Shri Ravi Shankar Prasad
Ministry of Electronics and Information Technology
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi: 110003

March 30, 2021

Dear Sir,

As the world's most populous democracy and a global leader in technology innovation, India is well positioned to demonstrate to the world how legitimate concerns about illegal content and conduct online can be addressed in a manner consistent with internationally recognized rule of law and human rights principles. Unfortunately, the recently notified Indian Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("the Rules") represent a missed opportunity for such leadership.

Given the lack of any formal response to the January 2019 consultation on an earlier set of proposed amendments to the Intermediary Guidelines, which the Global Network Initiative (GNI) and others took part in, the lack of any published timeline for further consideration, and the extensive changes between the Rules and the draft amendments, the notification of these Rules by the Ministry of Electronics and Information Technology ("the Ministry") last month took many of our members by surprise. The lack of effective consultation and parliamentary deliberation on these Rules stand in tension with the human rights principle of legality and our derivative recommendation that "when states consider particular forms of online content sufficiently harmful so as to require regulation, they should be deliberated upon openly and defined through legislation, consistent with domestic law."

Since submitting our input on the draft amendments, GNI has continued to engage with digital rights groups, industry, and government officials in India on this topic, including through a multistakeholder, virtual consultation on content regulation in June 2020, which focused heavily on the draft amendments. Our analysis of that earlier draft and other relevant proposals, together with the inputs from this and additional consultations, fed into our recent

policy brief on rights-respecting responses to digital harms: Content Regulation and Human Rights: Analysis and Recommendations ("Policy Brief"). It is with this context in mind, that we write to provide our high-level analysis of the Rules (attached), in the hopes that it will help inform related government policy and enforcement decisions going forward to ensure the Rules are necessary and proportionate to the government's stated, legitimate objectives.

We recognize the importance of addressing abuses of digital communications tools and appreciates the emphasis on transparency and opportunities for redress around content decisions in the Rules. However, a number of the concerns GNI and other stakeholders have consistently raised remain unaddressed or have been exacerbated. Included among these are: the extensive range of companies and content covered by the Rules; the lack of definitional clarity around key terms and expectations; disproportionate access to user data, including provisions that may undermine encryption; and overbroad enforcement authorities. Each of these concerns on its own can negatively impact freedom of expression and privacy in India; together, they create significant risk of undermining digital rights and trust in India's regulatory approach to the digital ecosystem.

We call on the Ministry to consider revising the rules and engage in an open, deliberative process about how to address and mitigate these concerns. We stand ready to support content regulations in India that will be effective in addressing the legitimate concerns around online harms, while respecting the human rights principles of legality, legitimacy, and necessity and proportionality that India is committed to upholding.

Sincerely,

Judith Lichtenberg

Judith Lichtenberg
Executive Director
Global Network Initiative

Global Network Initiative Analysis of the Indian Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

I. Overbroad Application

In the Policy Brief, which analyzed over 20 proposed or recently-enacted content regulations from around the world, we emphasize the need for laws to be "tailored, effective, and fit for purpose." However, the Rules include due diligence requirements that are uniformly applicable to a wide range of intermediaries, as defined in section two of the IT Act, which would appear to include email providers, Internet service providers, web hosts, content delivery networks, social media platforms, and possibly others, without appearing to take account of the significant differences in position, resources, and capabilities among these covered services. While we appreciate that the Rules do introduce some differentiation for "Significant Social Media Intermediaries" (SSMIs), we note that Rule 6 creates an unchecked, unilateral power for the Ministry to apply that label to any intermediary, regardless of its size or the services it provides. In addition to extending potentially burdensome compliance obligations to intermediaries, including small and non-profit services who may have very little impact on or ability to remediate the harms that the Rules seek to address, this overly broad approach is likely to lead to over-enforcement by intermediaries, which would in turn create chilling effects for individuals.

The Rules also establish two new categories of "publishers of news and current affairs content" and "publishers of online curated content," subjecting them to an entirely new digital code of ethics and corresponding due diligence requirements. This decision to significantly expand the scope of application of the Rules beyond intermediaries was not deliberated by parliament and does not appear to be justifiable under the parent IT Act. Furthermore, the lack of definitional clarity around these categories make it appear as if Part III of the Rules could apply to domestic and international news outlets, subscription newsletters, and citizen journalists alike, regardless of their size. The term "other such content" in the definition of "online curated content" in Rule 2(1)(q) seems to open the possibility of enforcement against a wide range of "audio-visual"

services, while the definition of “publisher of news and current affairs content” in Rule 2(1)(t) creates an uneven and unjustified playing field for online publishers vis-à-vis “newspapers” and their electronic copies. By contrast, as we set out in the Policy Brief, our experience indicates that international human rights law counsels toward the provision of specific carve-outs and safeguards for independent journalists and smaller media outlets, which form an important part of the health of any media ecosystem.

II. Lack of Definitional Clarity

Definitional uncertainties also appear in the aforementioned due diligence requirements in Part II of the Rules, which require intermediaries to prohibit certain types of information in their respective content rules, regulations, and policies. In our previous submission, we flagged how similar provisions potentially authorized restrictions exceeding those outlined under section 19(2) of the Indian Constitution. Vague new clauses in Rule 3(1)(b) calling broadly for the prohibition of content "harmful to a child," "information which is patently false or misleading," or “impersonat[ing] any other person,” reinforce these concerns. They also run counter to the landmark ruling in *Shreya Singhal vs. Union of India*, in which the Supreme Court struck down broad requirements for intermediaries to remove vaguely-defined categories of content in Section 66A of the IT Act, and clarified that orders to remove content must be transparent and “only come from a reasoned order from a judicial, administrative, or government body.”

It is one thing to trust interpretation and enforcement of such terms to independent judges, but another altogether to expect intermediaries to apply them in a nuanced, objective manner when the consequences of any perceived “non-observance” could result in a loss of protections from legal liability (safe harbor). Instead, as we note in the Policy Brief, the use of “vague and reductive definitions that would be very difficult to enforce in a manner perceived as fair and non-discriminatory,” is likely to result in over-removal of content, user self-censorship, and a degradation of trust among users and across services.

III. Due Diligence Requirements

In the Policy Brief, we emphasize how transparency around content decisions can help mitigate the risks of over-removal and self-censorship, and praise laws providing effective standards for due process and remedy around such decisions. We appreciate the government's effort to meet some of these goals through the required grievance mechanism set forth in Rule 3(3), and further transparency and redress requirements for SSMIs in Rule 4. However, we worry that, as currently prescribed, the onerous nature of the requirements may outweigh the potential for public understanding of such decisions and related access to remedy. These requirements may prove particularly challenging for smaller companies and not-for-profit intermediaries to implement.

Specifically, as we noted in our previous statement and in the Policy Brief, short and inflexible timelines limit companies' ability to review both government demands and user complaints in appropriate, circumstance-specific manners. Under the rules, *all* intermediaries are expected to establish a "grievance office" under rule (3)(2)(a), comply with *all* removal orders under rule 3(1)(d) within 36 hours, implement *all* requests for access to user data under rule 3(1)(j) within 72 hours, and resolve *all* complaints under Rule 3(2) within 15 days (within 24 hours for any complaints related to non-consensual sexual imagery). While decisions about content that present particular risk deserve to be addressed quickly, mandating short timelines for *all* content decisions can actually defeat that goal and will almost certainly lead some intermediaries to adopt a "remove first, ask questions later" approach.

IV. Government Demands

The new Rules grant a broad range of government authorities the ability to issue orders to restrict content or be provided access to user data. These provisions are particularly troubling given the lack of related oversight and accountability provisions, broad enforcement powers, and significant potential penalties.

Rule 3(1)(d) authorizes the "appropriate government or its agency" to order intermediaries to remove content prohibited by laws related to the potential reasonable restrictions on expression set out in Article 19(2) of the constitution, while rules 15 and 16, which are applicable to both intermediaries and publishers, also grant the Ministry of Information and Broadcasting authority to issue removal orders, including emergency orders requiring immediate response – a new power that is not warranted or justifiable under the parent act. Rule 3(1)(J), covering orders for intermediaries to "provide information under its control or possession" is also overly broad, stating that assistance must be granted to "any government agency which is lawfully authorized for investigative or protective or cyber security activities," provided there is a written order clearly stating the purpose.

V. Traceability Requirements

As with the previous draft, the rules continue to require SSMIs offering messaging services to be able to trace the identity of originators of content in response to a court order or government demand under section 69 of the IT Act. While this requirement is restricted to SSMIs, as others have pointed out, the Rules are not clear on who qualifies as a messaging service. In general, as we have pointed out in the Policy Brief and our previous submission, such traceability requirements can create significant risks for privacy and data protection. While certain limitations on the use of this authority (i.e., only in response to certain serious offences, "in cases where other less intrusive means are effective in identifying information," and limited to "first originators") may be well intentioned, they do not sufficiently mitigate the disproportionate technical, human rights, and economic impacts of this requirement.

While the government has stated it does not intend to break encryption, industry and independent technical experts alike have expressed skepticism that it would be feasible to comply with the Rules as written while maintaining strong end-to-end encryption. End-to-end encryption ensures that only the sender and recipient of a message can decipher its contents. Exceptional access to message content, meaning a mechanism by which the company can decipher messages traveling between two parties, would likely be necessary to ensure message

traceability. This would dramatically weaken the security of those communications, putting all users of such a service at risk of surveillance by other governments and malign non-governmental actors.

Even putting aside the impact on encryption, compliance with this rule would require SSMIs to make significant adjustments to their services and establish systems to capture and maintain all records of users' communications, including the location of users at the time of each message sent, significantly increasing the risk of privacy infringements, data breaches, leaks, hacks, and other compromises. These steps would undermine the commitments to free and secure communications that underpin human rights commitments, data protection principles, and cybersecurity best practices. These concerns are also raised by the vague language in Rule 3(1)(k) prohibiting intermediaries from "knowingly" deploying or modifying the technical configuration of their systems which "may change or has the potential to change the normal course of operation of the computer resource that what it is supposed to perform thereby circumventing any law."

These considerations are underscored by concerns some have expressed about how orders are authorized and enforced under section 69 of the IT Act, given excessive secrecy and limited procedural safeguards. Under rule 4(2), orders to trace originators can not only be issued for the investigation or prosecution of serious offences, but also for prevention or detection of them.

In addition to these privacy and data protection risks, limits to anonymity can also chill users' freedom of expression. And the pressures on anonymous communication are heightened by the account verification mechanism all SSMIs are expected to enact under rule 4(7), which, while currently voluntary for users to adopt, comes in the context of recent legal battles over efforts to link Indians' digital government identification to their social media accounts.

VI. Enforcement

In our Policy Brief, we note the importance of proportionate enforcement, calling on policy makers to "refrain from overly stringent enforcement and penalties" in order to comply with the principles of necessity and proportionality. Rule 7 states that companies can lose their safe harbor protections for user-generated content under section 79 of the IT Act for "failure to observe" any element of the rules, posing a significant risk of litigation for the full range of intermediaries in scope, and adding to penalties that already exist for failing to comply with orders to access data or restrict content.

SSMIs are further required to designate three different responsible company employees, all of which need to reside in India — the grievance officer (as discussed above), a nodal contact person for 24x7 law enforcement coordination, and a Chief Compliance Officer. The Chief Compliance Officer must be key managerial personnel from the company, and can be held personally liable for any company failure to meet the due diligence requirements prescribed by the law. Based upon penalties outlined in section 69 and 69A of the IT Act, this could include prison terms up to seven years, as well as significant fines.

While the desire for clear and responsive reporting lines between relevant authorities and intermediaries is legitimate, the ability to subject individual employees to personal, criminal liability is completely unnecessary, unjustified, and likely to further undermine intermediaries' trust in the government's intentions, and user trust in intermediaries' ability to stand up for their rights. This can put SSMIs in an impossible position when the law of the country where they are based prohibits a disclosure to a governmental entity in India, but complying with that prohibition subjects an on-the-ground employee to a substantial prison term. At a time when many non-democratic governments are introducing "hostage taking" language into their content regulations, this provision creates a troubling precedent that will undermine efforts, including by the Indian government, to argue against such provisions.

These broad penalties and enforcement authorities, when taken in combination with substantial expectations for intermediaries to prohibit and aggressively police vaguely defined forms of content, engineer access to data, and fulfill onerous due diligence requirements, will pose substantial burdens on intermediaries of all sizes and across the technology stack. They are also likely to incentivize excessive removals and undermine data protection. The substantially broadened scope of the rules, now covering "publishers of news and current affairs content" and "publishers of online curated content," reaffirms these concerns and poses particular risks for press freedom and a diverse media ecosystem in India.