Submission of Comments on MEITY's draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018

Digital Empowerment Foundation

Shri Ajay Prakash Sawhney,
Secretary, Ministry of Electronics and Information Technology,
Government of India,
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi - 110003
secretary@meity.gov.in

Subject: Submission of comments/ suggestions on the draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018

Dear Sir,

The Digital Empowerment Foundation (DEF) wishes to thank the Hon'ble Ministry for the opportunity to submit our comments on the draft Information Technology [Intermediary Guidelines Digital Empowerment Foundation is a New Delhi-based not-for-profit organisation. It was born out of the deep understanding that marginalised communities living in socio-economic backwardness and information poverty can be empowered to improve their lives almost on their own, simply by providing them access to information and knowledge using digital tools.

We recognise unhindered and universal access to the internet as a key driver of development and empowerment amongst the digital excluded masses in India. We are grateful that the MEITY has sought greater clarity on the discriminatory tariff regulations and has approached the concept of providing free data to all.

My colleague, Ms. Anulekha Nandi, who has drafted our response, and DEF are happy to provide any further support to MEITY.

Yours sincerely,

Osama Manzar
Founder and Director
Digital Empowerment Foundation
House 44, 3rd Floor, Kalu Sarai, New Delhi - 110017
Website: www.defindia.org

General Comment:

According to the invitation for the comments/suggestion on the draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 the proposed amendments are aimed at strengthening the legal framework to make social media platforms more accountable under the law in response to a calling to attention motion on 'misuse of social media platforms and spread of fake news'. DEF recognises the vital need to curb the misuse of social media to curb the spread of misinformation and disinformation channelised towards the incitement to violence in various parts of India. However, the intermediary guidelines have a broad mandate which cater to a wide range of intermediaries working in the digital space and not just to social media companies whose platforms are used for the distribution and propagation of misinformation and disinformation. As a result of this, it is important to carefully evaluate the causal, incidental, and eventual relationship between the objective and intent, the strategy, and the potential unintended consequences and knock on effects on current civic and economic practices in the digital space. Due to DEF's presence on the ground working with communities towards reducing information poverty and improving social and economic equity in underserved areas by enabling access to information and communication technologies for development, it recognises that the reception and virality behind the spread of rumours that has led to violent action in different parts of India is underpinned by a complex web of social dynamics. Therefore, increasing the conditions under safe harbour requirements for intermediaries in themselves would not be enough to address the issue in terms of its causal and enabling factors since there needs to sustained effort in engaging with the root causes of the problem. This has been one of the learnings from the misinformation sensitisation workshops conducted by DEF with support from local district administrators and law enforcement across 11 states in India.

Intermediaries provide infrastructure or service which is used by end-users as per their own communication requirements. Safe harbour provision exists to provide conditional immunity from liability for third-party content and exemption from general requirement to monitor content. This arrangement is indispensable for protecting constitutionally guaranteed fundamental rights so as not to delegate law enforcement functions of taking evaluative decisions restricting citizens' activities to private actors. With the proposed amendments, India is inching closer towards a stricter liability regimes by expanding the conditional requirements needed to qualify for safe harbour. A stricter liability regime that imposes greater obligations on intermediaries and proactive censorship requirements onto them undermines the expanded democratic potential and agency that digital media had afforded an ordinary individual. Moreover, definitional issues around terms such as "grossly offensive or menacing in nature"; "threatens public order"; "threatens public health or safety" should be resolved to avoid vagueness and achieve clarity. In order to ensure that ultimate objectives of aiding law enforcement to respond to the sensitive situations efficiently at a given time do not result in collateral damage and false positives, it is important to have clearly defined due process and safeguards in place with judicial oversight that lend transparency and accountability and ensure that only unlawful content, determined by a court of law, is restricted through intervention based on actual knowledge.

This general comment is followed by a discussion on the specific points of the proposed amendments such a traceability, automation and proactive monitoring, and the need for harmonisation with international standards and practices.

Specific Comments:

Traceability: Contention, contradiction, and evidence from the ground

Context: The past couple of years have seen an alarming rise in cases of lynchings and mob violence resulting out of rumours and misinformation spread via social media platforms like WhatsApp. The anonymity and the potential for virality afforded by social media obfuscate the detection of the actual perpetrator of the message. In a given locality gripped by violence-mongering rumours, traceability is understandably a prime law enforcement concern. Rule 3(5) of the proposed amendments aims to cater to this purpose. However, the said Rule contains a number of contradictions and could be interpreted to be sufficiently overbroad so as lead to its potential misuse. The Rule mentions a timeframe of 72 hours within which intermediaries would need to provide 'information or assistance' when *required by lawful order* by any government agencies *who are legally authorised*. However, this Rule does not mention the agencies and the rank of officials who would be legally authorised to issue lawful order mandating information and assistance from intermediaries. Clear delineation of due process is essential to foster accountability and transparency. While sensitive situations like lynching and mob violence demand expediency, it also calls for compliance with due process. Licensing agreements under The Indian Telegraph Act, 1885 for Internet Service Providers (ISPs) who can be classified as access providers already require ISPs to put systems in place that enable lawful monitoring and interception of communication by the Indian Government and they are also required to monitor content that communications that can be objectionable, obnoxious, malicious, or a nuisance. This is apart from their required compliance with provisions for data retention, disclosure, and provision of services towards aiding lawful monitoring and interception by government. Apart from this the license holders are also obligated to block Internet sites, URLs (Uniform Resource Locators), and/ or individual subscribers as identified and directed by the Licensor from time to time. Further, the Gazette notification of 20 December 2018 under s. 69(1) of the Information Technology Act, 2000 authorising 10 police and intelligence agencies to "intercept, monitor, and decrypt" all information on any computer resource in the country.

Analysis: The above concurrent developments and pre-existing regulations highlight an enmeshing of regulatory regimes that seem to work at cross-purposes and to the detriment of the users' fundamental freedoms and civil liberties. This is due to the lack of clarity on the grounds of balancing fundamental freedoms and public order and safety. Both the stated objective and the intent of amendments to the existing intermediary liability regimes stems from the need to regulate the proliferation of viral misinformation on the social media platforms. However, the proposed amendments will cover all types of intermediaries within its purview like payment gateways, advertisers, search engines and even access providers like ISPs who are already regulated under a licensing regime with its given set of compliances. In the absence of a surveillance law, the lack of clearly specified guidelines and procedures widen the ambit for abuse since the purposes for which information can be requested can range from security of the State to detection, prevention, and prosecution of crime and cyber security and matter connected or *incidental* thereto. The wide scope and ambit of Rule 3(5) without clear legally established tests or safeguards, and grievance redressal mechanisms in tandem with Gazette notification of 20 December 2018 mentioned above highlight the need for the much needed legal framework for state surveillance to ensure such powers are used for *bona fide* purposes only with clearly defined security safeguards and obligations on state agencies with the need for an effective review mechanism and judicial oversight as mentioned in the Srikrishna Committee Report.

Recommendations: Define parameters to classify services provided by intermediaries rather than intermediaries themselves. As a result of the transmutable nature of the internet a particular intermediary may provide a number of different services. For example, Facebook is a social media platform that also sells advertising space. Once parameters of service have been so defined, regulations should be tailored with respect to that particular category keeping in mind already pre-existing sectoral regulations. Further, any demands made on intermediaries should follow clearly defined guidelines of due process along with obligations on state agencies for which it is important for the government to delineate the legally authorised agencies and rank of officers along with a process that allows for review of decisions taken. Ultimately, it is important to mandate judicial oversight for state intervention because courts are the best placed to judge the lawful/ unlawful nature of a content and necessity and proportionality of a proposed intervention. Apart from legal and regulatory frameworks to respond to societal challenges posed by viral misinformation, it also important to build individual and institutional capacity for resilience. DEF has been working on the ground with communities and local administration and law enforcement around the country by conducting workshops on misinformation and disinformation in partnership with WhatsApp. Conducted with the support of the District Collector's office and Superintendent of Police, 4500 stakeholders at the local and community-level have been trained between September 2018 and January 2019 across 11 states in India including police officers, local administrative officers, teachers, NGO representatives, local entrepreneurs, students, and self-help groups. While conducting the workshops DEF came to know of existing local efforts already being undertaken by local administration and law enforcement. For example, the Police Department of Seoni, Madhya Pradesh regularly organises workshops for their personnel to understand cyber-crimes better. During one of the workshops, teachers in Palghar, Maharashtra who confessed to sharing misinformation are educating other teachers, students, and local community members. Law students in Jaipur, Rajasthan pledged to become agents of change and reach out to people voluntarily in order to spread awareness about misinformation and disinformation. Pre – and post – assessment of the workshops revealed that the percentage of respondents who hardly verified their WhatsApp forwards fell sharply by 10.4% and the percentage of respondents who are most likely to verify their information increased by 20.9%.

Automation and the delegation of enforcement

Context: Rule 3(9) of the proposed amendments state that "(t)he Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content". According to the Supreme Court judgement in the case of Shreya Singhal v Union of India [(2015) 5 SCC 1], an intermediary's proactive intervention is absent in s. 69A of the Information Technology Act, 2000 read with the Information Technology (Procedures and Safeguards for for Blocking for Access of Information for Public) Rules, 2009. A blocking order can only be passed by a Designated Officer after complying with 2009 rules or by a Designated Officer following a Court Order.

Analysis: Automated tools require large amounts of data to train. Bias in the data, historical or otherwise, as well as human bias creeps into the analysed outcome. Determination of what constitutes lawful and unlawful, especially in matters as nuanced, complex, and critical as those affecting fundamental rights such as freedom of expression and association online, cannot be authoritatively decided anywhere but in a court of law. Therefore, deploying such technologies to determine what is unlawful information or content becomes an exercise in building a pervasive system of myriad discriminations and prejudices that can have chilling effect on the democratic potential of the online space. While instances of child pornography, nudity, and sexual abuse are easy to detect and remove, instances of political speech are not. Moreover, delegating enforcement of online information and content to automated technologies and by translation private entities are incompatible with international standards of practice. Automated technologies have an endemic 'black-boxing' problem

where it is virtually impossible to trace the source and cause of a decision taken which undermine an aggrieved party's right to a due process. Furthermore, asking private entities to deploy such technologies to proactively identify and remove public access to unlawful information or content is tantamount to delegation of law enforcement to private actors. Private entities cannot be the arbiters of what constitutes lawful; this falls under the purview of the judicial system. Moreover, at the threat of losing safe harbour provisions, private entities would tend to err on the side of caution resulting in serious negative impacts on an individual's freedom of expression and association online. Further, proactive intervention of intermediaries in altering the status of the information or content they are hosting without actual knowledge might go against the very definition of qualifying as an intermediary and especially even more so as per the Supreme Court judgement issued in the case of Shreya Singhal v The Union of India [(2015) 5 SCC 1]. According to the latter, an intermediary can only remove content (a) upon receipt of court order that has found a particular content to be illegal within the course of court proceedings and (b) upon notification from an authorised government agency.

Recommendation: Rule 3(9) should be removed in its entirety because of implicit bias and black boxing inherent in automated decision-making, the lack of legal basis for delegation of law enforcement to private entities, and the lack of legal basis for proactive policing by intermediaries.

Harmonisation with international standards

Context: India's intermediary liability regime provides safe harbour protection for intermediaries which are conditional upon the fulfilment of certain obligations. This is distinguished from two other models: (a) broad protections and (b) strict liability regime. The former protects intermediaries from a wide range of third party content except in the cases of criminal activity or clearly defined categories of law. The latter holds intermediaries completely liable for third party content and require active monitoring and intervention by intermediaries. India's regime so far has been in-between these two extremes and closely reflecting The European Union E-Commerce Directive and US Digital Millennium Copyright Act. The argument against cumbersome intermediary liability regimes stems from concerns about 'collateral censorship', thereby undermining the expanded democratic space offered by digital media. As per the 2011 Joint Declaration on Freedom of Expression, 'liability should only be incurred if the intermediary has specifically intervened in content, which is published online'. It further states that 'ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and take-down'. Similarly in 2011, the Special Rapporteur on Freedom of Expression criticised States' attempts to force intermediaries to undertake censorship on their behalf and that intermediaries should only implement restrictions on users' fundamental rights and civil liberties upon judicial intervention. He further recommended transparent procedures to be adopted by intermediaries when required to take restrictive measures and keep the focus of such measure restricted to the specific content in question. The notice and take-down approach that is characteristic of conditional intermediary liability regimes like that of India have been criticised on the basis if lacking a clear legal basis. This is a result of unclear and complex notice and take-down provisions and their inherent arbitrary nature since they do not go through an independent judicial determination process on the (un)lawful nature of a given content. This is further exacerbated by a lack of due process available for appeals by the affected parties.

Analysis: Rule 3(9) of the proposed amendments have moved India closer to the stricter end of the spectrum by demanding proactive censorship. This in effect delegates the censorship to automated decision-making to be deployed by private entities, thereby holding serious implications for implicit bias, discrimination, and chilling effect. Rule 3(5) continues the trend of notice and take-down regime without any provision for judicial oversight. Moreover, the lack of differentiation between services provided by different intermediaries, there is a resultant entangling of sectoral regulatory regimes and

policy priorities with the proposed amendments thereby resulting in complex compliance processes for intermediaries who would then implement the highest restriction available in order to retain their safe harbour protection leading to an adverse effect on civic and democratic participation online.

Recommendations: In order to develop a progressive legal and regulatory regime that can balance justice, fairness, equity, and security in extending both liberty and security to its citizens India must work towards harmonising and emulating international standards and best practices. This would entail establishing clear guidelines, obligations, and due process on authorities in order to facilitate transparency and accountability towards fulfilling both expediencies of law enforcement as well as safeguarding long cherish constitutionally protected individual rights and liberties. Apart from establishing clear legal and regulatory frameworks like clarifying authorised government agencies, rank of authorising officers, and creating provisions for judicial oversight it is also important to work towards building capacity at the local administration and law enforcement level to respond to newer social exigencies created by proliferating technological penetration and the newer challenges thrown up by them. It important that any restriction sought to be placed by intermediaries on third-party content is based on narrowly defined legal tests and principles.