The Bangladesh Telecommunication Regulatory Commission
IEB Bhaban (5,6 & 7 floor)
Ramna, Dhaka-1000

Dear BTRC Colleagues,

The Global Network Initiative (GNI) appreciates the opportunity to provide input in response to the public consultation on the Regulation for Digital, Social Media, and OTT Platforms, 2021, ("draft regulation") from the Bangladesh Telecommunication Regulatory Commission (BTRC).

GNI is well positioned to comment on regulation of information and communications technology (ICT) companies as the preeminent, international multistakeholder organization working in support of freedom of expression and privacy in the ICT sector, bringing together academics, civil society, ICT companies, and investors from around the world. GNI has undertaken an initial review of the draft regulation, informed by the GNI policy brief, "Content Regulation and Human Rights," we launched in Fall 2020. This brief was the result of a series of multistakeholder consultations around the world, and examined over two dozen recent government initiatives that aim to address online harms. GNI evaluated these content regulation efforts according to the limited circumstances in which states may legitimately restrict freedom of expression, as set out in Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR). This framework consists of the three interrelated principles of legality, legitimacy, and necessity. Informed by this analysis, the brief identifies common pitfalls, as well as innovative approaches, and concludes with a series of recommendations.

We would like to start by acknowledging some of the BTRC's legitimate aims underpinning this effort, such as preserving the safety of individuals, cybersecurity, and the rights of members of marginalized groups. We also acknowledge the important role the government can play in

1325 G St. NW, Suite 500, Washington, D.C. 20005 • Globalnetworkinitiative.org
• info@GlobalNetworkInitiative.org

addressing illegal content, and we appreciate the BTRC's focus on providing greater opportunities for redress on content determinations. However, we are concerned by the very broad scope of the bill, from the companies and content it covers, to the significant, often-vaguely defined obligations and enforcement authorities, to potential "traceability" and data sharing provisions that may infringe on privacy rights. Such a regulatory environment undermines the otherwise positive aims of the draft regulation, failing to provide sufficient guidance to intermediaries tasked with implementing the law to "ascertain what sorts of expression are properly restricted and what sorts are not," in line with the principle of legality.[1] The proposal is likely to put undue pressures on intermediaries to remove content and share access to user data, and have chilling effects on individual speakers.

As litigation around this draft regulation has called for, we ultimately feel there is a need for further consultation with non-governmental stakeholders, and we call on the BTRC to step back and work with experts and affected stakeholders to revisit the current proposal. We also call for further clarity on how upcoming consultation and review will align with related regulatory efforts from the Ministry of Information and Broadcasting (MoIB). We have detailed our analysis of the bill below, and we stand ready to engage with the BTRC and the government more broadly to develop an approach that is effective in addressing the stated concerns, fit for purpose, and in line with relevant international obligations.

Process Concerns

We understand the BTRC has explored potential new content regulation in Bangladesh since at least January 2021, when the High Court Division first issued a directive calling for BTRC and MoIB to formulate regulations dealing with online content and over-the-top web-based platforms (OTT). When the BTRC shared its report to the Supreme Court via an affidavit in

[1] Human Rights Committee, General Comment No 34, CCPR/C/GC/34, 12 September 2011, paragraph 25

1325 G St. NW, Suite 500, Washington, D.C. 20005 • Globalnetworkinitiative.org
• info@GlobalNetworkInitiative.org

September 2021, the petitioner's submission called for further consultation and review from both government and non-governmental stakeholders, as well as opportunities for public hearings and roundtables. While the BTRC accepted this petition, it has failed thus far to meet this standard for consultation. We appreciate that BTRC has opened this window for public comment, but we are concerned by the lack of detail and clarity on desired areas of input and subsequent next steps for addressing the feedback BTRC receives.

As we note in the policy brief, careful, public, and participatory deliberation, allowing for diverse and expert inputs, based on empirical analysis, and accompanied by impact assessments, can go a long way in ensuring laws are tailored, effective, and fit for purpose, and less prone to potential errors. There are several areas of the draft regulation where we saw clauses that were incomplete, important terms left undefined, or areas transposed from India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, that seemingly failed to account for differences in the regulatory environment, adding to our concerns about the rushed deliberation processes. We encourage the BTRC and the government more broadly to reconsider its approach to consultation on this bill, helping to build an evidence base for the draft regulation to address the regulation's stated concerns in a rights-respecting fashion.

It is also essential that the government better clarify the authorities of the BTRC and MoIB regarding content regulation, as the MoIB has also recently issued draft OTT regulations. Without an official English-language translation, we understand the MoIB proposal details a set of similar obligations applicable to broadly defined "over-the-top (OTT) content-based service providers." These include requirements to register with MoIB, responsibilities for addressing certain forms of prohibited content, and potential loss of license or significant fines for failing to comply. However, Clauses 8 and 9 of the draft BTRC regulation also set out a "digital media code of ethics" overseen and enforced by the MoIB, covering "publishers of online curated

1325 G St. NW, Suite 500, Washington, D.C. 20005 • Globalnetworkinitiative.org
• info@GlobalNetworkInitiative.org

content" and "publishers of news and affairs content." Depending upon the interpretation of these definitions, they could also apply to ICT companies.

While MoIB has historically had oversight of the press and broadcast media, both the BTRC and MoIB regulations could create substantial new authorities for MoIB to restrict access to digital content and conduct. It is therefore critical to further clarify the relationship between the two proposals and the roles and expectations of different government authorities. Otherwise, the draft regulations risk introducing competing obligations and legal ambiguity, paired with significant liability risks for intermediaries of all sizes and business models who provide services in Bangladesh.

Broad Scope

In GNI's policy brief, we detail how laws and regulations targeting an overly broad range of ICT companies can fail to meet standards of necessity and proportionality, whereby any restrictions on freedom of expression "must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected."[2] It is important to recognize that companies such as Internet service providers, search engines, or web infrastructure companies are less well positioned than social media companies to address concerns about particular online content and conduct, and if subject to the same liability and legal requirements, may be forced to disable access to entire internet-based platforms, services, web pages, etc.

The opening clause of the regulation details an extremely broad scope, stating the regulation is applicable to any "internet service provider(s) providing (a)content, (b) a service, or (c) an application that is provided to the end-user over public Internet." The draft then defines

[2] Human Rights Committee, General Comment No 34, CCPR/C/GC/34, 12 September 2011, paragraph 5

1325 G St. NW, Suite 500, Washington, D.C. 20005 • Globalnetworkinitiative.org
• info@GlobalNetworkInitiative.org

intermediaries, who face extensive due diligence obligations, extremely broadly, so as to cover all services that "receiv[e], stor[e] or transmi[t] electroni[c] records" or "provide[] any service with respect to such records," and listing a broad set of examples, from telecommunications companies, to web hosts, to cyber cafes. We also emphasize a similarly broad definition of OTT service providers in the MoIB draft.

In addition, the regulation fails to distinguish at all between companies of different sizes. Clause 7, which adds additional obligations that may be specific to otherwise-undefined "social media intermediaries", features similar obligations to those that are specific to "significant" social media intermediaries in the IT rules in India. These types of requirements are likely to have significant implications for smaller and potentially local players in the digital ecosystem who lack sufficient resources for implementation. As we note in the policy brief, many other regulatory efforts have tailored company responsibilities to company size. Policymakers may also consider tailoring regulations to companies' reach and ability to address the specific concerns that they believe are not being sufficiently well addressed.

Sweeping Obligations for All Intermediaries

Clause 6.01 set out a sweeping range of content and conduct that intermediaries would be obliged to prohibit under their own "rules and regulations." These include prohibitions on information that is "insulting," "hurts religious values or sentiment," or "misleads the addressee as to the origin of the message." As we set out 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. Here, it is critical to note that, in line with the principle of legitimacy, the right to freedom of expression is broad in scope, encompassing

1325 G St. NW, Suite 500, Washington, D.C. 20005 • Globalnetworkinitiative.org
• info@GlobalNetworkInitiative.org

"even expression that may be regarded as deeply offensive."[3] Furthermore, prohibitions on content in digital form that is otherwise legal offline raises the risk of potential discriminatory impacts. These concerns are reaffirmed by intermediaries' responsibilities to address broadly defined categories of prohibited content in the draft MoIB regulation as well.

There is a lack of clarity in the proposed regulation about whether intermediaries benefit from immunity from liability for decisions to either leave up or take down content that is the subject of a complaint or notice, adding to the potential pressures to restrict legitimate expression. The final paragraph in Clause 6.01(d) comes close to articulating what might be understood as a "Good Samaritan" rule protecting intermediaries from liability for voluntarily removing content specified in the clause, but appears to be incomplete (at least in the English version of the draft regulation). Meanwhile, Clause 7.02(a) states that the appointed Compliance Officer or an intermediary can be held liable for "any relevant third party information, data or communication link made available or hosted by that intermediary where he fails to ensure due diligence while discharging its duties…" However, the draft regulation fails to define what "due diligence" means in this context, leaving intermediaries clueless as to how to protect themselves and their employees from such liability.

Furthermore, Clause 6.01(d) gives the BTRC (and potentially other "authorized agencies") unfettered and unilateral discretion to adjudicate and demand removal of content without any provisions requiring an explanation of the rationale for such a demand, review by an independent judicial authority, or opportunity for appeal. The requirement for such orders to be complied with in 72 hours or less only exacerbates concerns that intermediaries will not have sufficient time or discretion to properly evaluate and respond to complicated or overbroad demands. As we note in the Policy Brief, short and inflexible timelines limit

[3] Human Rights Committee, General Comment No 34, CCPR/C/GC/34, 12 September 2011, paragraph 11

1325 G St. NW, Suite 500, Washington, D.C. 20005 • Globalnetworkinitiative.org
• info@GlobalNetworkInitiative.org

companies' ability to review both government demands and user complaints in an appropriate, circumstance-specific manner.

Disproportionate Enforcement Authority

In the GNI policy brief, we call on authorities to "refrain from overly stringent enforcement and penalties" to help preserve companies' capacity to innovate around content moderation and guard against potential chilling effects that might emerge from excessively punitive approaches. Unfortunately, it appears that the draft regulation features excessive penalties for violations, including targeting company personnel. The regulation specifically refers to violations incurring penalties spelled out in section 66A and section 64 of the Bangladesh Telecommunication Regulation Act, 2001, which contemplate fines of up to BDT 3 billion (approximately US$ 35m) and/or imprisonment for up to 5 years. Clause 12 provides a basis for the BTRC to "take action following the provisions of section 64 of the Act" should a service provider violate "any provision of regulations." Furthermore, Clause 4 requires registration by publishers, including any publisher of "online content," and threatens loss of registration for violations of the act. These significant penalties paired with stringent obligations will put undue pressure on intermediaries to restrict content or share user data. Adding to these concerns, we also highlight the separate registration requirements and risks for loss of operating licenses under the MoIB proposal.

Clause 7 sets out additional requirements for "social media intermediaries'' without clearly defining what distinguishes social media from other intermediaries covered by the regulation. Social media intermediaries must appoint a compliance officer, who must serve as senior company personnel and reside in Bangladesh. This officer can be held personally liable in proceedings related to the intermediary if they "failed to ensure due diligence while discharging its duties under the Act and rules made hereunder." While the desire for clear and responsive

1325 G St. NW, Suite 500, Washington, D.C. 20005 • Globalnetworkinitiative.org
• info@GlobalNetworkInitiative.org

reporting lines between relevant authorities and intermediaries is legitimate, as we have noted previously, 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, as well as user trust in intermediaries' ability to safeguard their rights.

Finally, it's worth noting the excessive authorities granted to a broad set of government agencies to issue orders to take down content under the draft regulation. While Clause 6.01(d) states that orders to remove illegal content can come from courts of competent jurisdiction, it also allows notification from the BTRC and references orders from undefined "authorized agencies.'' Furthermore, Clause 10 reiterates the authority for other government ministries to issue written orders to the BTRC to "stop/block/remove" a broad set of categories of content, citing authorities in the telecommunications regulatory act of 2001 (amended 2010). Finally, Clause 11 further clarifies that these authorities are enhanced under certain emergency scenarios, including granting the BTRC authority to issue orders to block access to information without opportunity of hearing. When paired with the significant penalties detailed above, these vague provisions empowering a range of authorities to issue orders will likely lead to significant confusion and uncertainty and make it difficult for intermediaries to respect their users' rights to freedom of expression and privacy.

Privacy Risks

As GNI has noted in our Content Regulation Policy Brief as well as in relation to a similar provision in India's Information and Technology (IT) Rules, traceability requirements create unnecessary risks for privacy and data protection, especially in the case of end-to-end encrypted messages. The incompatibility of traceability provisions with end-to-end encryption was noted repeatedly with respect to India's IT Rules, and Bangladesh's draft OTT Regulations raise the same concerns. End-to-end encryption ensures that only the sender and recipient of a

1325 G St. NW, Suite 500, Washington, D.C. 20005 • Globalnetworkinitiative.org
• info@GlobalNetworkInitiative.org

message can decipher its contents; while the draft law specifies that "no social media intermediary shall be required to disclose the contents of any electronic message," the institution of a mechanism by which the company can decipher messages traveling between two parties, which would likely be necessary to ensure message traceability, would require the company to break encryption and expose user messages to surveillance by other governments and malign non-governmental actors. Breaking encryption in this way may violate Article 43 of the Constitution of Bangladesh, which entitles citizens to a reasonable expectation of privacy in their correspondence and communications.

Even putting aside the impact on encryption, compliance with this rule would require intermediaries 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 privacy infringements. As such, the traceability requirement undermines the commitments to free and secure communications that underpin relevant human rights commitments, data protection principles, and cybersecurity best practices.

Other caveats to the traceability requirement are overbroad, creating risks for first-originator tracing to be abused. Though the draft limits the requirement to social media intermediaries "providing services primarily in the nature of messaging", it does not define how that distinction is made, nor who is responsible for making it. While the draft law states that "less intrusive means" be explored before resorting to first-originator tracing, it does not define what such means may be. The inclusion of "prevention [and] detection" of certain crimes as acceptable purposes for ordering the tracing of a message's first originator is also vague, and potentially allows for overuse of the provision.

1325 G St. NW, Suite 500, Washington, D.C. 20005 • Globalnetworkinitiative.org
• info@GlobalNetworkInitiative.org

Traceability inherently limits anonymity, and as such it poses a threat to freedom of expression by chilling speech. The provision in the clause that "where the first originator [...] is located outside the territory of Bangladesh, the first originator [...] within the territory of Bangladesh shall be deemed to be the first originator" is especially concerning for its implication that a message recipient who passes along that message and happens to be the first one within Bangladesh's borders to do so, could be held accountable for crimes relating to the message's content.

The draft law's provisions regarding data storage and government access to user data raise additional concerns about undermining the protections against arbitrary or unlawful interferences in the right to privacy as established in the Universal Declaration for Human Rights and the ICCPR. The requirement for intermediaries to keep user data for 180 days following the cancellation or withdrawal of an account (Clause 6.01(g)), as well as the provision requiring the storage of voluntarily removed data (as mentioned in 6.01(f)), are in tension with data protection principles, user autonomy, and expectations around corporate responsibility.

Clause 6.01(f) stipulates that deleted data must be retained "for investigation purposes" for 180 days "or for such a longer period as may be required by the court or by Government agencies who are lawfully authorized". The lack of definitional clarity with respect to the time period for which the data must be retained, the government agencies authorized, and the types of investigations conducted expose users to potentially indefinite retention of their personal information for unspecified purposes and without adequate oversight, transparency, or accountability. Similarly, the requirement in clause 6.01(i) that intermediaries must provide government agencies with user data under any government order 72 hour will make it difficult for intermediaries to adequately assess particularly complicated or broad demands, resulting in unnecessary and disproportionate disclosure of user information.

1325 G St. NW, Suite 500, Washington, D.C. 20005 • Globalnetworkinitiative.org
• info@GlobalNetworkInitiative.org