choudhary, SFLC, New York, (Founder SFLC.in)
Prasanth Sugathan, SFLC.in
Radhika Jhalani, SFLC.in
Rajeev Gowda, Member of Parliament, Indian National Congress
S. Verma, Ford Foundation
Sarvjeet Singh, CCG
S. Chandrasekhar, Microsoft
Shaurya Aron
Shruti Grover
Smitha Prasad, CCG
Snehashish Ghosh, Facebook
Tanya Sadana, Ikiglaw
Udbhav Tiwari, Mozilla
Usha Ramanathan
Uthara Ganesh, Amazon
Vikram KB, Amazon