Internet Impact Brief

Bangladesh: Regulation for Digital, Social Media and OTT Platforms, 2021

Neeti Biyani, Internet Society
Noelle Francesca De Guzman, Internet Society
Namrata Maheshwari, Access Now
Shahzeb Mahmood, Centre for Governance Studies

Abstract

The draft 'Bangladesh Telecommunication Regulatory Commission Regulation for Digital, Social Media and OTT Platforms, 2021' presents a new content governance framework for digital, social media and OTT platforms operating in the country. It seeks to legally limit intermediary liability protection and introduce traceability within end-to-end encrypted services offered by social media and messaging platforms.

This report uses the Internet Impact Assessment Toolkit[1] (IIAT) to assess how the draft regulation may affect Internet development in Bangladesh, and more broadly, the health of the global Internet. It finds that the provisions outlined in the draft regulation, specifically the stringent and overly broad requirements for Internet intermediaries, including infrastructure providers, could have serious repercussions on the usefulness of the Internet for Bangladesh and its people, endangering the very sectors that the regulation seeks to foster and protect. If enacted in its current form, the regulation could curtail the country's digital transformation without imparting clear benefits for its economy and society.

Methodology

The Internet owes its strength and success to a foundation of critical properties that, when combined, represent the Internet Way of Networking (IWN). This includes: an accessible Infrastructure with a common protocol, a layered architecture of interoperable building blocks, decentralized management and distributed routing, a common global identifier system, and a technology neutral, general-purpose network.

To assess whether the present proposal has an impact on the Internet, this report will examine its impact on the IWN foundation the Internet needs to exist, and what it needs to thrive as an open, globally-connected, secure and trustworthy resource.

[1] The IIAT was developed by the Internet Society to be used by anyone who wants to check if a particular policy, development, or trend affects the critical properties of the Internet Way of Networking (IWN). https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/

To ensure that Bangladesh continues to benefit from the Internet, future iterations of the regulation must align its provisions with the principles that make the Internet an open, globally connected, secure and trustworthy resource for all.[2]

Context

On February 3, 2022, the Bangladesh Telecommunication Regulatory Commission (BTRC) published the first draft of the 'Bangladesh Telecommunication Regulatory Commission Regulation for Digital, Social Media and OTT Platforms, 2021' (hereafter, the 'draft Regulation'). The BTRC, empowered under the Bangladesh Telecommunication Regulation Act, 2001, introduced it to govern online content to protect end users and vulnerable groups, including women and children; prevent fraud and threats to public tranquility and sovereignty; and discourage piracy and obscenity. Much of the draft Regulation mirrors provisions in India's 'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021'.

The draft Regulation defines an intermediary as "any person who on behalf of another person receives, stores or transmits electronic records or provides any service with respect to such records and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes." Although there is no specific definition of a social media intermediary, the draft Regulation refers to it throughout its provisions. There is also no distinction between a social media intermediary and a significant social media intermediary, but the Bangladesh's Ministry of Information and Broadcasting's draft 'Over The Top (OTT) Content-Based Service Delivery and Operations and Advertisement Broadcasting Policy, 2021' defines a significant social media intermediary as having more than one million registered users.

Bangladesh's draft Regulation requires intermediaries, including social media intermediaries, to comply with a number of new requirements:

1. Intermediaries must visibly publish the rules and regulations, privacy policy, and user agreement on their website or app. Terms of service should inform users "not to host, display, upload, modify, publish, transmit, store, update or share any information" that:
   - belongs to another person
   - is illegal, defamatory, obscene, pornographic, or intrusive of one's privacy including bodily privacy

[2] This report draws from the analysis undertaken for the Internet Impact Brief on India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 given the similarity between both the legislative proposals. https://www.internetsociety.org/resources/doc/2021/internet-impact-brief-2021-indian-intermediary-guidelines-and-the-internet-experience-in-india/

- is harmful to children
- threatens the unity, integrity, defence, security or sovereignty of the country, or its relations with other countries, public order (including communal and social harmony), or breaches the secrecy of the government
- goes against Bangladesh's liberation war and its spirit, national figures, anthem or flag
- is offensive, false, humiliating or threatening, or hurts religious values
- violates intellectual property rights
- impersonates another person, is willfully misleading or deceiving in nature, is patently false or untrue.

2. Social media intermediaries providing services primarily in the nature of messaging should enable the identification of the "first originator" of information in response to a BTRC or court order. In this case, the first originator of information is assumed to mean the first person who introduces a certain message on the messaging platform in question. The BTRC reserves the right to pass an order to prevent, detect, investigate, prosecute or punish an offence to the country's sovereignty and integrity, national security, international relations, public order, or if the content involves child sexual abuse material (CSAM) or violence against women. In case the first originator is located outside Bangladesh, the draft Regulation specifies that the first sender within the country's territory will be deemed to be the first originator of the information.

3. Intermediaries must remove unlawful content[3] within 72 hours after receiving an order from the BTRC, the judiciary or any competent government agency. End users too, can file content takedown requests with the intermediaries' appointed Resident Complaint Officer, which must be taken down within the same timeframe should it *prima facie* concern nudity, sexual content, morphed images, or impersonation. Intermediaries are encouraged to deploy technology-based, automated content filters on their platforms, to "proactively identify information that depicts any act or simulation in any form" depicting CSAM or violence against women, as well as content that is identical to those previously removed or made inaccessible on their platform. There are clauses however, that safeguard free speech and the privacy of users against the use of automated content filters, as well as ask for their human oversight and periodic review.

Further, intermediaries are required to preserve information on content that was removed due to users violating terms of service, government or court order, or based on a grievance received for 180 days.

[3] The draft Regulation deems content related to national security, integrity, sovereignty, international relations, public order, decency, morality, contempt of court, defamation, among others, as unlawful.

How Bangladesh's Draft Regulation Affects its Internet Development

Bangladesh's socio-economic transformation has relied on an Internet that is open, globally connected, secure and trustworthy. To reach the goals of Digital Bangladesh, the country needs the Internet to continue working this way. We assess how the draft Regulation might limit or encourage further Internet development in the country by examining how it could impact the properties that enable the Internet's growth and utility.

Easy and Unrestricted Access

It is easy to become part of the Internet, for networks and users alike. Networks operators can easily add themselves to the Internet's infrastructure without unnecessary regulatory or commercial barriers. Responsive Internet infrastructure creates an Internet that is affordable for users and that has accessible services, empowering users to connect and use the Internet with minimal barriers.

The requirement for intermediaries to retain user data for at least 180 days, and to build a database of previously flagged content, along with tight deadlines imposed on them to take down objectionable content, entails significant costs that only the largest intermediaries can afford.

Only businesses with resources to process requests in a timely manner, maintain huge databases of user information, and keep these and other processes to adhere to the regulation secure, will be able to comply, and thus operate, in Bangladesh.

This poses hurdles for Bangladesh's startups and small businesses, several of whom have been internationally recognised,[4] and their ability to grow and scale, ultimately hurting the country's ability to compete globally. This directly counters the draft Regulation's goal to "ensure fairness for all players in digital and OTT platforms" (sic). The Internet in Bangladesh will be less open as a result, with only a few intermediaries dominating the market, consequently limiting the choices available for local users.

Unrestricted Reachability

Internet users have access to all resources and technologies made available on the Internet and are able to make resources available themselves. Once a resource has been made available in some way by its owner, there is no blocking of legitimate use and access to that resource by third parties.

[4] "9 Bangladeshis on Forbes Asia 30 Under 30 list." Dhaka Tribune, April 20, 2021. https://archive.dhakatribune.com/business/2021/04/20/9-bangladeshis-on-forbes-asia-30-under-30-list

The scope of objectionable content and content takedown laid out in the draft Regulation is overly broad and loosely defined, which risks making a substantial portion of global knowledge inaccessible to Internet users in Bangladesh.

Government authorities tasked with issuing takedown orders for content that violates 'decency', 'morality,' 'integrity', 'public order' or 'any law', or that depicts 'imitable behavior' may interpret these concepts differently, and possibly subjectively. This ambiguity increases due to provisions like 'insulting', 'humiliating' and 'harmful' for content takedown, impacting access and reachability. This was exemplified by a BTRC ban on pornographic websites that resulted in Google Books being blocked in the country.[5]

Such restrictions on content governance contravene internationally agreed upon standards, such as the Manila Principles[6] and the Santa Clara Principles[7] that govern intermediary liability and content moderation. A violation of these standards will impact the information available to Internet users in the country.

To police a broad swath of content on their platform, intermediaries will most likely need to rely on automated systems, which are notorious for their inability to meaningfully distinguish between legal and illegal information. For instance, filters designed to target the word 'breast' have previously blocked content about breast cancer.[8] This could inhibit the government's efforts to deliver crucial health information to citizens, and hamper the rollout of medical services online.

The intermediaries covered by the draft Regulation, specifically those subject to content takedown and user suspension requirements, include "telecom service providers, network service providers, Internet service providers, (and) web-hosting service providers." These are infrastructure providers which do not transmit content directly to end users, but provide services that support the operations needed for the Internet to function properly. At this level, services are not able to target a response to a takedown order to a specific piece of content – they will, for example, end up denying services to an entire website. When asked to moderate content, their actions will be less precise and more extreme, which risks pulling an even larger proportion of legitimate content offline. The infrastructure sector is also less

[5] Dhaka Tribune, 'Major Bangla blog, Google Books on BTRC porn list', January 21, 2019. https://archive.dhakatribune.com/bangladesh/nation/2019/02/21/major-bangla-blog-google-books-on-btrc-porn-list?fbclid=IwAR21KDj9teIBN_fBCnHkr886mh0yhS6aBzTuwzGmbQYeF3xlLRju-19UVOk

[6] Manila Principles on Intermediary Liability: Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation, March 2015. https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf

[7] The Santa Clara Principles on Transparency and Accountability in Content Moderation. https://santaclaraprinciples.org/

[8] Glaser, A., '404 Day: A Day of Action Against Censorship in Libraries', *Electronic Frontier Foundation,* March 26, 2014. https://www.eff.org/deeplinks/2014/03/404-day-day-action-against-censorship-libraries-and-schools

diverse, meaning it will be harder for those whose websites were inadvertently made inaccessible to find suitable alternatives to get their site back up.

Data Confidentiality of Information, Devices, and Applications

Data confidentiality, usually accomplished with tools such as encryption, allows end users to send sensitive information across the Internet so that eavesdroppers and attackers cannot see the content or know who is communicating. Allowing the transfer of sensitive information helps create a secure Internet. Data confidentiality also extends to data-at-rest in applications. (N.B., "confidentiality" also contributes to privacy, which is part of a trustworthy Internet).

Bangladesh's draft Regulation requires social media intermediaries providing messaging services to identify the "first originator" of information in response to a BTRC or court order. Doing so would effectively expose sensitive information held by the public and private sectors being transmitted online to criminals and bad actors, and restrict the use and deployment of security technologies in Bangladesh.

Internet applications, including messaging services, increasingly depend on encryption technologies, specifically end-to-end encryption, to keep information safe online. Encryption is a way of scrambling a message or a piece of information, making it unreadable except to a person who has the 'key'[9] to turn it back to its readable (plaintext) form. The most secure messaging platforms use end-to-end encryption, which keeps information indeciphrable except to its sender, and its intended recipient. This means no one else, not even the messaging platform, would know what information is being conveyed.

This is a crucial advancement in security, as companies that hold and have access to a lot of data are a prime target for cyberattackers. We can thank encryption for making Bangladesh's Internet services secure – from its e-commerce industry to its critical infrastructure systems.

By keeping encrypted information indeciphrable except to its sender and its intended recipient, end-to-end encryption leaves messaging services without the ability to identify the first originator of a message. Upon receiving a request to trace the originator of a specific message – one that law enforcement presumably has accessed through other means, such as access to a device or another user reporting it – an intermediary may need to link the known content of a message with the originator.

The two proposed methods of implementing traceability in India[10] – tagging and including the identity of the originator in an encrypted form with each message; and comparing messages against a library of alpha-numeric hashes maintained by the messaging services – have revealed how error-prone traceability can be, and how it can link information to users who had no role in introducing the content

[9] A 'key,' in this context, refers to a piece of data that lets you encrypt or decrypt something.

[10] Internet Society, 'Internet Impact Brief: 2021 Indian Intermediary Guidelines and the Internet Experience in India', November 2021. https://www.internetsociety.org/wp-content/uploads/2021/11/IIB_India-Intermediary-Guidelines-EN.pdf

of concern on a messaging platform.[11] To reliably link a piece of content to its first sender, an intermediary will need to read each message in a forwarding thread[12] – something it cannot do if it cannot decrypt these messages. To comply with the regulation, intermediaries will have to effectively abandon end-to-end encryption.

The draft regulation contains a sub-provision here stating that a tracing order cannot be issued in cases where "other less intrusive means are effective in identifying the originator of the information." However, it is not clear what "other less intrusive means" must be explored before a tracing order can be issued, thereby giving the regulator disproportionate discretion in exercising its mandate.

As the government makes progress with its digital inclusion programs, more and more people will use the Internet and messaging services in Bangladesh. Governments and businesses have begun to rely on these same services to reach citizens, transact with customers, and exchange information with each other. Without end-to-end encryption to protect it, online communications in Bangladesh will be at the mercy of fraudsters, and malicious actors. Having data readily available in plaintext for well-resourced, bad hackers to access will make attacks such as the USD 1 billion attempted raid on Bangladesh's national bank[13] – one of the world's biggest cyberheists – easier to execute, and more likely to succeed.

Such incidents degrade users' trust in the Internet, and could slow the uptake of digital services and applications in Bangladesh, including those offered by the government. At the same time, potential investors to Bangladesh's economic zones and IT parks will be assessing the robustness of its digital security in deciding whether to locate their businesses in the country.

Bangladesh's digital competitiveness, and the success of its flagship programmes for inclusive development, including its mobile financial services, depend in large part to its adoption of secure technologies. By mandating traceability, the government will not only deprive the country of data

[11] The first proposal will require the identity of the originator to be tagged and included in an encrypted form with each message, so that the intermediary can decrypt the originator's information if required by a government order. This completely breaks user expectations from end-to-end encryption. The first proposal also suggests that users mark a message 'forwardable' or 'non-forwardable' in order to indicate assumption of responsibility as an originator. If a user originates a message and marks it as 'forwardable', their information gets linked with the message. However, if a sender marks a message 'non-forwardable' and the recipient forwards it nonetheless, the recipient becomes the originator and their information is linked with the message. The second proposal requires that a library of alpha-numeric hashes for every message be maintained, against which the hash of a message subject to a government order can be compared to enable traceability. Hashing is the practice of using an algorithm to map data to a fixed length. An end-to-end encrypted messaging service would therefore have to maintain a library of numerous hashes to assist the government trace the originator of a message in case of an authorized order. However, even a small change to a certain message can alter its hash, and subject it to an illegitimate government order for tracing.

[12] Internet Society, 'Traceability and Security: Experts' Workshop Series on Encryption', November 2020. https://www.internetsociety.org/wp-content/uploads/2020/11/2020-Encryption-in-India-EN.pdf

[13] Banka, N., 'Explained: The story of how North Korea hackers stole $81 million from Bangladesh Bank', The Indian Express, June 30, 2021. https://indianexpress.com/article/explained/bangladesh-bank-robbery-north-korea-lazarus-heist-7375441/

confidentiality, it will also compel businesses to stick with out-of-date security features, rendering them ill-equipped to tackle an ever-evolving cyberthreat landscape.

Reliability, Resilience, and Availability

The Internet is reliable when technology and processes are in place that permit the delivery of services as promised. If, for example, an Internet service's availability is unpredictable, then users will observe this as unreliable. This can reduce trust not just in one single service, but in the Internet itself. Resilience is related to reliability: a resilient Internet maintains an acceptable level of service even in the face of errors, malicious behavior, and other challenges to its normal operations.

The draft Regulation's traceability requirement for intermediaries will make online messaging services, and other platforms with a messaging function, unreliable. Without end-to-end encryption, and with their information available for platforms and bad actors to exploit, users in Bangladesh will be vulnerable to threats that they have no capability of ascertaining. Proposed methods[14] to carry out traceability could also link users to content that they may not have generated, further increasing their reluctance to communicate online.

The heightened uptake of other secure messaging platforms in Bangladesh after Whatsapp changed its privacy policy[15] shows that Bangladeshis want services that they can trust and rely on to keep their data safe. Without the guarantee of robust encryption, Bangladeshis may hesitate to share resources and important data on the Internet, reducing the flow of information in the country. Patients consulting through telemedicine may opt not to tell their doctor about their health condition; trading partners from different parts of the country may need to meet physically to close a deal. This could undo the progress that Bangladesh has made in digitisation.

Accountability

Accountability on the Internet gives users the assurance that organizations and institutions they interact with are directly or indirectly acting in a transparent and fair way. In an accountable Internet, entities, services, and information can be identified and the organizations involved will be held responsible for their actions.

The draft Regulation provides overarching powers to the BTRC, the judiciary or any competent government agency to order removal of content, without procedural safeguards that would serve as a check on this power. This, and the regulation's vague scope of objectionable content, would allow government authorities, including non-judicial bodies, to have content removed arbitrarily, with no objective standards to guide its decisions.

[14] 'Traceability and Security: Experts' Workshop Series on Encryption' Internet Society. November 2020. https://www.internetsociety.org/wp-content/uploads/2020/11/2020-Encryption-in-India-EN.pdf

[15] Kamruzzaman, M., 'Turkish messaging app booms in Bangladesh', *Anadolu Agency*, November 17, 2021. https://www.aa.com.tr/en/asia-pacific/turkish-messaging-app-booms-in-bangladesh/2112664

That content must be removed within 72 hours of receiving an order mounts inordinate pressure on social media intermediaries to urgently adhere to takedown notices. This could cause them to disregard transparency and accountability mechanisms – such as informing the user that their account will be suspended or their content taken down, and on what grounds – and lead to hasty and opaque procedures. Smaller, less-resourced intermediaries may be discouraged from even putting such policies in place. Additionally, the draft Regulation does not lay out a provisions for users to raise grievances and challenge an unfair takedown of content.

Meanwhile, the lack of meaningful definitions around objectionable content would prevent intermediaries from communicating clear and precise rules on what users are allowed to share on the platform. This is even more unworkable for intermediaries providing services at the infrastructure level, most of whom do not have a direct insight into end user content.

A separate clause strongly encouraging social media intermediaries to introduce technology-based measures, including automated tools, to proactively detect and filter content would have a similar effect. While the aim to remove content depicting child sexual abuse material and violence against women is justifiable, automated content filtering systems are error-prone, have inherent biases and prejudices, and routinely filter out legitimate content, resulting in an over-removal of content[16] and unnecessary takedowns. While intended for legitimate reasons, these systems can also be easily repurposed to track other types of user information, not only by platforms but by criminals who get access to them. Neither does the draft Regulation set out provisions to allow users to appeal against takedown of legitimate content, making it even more likely that perfectly legal, and informative content will remain inaccessible for good.

Social media platforms are already under fire for their opaque use of algorithms to manage content on their site.[17] The draft Regulation emboldens them to design and deploy more of these systems to monitor content and determine the scope of allowable speech, pushing them further to assume an adjudicatory role.[18]

Together, the lack of accountability and transparency mechanisms undermines trust in Internet services in Bangladesh, and creates an unpredictable online environment for businesses and ordinary users in the country, hindering the growth of a healthy digital ecosystem.

[16] Article 19, 'Freedom of Expression Unfiltered: How blocking and filtering affect free speech', December 2016. https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf

[17] Mostert F. & Urbelis A., 'Social Media Platforms must abandon algorithmic secrecy', Financial Times, June 17, 2021. https://www.ft.com/content/39d69f80-5266-4e22-965f-efbc19d2e776

[18] Praveen Arimbrathodiyil vs. Union of India. https://sflc.in/praveen-arimbrathodiyil-vs-union-india-sflcin-assists-challenging-part-ii-intermediary-rules-2021

Privacy

Privacy on the Internet is the ability of individuals and groups to be able to understand what information about them is being collected and how, and to control how this is used and shared. Privacy often includes anonymity.

The reguirement for social media intermediaries to trace a message's first originator, and to monitor user content based on an ill-defined criteria, infringes upon the right to privacy of correspondence and other means of communication guaranteed in the Constitution of Bangladesh.[19]

By effectively forcing messaging service providers to give up end-to-end encryption, the draft Regulation reduces privacy assurances for its citizens and the entities operating in the country, and will cause insecurity in Bangladesh's ability to safeguard vital information that is conventionally shared and stored online, including trade secrets, and commercial and financial communication. Loss of privacy may also leave Bangladesh's vulnerable groups, such as women and children, more prone to exploitation, as criminal syndicates can more easily access information about them – unnecessarily exposing to abuse the same communities that the draft Regulation seeks to protect.

Summary and Recommendations

Using the Internet Impact Assessment Toolkit, this brief has found that the main provisions under the Bangladesh Telecommunication Regulatory Commission Regulation for Digital, Social Media and OTT Platforms, 2021 will have negative repercussions on the open, globally connected, secure and trustworthy Internet.

The proposed regulation introduces significant compliance costs to service providers in Bangladesh, and poses barriers to entry especially for its burgeoning tech industry, making the Internet *less open* to those that want to utilise it.

Its vaguely defined scope for objectionable content risks depriving Internet users in Bangladesh of useful and educational information from government and other legitimate sources, and making them less reachable to the outside world, thus *limiting global connectivity*.

To adhere to the traceability requirement service providers operating in Bangladesh would have little choice but to resort to using outdated security standards, which leaves the country's ecosystem exposed to rapidly evolving cyberthreats, making the Internet *less secure* for all its users.

The regulation enables a lot of unaccountable actors and actions, both from government enforcers and complying intermediaries. Along with the resulting lack of privacy in online communications, it will

[19] Constitution of the People's Republic of Bangladesh, Art. 43, cl. A. http://hrlibrary.umn.edu/research/bangladesh-constitution.pdf

create an uncertain, unpredictable, and non-transparent environment for businesses to operate in. It will make the Internet and online services in Bangladesh *less trustworthy*, and less appealing for citizens to use, curtailing the country's efforts at digital inclusion.

Recommendations:

To align the draft Regulation with global standards and best practices, it should be redrafted to:

- Strictly limit the types of content that intermediaries are required to block, remove or otherwise limit the availability of, and provide concrete, unambiguous and specific definitions for each type of content covered by the draft Regulation. Limitations must be in line with Article 39 of the Constitution of the People's Republic of Bangladesh, and Article 19 of the International Covenent of Civil and Political Rights and the Universal Declaration of Human Rights, and any restrictions on speech must be 'reasonable,' and therefore meet the principles of necessity and proportionality.[20]
- Remove the traceability requirement for intermediaries offering secure communications services enabling privacy and anonymity, including encrypted messaging services. Bangladesh will rely more and more on encrypted technologies as it pursues a data-centric development. As such, it should foster, and not curtail, the use of robust security technologies, including end-to-end encryption, in all facets of digital life in the country.
- Incorporate strict safeguards against potential abuse by government and law enforcement agencies and intermediaries empowered to act on their orders. There must be independent and judicial oversight of any takedown order sought to be issued by government or law enforcement agencies and other authorised bodies. Intermediaries must be allowed to process and respond to orders in a manner that is accountable and transparent to Internet users, and a mechanism must be created to ensure remedy and redressal for affected persons.
- Content moderation must not be based solely or heavily on automated tools as they are prone to returning erroneous results and perpetuating biases. Automated tools, supported by human reviewers, should not be developed and implemented by social media intermediaries alone; they should instead be developed in a collaborative manner between the technological industry and relevant stakeholders, including civil society, security experts, and women's and child rights organizations.

[20] (2014) Necessary and Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance. *Office of the High Commissioner for Human Rights*. https://www.ohchr.org/documents/issues/privacy/electronicfrontierfoundation.pdf