4 March 2022

Asia Internet Coalition (AIC) Comments on Bangladesh Telecommunication Regulatory Commission Regulation for Digital, Social Media and OTT Platforms, 2021 ("Draft Regulation")

To,

Mr. Shyam Sunder Sikder
Chairman, Bangladesh Telecommunication Regulatory Commission
IEB Bhaban (5, 6 and 7 floor)
Ramna, Dhaka 1000
Bangladesh

Subject: Asia Internet Coalition (AIC) Industry Letter in response to the call for public consultation on the Bangladesh Telecommunication Regulatory Commission Regulation for Digital, Social Media and OTT Platforms, 2021 ("Draft Regulation").

The Asia Internet Coalition ("AIC") and its members convey our sincere appreciation to the Bangladesh Telecommunication Regulatory Commission **("BTRC")** and the Government of Bangladesh **("Government")** for its efforts in undertaking a public consultation on the Draft Regulation for Digital, Social Media and OTT Platforms, 2021 ("Draft Regulation")**.** AIC strongly believes in the benefit of expert opinion, multi-stakeholder dialogue and open discussions that consider the broader issues and implications surrounding this Draft Regulation.

Ultimately, the AIC and Government are aligned in seeking policies that foster innovation and technological advancement in Bangladesh, while protecting the right of Bangladeshi to freely and securely communicate. We commend the Government's commitment to the objectives of Digital Bangladesh, including safeguarding fundamental rights under the Constitution of Bangladesh, and implementing its obligations under various international treaties and conventions.

As an introduction, the AIC is an industry association of leading internet and technology companies that seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our mission is to represent the internet industry and participate and promote stakeholder dialogue between the public and private sectors, sharing best practices and ideas on internet technology and the digital economy.[1]

[1] In the past, AIC has worked extensively on key policies in Bangladesh such as the Digital Security Agency Rules, 2020 ("DSA Rules 2020"), the Draft Information Privacy and Security Rules, 2019 ("Privacy Rules"), and Caching Approvals. AIC also works with regulators across several countries in the Asia Pacific region (for example Indonesia, Vietnam, Thailand, Malaysia, Philippines, Singapore, Australia, Sri Lanka, India, Pakistan among others) to help shape technology and internet guidelines.

We understand that in January 2021, the Hon'ble High Court directed the BTRC and the Ministry of Information and Broadcasting (MoIB) to formulate a "guideline to operate OTT (over-the-top) web-based platforms." Pursuant to the High Court's order, BTRC has prepared the Draft and invited public consultation.

The unprecedented digital transformation that Bangladesh is currently undergoing poses many opportunities for both consumers and companies offering OTT services.

Rapid Development of Domestic Players: Growth of online services have transformed the economies of both developed and developing countries. This positive effect has clearly benefited small businesses and individuals. Furthermore, the local audience's appetite for original local content, together with several payment barriers making it difficult to access foreign services, have seen the growth of home grown platforms such as Bongo, Bioscope, Chorki and Binge which are becoming very popular among the public by adding some of their original content as well as allowing them to add international content to the library[2].

Enhancing the Creative Industry: Online services can increase consumer choice, productivity, and innovation, and give local businesses and content creators access to a global customer base, providing individuals with great choice, also at a lower cost compared to traditional broadcast and media. This ultimately expands the nation's creative industry and overall economy and helps to export Bangladeshi culture to the world.

Promoting broadband and ICT value chain: It is also important to note that online services are an essential element of the broadband and ICT value chain. Innovation in this field has led to a rich and diverse Internet, and has stimulated consumer demand for broadband Internet access, which in turn is a key driver for network operators' revenues, incentivising them to upgrade and expand their networks.

As Bangladesh, its people and businesses increasingly benefit from the evolution of the global technology ecosystem, it is essential to avoid introducing rigid frameworks that could impede innovation and competition or cause consumer harm or create obstacles to conducting businesses in Bangladesh. A one-size-fits-all approach to regulating multiple services that are functionally, technically, and operationally different would be problematic and deter growth of the industry as a whole, including local businesses.

In that context, we have some key concerns with the Draft Regulation, including the following:

1. Need for robust safe harbour provisions to limit liability in relation to user generated content;
2. Restrictive local presence requirements that impede growth;
3. Untenable turnaround time with disproportionate penalties;
4. Potential infringement of users' right to free speech and privacy.

AIC is concerned that the Draft Regulation may result in a strict and unyielding regulatory framework based on legacy telecommunications regulation and licensing could engender new

[2] https://www.dhakatribune.com/showtime/2021/02/26/the-r-evolution-of-ott-in-the-local-and-global-market-for-bangladesh

risks. Comments from the UN Special Rapporteur on Promotion and Protection of the Right to Freedom of Opinion and Expression provide guiding principles in this regard:

> "*Smart regulation, not heavy-handed viewpoint-based regulation, should be the norm, focused on ensuring company transparency and remediation to enable the public to make choices about how and whether to engage in online forums. States should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy. States should refrain from imposing disproportionate sanctions, whether heavy fines or imprisonment, on Internet intermediaries, given their significant chilling effect on freedom of expression.*"

Prior to enacting new regulation, we would encourage BTRC to undertake an in-depth analysis of the policy and regulatory implications of online services. We are also supportive of a thorough, transparent and inclusive process for consultations with relevant industry and civil society stakeholders.

Please find our detailed comments on the Draft Regulation in the attached Appendix A.

Should you have any questions, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Appendix A: Detailed Comments and Recommendations

1. Need for robust safe harbour for intermediaries framework

We are concerned that the current legal framework, including this Draft Regulation, does not provide internet intermediaries with safe harbour in relation to unlawful user generated content, that is hosted on or transmitted through the intermediaries' networks without their knowledge. The presence of safe harbours, which are a cornerstone of Internet law internationally, is a critical factor in encouraging a thriving environment for local businesses, the right to communicate, and ensuring a fair distribution of liability.

The concept of safe harbour is critical to the success of the Bangladesh digital economy. In business and economic terms, the content and media industry is well poised to contribute to a nation's overall economic growth and prosperity in both the near and long term. Taking the global video on demand market size as an example, it was USD 53.96 billion in 2019 and is projected to reach USD 159.62 billion by 2027, exhibiting a CAGR of 14.8%,and with Asia Pacific highlighted as the fastest growing market[3]. Bringing these numbers closer to home in Bangladesh, as of February 2021, the BTRC reported there were about 112.715 million Internet users in Bangladesh. Users in the video streaming platforms are increasing with the improvement of internet speed and a growing number of internet users. In addition, along with smartphones, the adoption of smart TV is also increasing[4]. This suggests that there is huge potential for this market to continue and grow in Bangladesh.

An enabling regulatory framework for internet intermediaries is crucial, to bolster the exchange of information, ideas, trade and commerce. There is a direct correlation between a strong safe harbour protection and the fundamental rights protected under Article 39 of the Constitution and international human rights instruments, such as Article 19 of the International Covenant on Civil and Political Rights. Safe harbour protection gives the users the confidence to express themselves online by lessening the risks of excessive self-censorship by intermediaries. In the absence of a safe harbour framework, intermediaries may either be dis-incentivised from growing in a market or over-incentivised to remove content, which is unsustainable and inconsistent with international commitments.

In line with international best practices and the provisions of the Digital Security Act, 2018, the Draft Regulation ought to provide a safe harbour for internet intermediaries, according to which internet intermediaries should not be held liable for content generated by third parties, where the internet intermediaries are not aware of the illegality.

[3] https://www.fortunebusinessinsights.com/industry-reports/video-on-demand-market-100140

[4] https://businessinspection.com.bd/rise-of-video-streaming-platforms-in-bangladesh/

The legal framework should be amended to include a clearly defined safe harbour provision covering service providers hosting user-generated content on their platforms, from both primary and secondary liabilities. This safe harbour provision should cover service providers and their owners, directors, officers, employees, and representatives.. Putting in place a predictable regime for safe harbour – including through an established procedure for serving content takedown notices, following a duly reasoned order and having adequate procedural safeguards would uphold fundamental rights and foster both transparency and accountability.

2. Overbroad, missing and inconsistent definitions

We are concerned that the Draft Regulation defines certain important terms too broadly and introduces inconsistencies with the definitions provided in the Information and Communication Technology Act, 2006 ("**ICT Act**").

Overbroad definitions. For example, the term "OTT" (referring to over-the-top) is defined in Article 2.01(k) as "content, a service or an application that is provided to the end-user over the public internet." At face value, this definition goes beyond what is technically understood as OTT to capture a wide range of online services. It is worth clarifying that an OTT service is not a transmission network, but is instead a service that runs over an Internet network; moreover, the OTT service provider is typically distinct from the operator of the underlying network and does not include services which are not provided for a profit. In the terms of the Draft Regulation, OTT's scope would cover a diverse group of services, which require different market models, infrastructures, and business impact. These services would include but would not be limited to: entertainment, media, communication, telework/telepresence, cloud computing/storage, social media, financial services, e-commerce, Internet of things and online gaming. The phrase OTT can easily become shorthand for almost any internet application or online service available in Bangladesh. This lack of scope limitation is concerning and at odds with international best practices, especially considering the wide grounds for requesting removal of content. We are particularly concerned that if left without modifications, Article 2.01(k) can lead to poorly developed, overbroad, or misapplied regulations of OTT, that harm human rights, limit economic growth and hinder innovation on a broad scale.

As noted in the letter, this Draft Regulation should avoid taking a one-size-fits-all approach to regulating multiple services that are functionally, technically, and operationally different. Including separate definitions for social media intermediaries, video-on-demand services, and other OTT service providers, would be a big step in that direction. We reference a previous AIC study "Online Video Study in Thailand", which was jointly led by Thammasat University's Consulting Networking and Coaching Center (CONC Thammasat) and provides useful elements for consideration by BTRC.

The Draft Regulation seeks to build on best practices and recommendations from the International Telecommunications Union (ITU). A recent official report from the ITU urges Governments to avoid one-size fits all approaches to regulation of OTT's, which we consider should be taken into account in the Draft Regulation to limit the definition of Article 2.01(k): : "regulators must also keep in mind that OTTs are a vast and diverse collection of businesses. A search engine is not the same as an app-store, a subscription movie service is not the same as a social network. In a world where a substantial proportion of all business is transacted over

the Internet, it would be absurd for the nature of regulation to be determined by a one-size-fits-all approach"[5].

Missing definitions. As currently drafted, the Draft Regulation does not define certain key terms. For example, the terms "social media" and "social media intermediary" are not defined.. Similarly, terms such as "service" and "application" are undefined. As such, *any* service or application provided by an internet-based service provider is potentially covered by the Draft Regulation (*See* Article 1(3)(b)-(c)). That cannot be the intention of the lawmakers. This lack of key terms would be highly problematic, as it would bring every company whose services are provided to end-users over the internet and require it to comply with the Draft Regulation even if it was not the intent of the regulation. Additionally, the scope of individual complaints is not expressly provided which could result in individuals seeking takedown of content which was not intended by the Draft Regulation. The elements of ambiguity and unpredictability would result in deterring growth and innovation of start-ups and home grown platforms such as Bongo, Bioscope, Chorki and Binge.

Inconsistent definitions. The Draft Regulation's current definitions of the terms "computer" and "data" (*see* Articles 2.01(e),(f)) are inconsistent with the ICT Act's definition of the same terms (*see* Sections 2(10),(13) of the ICT Act). The presence of inconsistent definitions increases ambiguities and could result in creating hurdles for effective implementation. To avoid conflicting definitions and duplicative provisions across laws, the Draft Regulation should maintain consistency with the terms' definitions from the ICT Act.

3. Local incorporation and physical office

As it stands, the Draft Regulation carries the risk of introducing unnecessary and restrictive requirements on local presence through provisions requiring physical contact address, local representatives and registration with BTRC. This is highly problematic for global companies who make their products and services available to Bangladesh citizens and businesses and may inadvertently inhibit further foreign direct investment in the country. The global internet is built on the principle of cross-border flows and the ability to service global consumers with the same high level products and services, without discrimination. Such provisions not only result in onerous costs and obligations for foreign companies but also adversely impact the national ecosystem. This deviation erects unnecessary barriers to cross-border services trade, which will increase the cost and risks of doing business in Bangladesh and thereby hinder or make access to information and internet-based products more expensive for Bangladeshi consumers.

Such requirements would:

a. **Reduce Bangladesh's competitiveness**: Any requirement for forced local incorporation, criminal liabilities for local officers, and physical office presence will have a negative impact on foreign direct investment, economic growth, and Bangladesh's growing IT industry. A study conducted by European Centre for International Political Economy on forced localization found that the economic impact

[5] https://www.itu.int/dms_pub/itu-d/oth/07/23/D07230000030001PDFE.pdf

of such policies on GDP across seven countries and found that it had a negative impact across the board. The impact on China was (-1.1%) and Vietnam (-1.7%).

b. **Restrict growth of SMEs and stifle innovation**: By focusing on local presence and adding compliance costs, this Draft Regulation artificially restricts market and growth prospects of small businesses by limiting their ability to engage potential overseas partners and resources. Therefore any measures pertaining to the Draft Regulation should not adversely impact small and medium businesses.
c. **Amount to a non-tariff barrier to trade:** Requiring local incorporation and presence unnecessarily discriminates against foreign businesses and poses a non-tariff barrier to trade.. This is particularly stark in view of the nature of the services provided through the internet, which can be provided on a cross-border basis without the need for physical presence.
d. **Limit consumer access to technology**: The global nature of the internet adds to the affordability of services. Changing this virtuous dynamic by requiring local presence will harm economic potential as well as consumer experience on the open Internet whilst increasing costs and limiting the benefits from products, services and information which would have otherwise been available.

The ability for platforms to abide by local laws and customs, such as in order to take down or prevent access to unlawful content, does not depend on having local presence, but rather on having well established processes and product-specific policies, clear local laws to guide the process, and properly informed and valid requests for takedowns and access restriction to unlawful content.

In lieu of focusing on local presence, including punitive criminal measures on local employees, we suggest that the Draft Regulation consider enhancing accountability and transparency of internet content moderation by formalising procedures for routine engagement with platforms and clear parameters for unlawful content take down and access restriction. Such engagement could create a workable standard where platforms are able to work hand-in-hand with regulators to improve their policies and process to effectively manage unlawful content.

We would also like to emphasize that there are no materiality thresholds under the draft rules applicable to the more onerous requirements, such as local presence and transparency reporting.

In addition, to demonstrate the extent of compliance, companies regularly publish transparency reports to give the community visibility into how policies are enforced, respond to data requests and protect intellectual property. These reports contain information on user data disclosure as well as technical efforts to enhance security, disclose data on content removal requests in an effort to inform discussions about online content regulation, and share data on a range of issues relating to policies, practices, and access to information.

4. Appointment of resident compliant officer (6.02) and additional responsibility of intermediary (7.02)

Firstly, Sec 6.02 “Appointment of Resident Complaint Officer " requires disclosure of contact details of such Officer and the timeframe of settling a complaint is unrealistic. OTT platforms

or intermediaries should be allowed to establish a robust mechanism to handle complaints and provide solutions within a reasonable period of time. In addition, the Draft Act is unclear on its ex-territorial reach to overseas OTT platforms and the enforceability of any directives/penalties. Therefore we seek further clarity on ex-territorial reach.

The requirement in the Draft Regulation for intermediaries and social media intermediaries to appoint a resident complaint officer, a compliance officer, and agents (*see* Articles 7.02 and 7.03), is not essential to ensure compliance with local law requirements or to allow for ongoing communications with the Government authorities.

More importantly, this requirement creates substantial law enforcement risks against the resident officers and representatives, especially in light of Section 76 of the Bangladesh Telecommunication Regulation Act, 2001. We are extremely concerned that this section assumes the guilt of individuals for certain criminal offences, based solely on their association, with an allegedly non-compliant company. By forcing these individuals to prove their innocence, this provision turns on their head two fundamental principles, which form the bedrocks of Bangladesh's modern criminal system: the legal burden of proof and the presumption of innocence. Without a clear safe harbour provision in the Draft Regulation protecting the resident officers and representatives of the company from prosecution (see Section 1, above), many service providers would be unwilling to enter the Bangladeshi market and offer services to Bangladeshi citizens, which will not only impede innovation and technological advancement, but also negatively affect the country's internet and start-up ecosystem as well as the national economy, resulting in losses for Bangladeshi society. From a practical standpoint, intermediaries would also struggle to find sufficiently qualified individuals for these roles unless these individuals have the assurance that the safe harbour protection will extend to them as well.

We recommend deleting the requirement to appoint resident officers and representatives. Further, we strongly recommend incorporation of a safe harbour provision that protects both the service providers and its officers and representatives, from primary and secondary liabilities (*see* Section 1, above). In fact, many global companies operate centralized channels and contact points for handling customer and regulatory queries, which allows for the fastest and most efficient handling of such requests as opposed to local operations

5. Fixed turnaround times for response:

We highly recommend that the Draft Regulation should not prescribe a fixed time frame for complying with a takedown notice because such a provision could lead to unintended consequences such as reducing the overall capabilities of service providers from removing user-generated unlawful content, disproportionate enforcement outcomes, and unconstitutional restrictions on speech.. A more effective strategy for creating accountability would be to require companies to make best efforts to respond promptly depending on the complexities and volume of content under consideration.

a. ***72 Hour compliance for content removal requests are unjustifiable***

At the outset, the 72-hour removal requirement is unjustifiable, as 72 hours will often be an insufficient amount of time to investigate the content in question, particularly when the volume of requests is high or the requests relate to complex matters. It is often procedurally impossible in the context of global data requests governed by third country laws and mutual legal assistance treaties or for intermediaries to request for additional information or clarifications within this exigent timeframe. This curtails the ability to meaningfully engage when further information or context is required to address the request. Instead, the regulation should aim for such actions to be carried out without undue delay.

b. ***Penalty for failure to meet fixed turnaround time is disproportionate***

Furthermore, the penalties for noncompliance with the 72-hour response requirement are disproportionately severe. By referring to Section 66A of the Bangladesh Telecommunication Regulation Act, 2001, Article 10 of the Draft Regulation provides that a service provider could be subject to a criminal fine amounting up to BDT 3 billion (approx. US $35m) and/or imprisonment for up to 5 years for failure to remove contents in a timely manner from its platform.

There is no graded approach to these penalties or clarity on how they could be imposed. These penalties are disproportionate and should only be reserved for instances of severe systemic non-compliance.

c. ***Free speech and user rights concerns: This requirement is likely unconstitutional and may amount to an unlawful restriction of speech***

The Draft Regulation stipulates wide and over-broad grounds for removal of content. Under the constitutional frameworks of Bangladesh, each citizen has a guaranteed right to the freedom of speech and expression, subject to certain exceptions and qualifications prescribed by law. This fundamental right is essential to the development and functioning of the country's democracy and the rule of law, and to infringe upon free speech without due consideration to the restrictions and its reasonableness in the context of the overall circumstances is contrary to the letters and spirit of the well-established constitutional principles. The user-generated content removal scheme contemplated by the Draft Regulation lacks safeguards that could amount to an unlawful restriction on free speech and user rights, and would have the inadvertent effect of self-censorship in many cases. Given that these interests are enshrined within the Constitution of Bangladesh as a fundamental right of every citizen, the Government should adopt an approach to regulation which is both balanced and practical. Any notice takedown regime for online content must incorporate safeguards around due process, proportionality, and definitional clarity, to bring it in line with international best practices.

d. ***Fails to address the most harmful unlawful content****:* If intermediaries are compelled to remove unlawful content within a fixed deadline, they could be incentivised to either excessively remove contents or impose prior restraints on contents, or both. Additionally, it is counterproductive to focus on the average speed of assessment as it

would act as a bottleneck to prioritising review of the most harmful content (based on nature and prevalence of such content). To avoid such pitfalls, we propose that requests should be responded to within a reasonable timeframe, or "without undue delay." instead of stipulating an untenable timeline.

6. Government request and data retention

As noted above, the requirement of compliance to government requests in 72 hours can be technically unfeasible, considering the sheer volume and complexity of the requests. It is also often procedurally impossible to comply with for foreign requests for data governed by foreign laws and Mutual Legal Assistance Treaties (MLAT) within 72 hours. Instead, the law should state such actions should be carried out within a reasonable time and following established procedures under international law. To enable compliance in a reasonable time, valid legal requests should provide specific and required details such as the nature of offence along with the purpose of seeking information.

In addition to this, the Draft Regulation's requirement to store user information collected by service providers for a period of 180 days (*see* Article 6.01(f), (g)) is cumbersome and costly. It is also unclear whether such a requirement would be consistent with the principles and rules of the upcoming Bangladesh data protection law. Particularly for service providers operating in several jurisdictions and at a global scale, this requirement would impose undue financial burden and create capacity issue, as many of these online service providers have a rapidly increasing user-base and it may not be feasible to ensure such long-term retention without investing substantially in safeguard measures to mitigate the risks of a privacy breach. Such a requirement would be counterproductive to the objective of ensuring user privacy because it would require collection and storage of data for longer than required.

Additionally, many companies have adopted automated data retention and routine deletion and recycling procedures, requiring such companies to restructure their policies and practices to meet the specific legal requirement of each jurisdiction they operate in is unreasonably burdensome from both a technical and a financial perspective.

All in all, these requirements will substantially increase the cost of business operation, making internet and online products more expensive and less accessible to consumers. This will be especially harmful in Bangladesh, where the openness and affordability of the internet-based tools and services are catalysing business expansion and stimulating economic growth at an unprecedented rate.

7. Enabling traceability of originators (Article 7.03)

Article 7.03 would require social media intermediaries providing messaging services to enable the identification of the "first originator" of information upon court order or an order from the BTRC. The need for this provision to enable tracing out of originators of information on its platform or traceability is unclear especially considering that basic subscriber information is already provided by various online platforms pursuant to lawful and valid requests.

In the case of encrypted services, such a provision would have no effect as an intermediary cannot be required and may be in practice technically unable to weaken encryption in order to provide relevant details, at least without severely compromising the overall security of the service and of all other users who rely on said service. Traceability requires messaging services to store information that can be used to ascertain the content of people's messages, thereby compromising the very guarantees of privacy and encryption and would be highly susceptible to abuse. This would infringe upon the legitimate expectation of privacy that individuals have in their private communications, especially when those communications are encrypted, as provided for under Article 43 of the Constitution. The Draft Regulation does not: (i) respect the baseline privacy expectation of Bangladeshi citizens; (ii) articulate the reasonableness considerations that should be taken into account before an order is issued; and (iii) explain what 'other less intrusive means' are required to be explored before an order is issued.As it stands, Article 7.03 will likely deter multiple companies from offering their services in Bangladesh, as it introduces a requirement for excessive data collection, and weaker security and encryption. As a result, Article 7.03 would de facto result in less secure and privacy intrusive products and services specifically for the Bangladeshi market. That cannot be the intention of the Draft Regulation, as it aims to achieve the exact opposite by building a more secure and trustworthy online ecosystem for Bangladesh. Additionally, to enable tracing would require companies that operate at a global scale to collect and store additional information which would be cumbersome, costly and unfeasible.

The traceability requirement reverses the burden of proof and requires individuals to demonstrate that they did not intend to misinform. The inevitable outcome is self-censorship. We recommend this provision to be removed in its entirety.

The lack of clarity, technical infeasibility (especially for smaller players), undue weakening of security and encryption, potential for breach of privacy via surveillance and subjectivity in enforcement are all reasons why this provision should be removed.

8. Broad power of MoIB

The MoIB's authority to regulate publishers of online curated content, publishers of news and current affairs content and web-based programs is both broad and undefined. To ensure clarity and predictability around the definition of publishers of online curated content we would recommend it is limited to the exercise of effective control both over the content itself and over its editorial organisation either in a chronological schedule, in the case of television broadcasts, or in catalogue, in the case of on-demand audiovisual media service. It is important to note that content sharing platforms are not the same as being a publisher of online curated content. This notion of publisher is also not applied to the undefined reference to web based programs/films/series, with the uncertain consequence that intermediaries on whose service these programs are made available may also be subject to this provision.

The lack of specificity regarding the MoIB's scope of authority creates an unpredictable regime for online service providers to operate in. Particularly, it exposes curated content and video-on-demand service providers to an unforeseeable risk of being subject to the same stringent screening and censorship standards typically applied to the traditional film and broadcasting industry. With the development of internet-based media distribution systems, content creation

and distribution has become more democratised and consumers now have more access to more and better content, and these stringent standards, if applied to online streaming services, would adversely impact content availability, significantly limit consumer choices, and lead to further internet fragmentation.

Additionally, the policy prepared by the MoIB appears to be inconsistent with the Draft Regulation and it is unclear as to how the policy and the Draft Regulation will interact with one another. It is equally unclear as to how the policy and the Draft Regulation will apply to companies that provide both curated and user-generated content, and which government authority – BTRC or MoIB – will exercise jurisdiction over such companies. In the interest of a predictable and transparent regime, to avoid undue restriction on speech, and to avoid conflict of laws, there should be one instrument and one nodal authority regulating service providers using the internet as a delivery medium.

Recommended Policy Route

"One size fits all" legislation is unlikely to effectively address a highly complex and nuanced problem in practice. Broad and expansive legislations are likely to deter innovation in the industry and also harm freedom of expression and speech, and dampen public debate and exchange of ideas, information and knowledge - a fundamental feature of successful digital economies. To ensure that the Internet remains a safe place for innovation, knowledge and business to thrive, diverse entities including industry, government and policy makers, media and publishers, academia, and users themselves must be part of the solution.

Promising, alternative solutions have emerged and should be considered to address the multifaceted issues which BTRC seeks to address through the Draft Regulation . Bringing together stakeholders across industry, governments, and civil society can help identify solutions that can more effectively address the BTRC's concerns. These range from jointly-developed technology tools that reduce the prevalence and impact of unlawful content, to digital literacy, and to the establishment of fact checking centres.

Combating unlawful content online is best achieved through a combination of hard and soft law instruments. What this means is having a balance of regulation to address clearly illegal content (such as child sexual abuse materials and terrorist related content) combined with co-regulatory or self-regulatory measures, such as Codes of Practice and internal policies, to address disputed content that may be legal but potentially harmful (such as misleading or false information). This allows for greater flexibility to adapt to ever-changing threats, as well as evolving definitions and understandings of societal harm and illegal activity.

We would welcome a discussion with the BTRC on how a self- or co-regulatory industry code, such as those implemented in the European Union, Australia and in development in New Zealand. Industry codes of practice can be an effective way to ensure a sufficiently flexible regulatory framework that clearly holds companies accountable while allowing for flexibility and speed to adapt to ever-changing and evolving safety concerns and threats on the internet.

An industry code of practice developed by the industry (alongside other relevant stakeholders, e.g. government and civil society) would: 1) ensure technical requirements and obligations are appropriate, feasible and suitable for the local market, while also aligning with global standards; 2) ensure legitimacy and support of the code among key stakeholders; 3) facilitate multi-stakeholder collaboration and cooperation; 4) provide greater flexibility to iterate, improve, adapt and respond quickly to ever-changing or emerging threats; and 5) provide a period of monitoring, observation and testing to gather data/evidence to inform policy-making.

We therefore promote a self-regulatory approach that comes with innate and significant advantages in terms of administrative efficiency. In a self-regulatory model, the rules are made by those to whom they apply, and therefore are likely to be more effective because they enable a regulation of the spirit, rather than the letter, of the law. In addition, a self-regulatory body can be quicker at rewriting rules than can a government department and can therefore respond more flexibly in dealing with problems and new developments. Self-regulatory approach is also cheap for the government, because the regulated bear the costs of regulating.