18 June 2019

Zunaid Ahmed Palak
Hon'ble State Minister for ICT Division
Government of the People's Republic of Bangladesh
E-14/X, BCC Bhaban, Agargaon, Dhaka-1207, Bangladesh

Subject: Industry submission on Bangladesh Digital Security Act, 2018.

Dear Hon'ble Minister,

On behalf of the **Asia Internet Coalition ("AIC") and its members**, I am writing to express our sincere gratitude to the Ministry of ICT - Information and Communication Technology Division of the, Government of Bangladesh, in its efforts on the **Bangladesh Digital Security Act, 2018 ("BDSA")**, which marks a landmark effort to provide a boost to the burgeoning ICT market in Bangladesh, overhauling the previous Information and Communication Technology Act, 2006 and updating the regulatory regime to be better equipped at addressing the challenges of recent developments in technology.

The AIC is an industry association comprised of leading internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia region. Our members include Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, Grab, LinkedIn, LINE, Rakuten, Twitter, and Yahoo (Oath).

While we commend the government's commitment towards the digital economy enablement in Bangladesh, the underlying regulatory regime poses some serious concerns that we would like to express. These include concerns related to lack of specificity in speech related offences, unpredictable regime for content regulation and takedown notices, gaps in intermediary liability framework, and lack of procedural safeguards. Bangladesh vision to emerge as a developed nation by 2041 has been significantly demonstrated by your ministry, through efforts such as the launch of Bangabandhu-1, enhanced budget to boost digitalization, and job creation in the ICT sector. We understand that ICT is the government's top priority sector and government is providing training and ensuring facilities to meet the goals of Digital Bangladesh.

As part of AIC's legislative development efforts and to continue to support the goals of your Ministry , we wanted to share specific concerns and recommendations on BDSA. As responsible stakeholders in the developmental progress, we appreciate the ability to participate in this discussion and the opportunity to provide input into the policy-making process.

As such, please find appended to this letter detailed comments and recommendations, which we would like to respectfully request the ICT Division to consider. Importantly, we would also be happy to offer our inputs and insights directly through meetings and discussions in Bangladesh.

Should you have any questions or need clarification on any of the recommendations, 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)
www.aicasia.org

Cc.: Hon'ble Minister Mustafa Jabbar, Posts, Telecommunications and Information Technology

Enclosure

(detailed comments and recommendations are provided from next page onwards)

DETAILED COMMENTS AND RECOMMENDATIONS ON BANGLADESH DIGITAL SECURITY ACT, 2018

A. General Comments

The recently enacted Bangladesh Digital Security Act, 2018 ("**BDSA**") marks a landmark effort to provide a boost to the burgeoning ICT market in Bangladesh, overhauling the previous Information and Communication Technology Act, 2006 and updating the regulatory regime to be better equipped at addressing the challenges of recent developments in technology.

The changes in the regulatory regime in Bangladesh are triggered by an exponential growth in connectivity in recent times, leading to new challenges on the usage of social media. Recent studies have shown that as much as 49% of Bangladeshis used the Internet in 2018, marking a leap from 29% as of the same period in early 2017. A key driver of this growth has been visionary policies and access initiatives adopted and implemented by the Bangladesh Government under the collective banner of projects like 'Digital Bangladesh' and A2i. In response to these policies, the size of the Bangladeshi ICT industry is estimated to have swelled from USD 28 million in 2008 to around USD 700 million in 2018. While we appreciate the effort to overhaul existing law to rise to the new challenges posed by increasing digital penetration and the rise of innovative goods and services, we believe that the BDSA should streamline its processes, remove vague and commercially unsound policies, and reflect the legitimate concerns of all concerned stakeholders including the Government, private sector / industry, as well as civil society and academia.

Some of the provisions of the BDSA which give rise to cause for concern are as follows:

a. Speech related offences being vague and unspecific, leading to questions of impingement on constitutional rights;
b. No predictable regime for content regulation and takedown notices;
c. Intermediary liability not at par with global standards;
d. Lack of procedural safeguards in all processes including investigation.

It is important for industry and consumers alike to operate within a clear, predictable, and stable legal environment, and a safe and conducive environment for users to adopt the digital ecosystem. Such a framework must be balanced so as to account for the various legitimate interests involved in relation to use of the digital ecosystem. These include:

a. The interests of users to freely express themselves online including in relation to content creation, communication, and correspondence as guaranteed by Article 39 of the Constitution of Bangladesh.
b. The interests of the Government in providing a safe and facilitative digital environment suited to the needs of users, removing unlawful content, and facilitating the offering of e-governance and digital delivery of public services online.

c. The interests of small enterprises, entrepreneurs, and other commercial entities to carry out business and pursue any trade or profession as guaranteed by Article 40 of the Constitution of Bangladesh.

Given that these interests are ensured under the Constitution of Bangladesh, it is the duty of the Government to adopt an approach to regulation which balances and seeks to harmoniously construe and apply them in practice. This applies equally to the regulation of a transformative medium such as the Internet.

In its present form, the BDSA creates several obstacles to the conducive use of the Internet ecosystem due to several vague obligations, unchecked powers, disproportionate penalties, and unworkable compliance requirements. Within this context, we would like to take this opportunity to communicate our comments in relation to the recently-passed BDSA.

B. Speech-related Criminal Offences

The BDSA contains several provisions that are vaguely drafted, leading a potential for chilling effect on speech. We would like to emphasise the need to have clear, necessary, and proportionate penalties in relation to criminal offences and especially those which have a core impact on key human rights such as free speech.

In this regard, we request reconsideration of the following offences as currently contemplated under the BDSA:

a. **Propaganda**: Section 21 contains the punishment for any type of propaganda or campaign against the Liberation War, the Father of the Nation, National Anthem or National Flag. This provision contains punishment for even those who assist in the carrying out of any type of propaganda or campaign.
While this is no doubt a sensitive issue, the offence – as currently defined – is not sufficiently precise and may also result in disproportionate penalties. This may require further clarification.

b. **Dissemination of offensive / false / fear-inducing information / creating hostility**: Section 25 and 31 of the BDSA contains provisions penalising individuals for content that is:
    - offensive
    - fear inducing
    - intended to annoy, humiliate or denigrate a person
    - tarnishing the image of the nation
    - spread confusion
    - creating hostility among people

    There are several issues with such provisions. Firstly, the understanding of 'offensive', 'fear inducing' and 'annoying' is inherently subjective. The threshold of annoyance or insult varies from person to person and this lends a great deal of vagueness to the provision. Further, the idea of 'spread[ing] confusion' as a barometer to test if an act falls within the contours of the provision, lends primacy to a subjective feeling rather

than actual content, whose interpretations can lead to widely varying outcomes. It is unclear what the executive understanding or judicial determination of these terms will entail. The cumulative impact of such provisions is that it might have a chilling effect on free speech and expression of opinions through digital media – not only impact ordinary users but also stymie the growth of healthy journalism.

In this context, the Indian example would serve to highlight the deficiencies of this provision. A similarly worded provision of Indian law – that is, Section 66A of the Information Technology Act, 2000, prescribed content held to "annoying" and "insulting" (among others) as wrongful. This provision was struck down by the Indian Supreme Court for being "open ended, undefined, and vague" and the words used in the text of the provision being "nebulous in meaning".

It is important that the digital space be permitted to serve as an arena for diversity of views and freedom of expression, allowing citizens to use them as channels of communication with their peers and other users of the Internet. Thus, it would be recommended to issue clarifications making such provisions more pointed and clear, with appropriate safeguards to the process determining liability, so as to avoid overarching criminalisation.

c. **Cyberterrorism**: Under Section 27, the offence and punishment for cyber-terrorist activities is provided, and it makes damaging or destroying supply of daily necessities or services of public products or causes adverse effects on Critical Information Infrastructure an offence under the BDSA. However, it is not clear as to what kind of impediment to supply of daily necessities/ services can be effected through a digital medium, and more clarity is required on this front. In its present form, the provision is vague.

d. **Hurting Religious Sentiments**: While again a sensitive issue which merits consideration, Section 28 of the BDSA takes the approach of punishing anything that could be construed as "hurting religious sentiments" – without linking it to any actual threat. As the range of content that could be considered hurtful by a variety of religions would differ widely, it is recommended that a law carrying penal consequences should closely tie in said penalties only to any actual threat or discrimination.

e. **Defamatory Content**: The BDSA in Section 29 penalises defamatory content without linking the same to an actual offence of defamation in law, and without clearly setting out the standards for what may constitute defamatory content under law. As the vast majority of content on the internet could be considered to be in the nature of commentary on others, be it political reporting or satire or any kind of journalism – this provision could serve as an impediment to important democratic expression.

While revaluating the above provisions to being them in line with the norms of a constitutional democracy, we would request the Government of Bangladesh to bear in view the well-established tenets of international human rights law recognised by instruments such as Article 19(3) of the International Convention on Civil and Political Rights. Under this, restrictions on speech must satisfy the conditions of:

a. **Legality:** Restrictions should be provided by law, and limiting government discretion in a manner that distinguishes between lawful and unlawful expression with "sufficient precision".

b. **Necessity and Proportionality**: States must demonstrate that the restriction imposes the least burden on the exercise of the right and actually protects, or is likely to protect, the legitimate State interest at issue. States may not merely assert necessity but must demonstrate it, in the adoption of restrictive legislation and the restriction of specific expression.

c. **Legitimacy**. Any restriction, to be lawful, must protect only those interests enumerated in Article 19 (3): the rights or reputations of others, national security or public order, or public health or morals – and should not be open ended and broad ranging.

C. Content Regulation

We would like to submit that the BDSA should put in place a predictable regime for content regulation – including through an established procedure for serving content takedown notices on private parties, following a duly reasoned order and having adequate procedural safeguards to avoid misuse.

At present, Section 8 of the BDSA provides that the Director General of the Digital Security Agency ("**DSA**") can request the Bangladesh Telecommunications Regulatory Commission ("**BTRC**") to remove or block any information or data published on a digital medium if it threatens breach of digital security. If it appears to law enforcement agencies that any information or data undermines the solidarity of the country, economic activities, defense, religious morality or public order, etc., they too can request the BTRC through the Director General to remove or block such information. The BTRC then has to remove access to the data. As the BTRC only has limited jurisdiction, this is not a requirement that is likely to be applicable to all service providers, but rather only to those entities (such as telecom and internet service providers) that the BTRC has jurisdiction over, which is also restricted to the territory of Bangladesh.

We believe that the powers of the relevant agency with jurisdiction over service providers or intermediaries should be expanded to include the service of binding takedown notices. This could be notified under the rules specified in Sections 5(3) and 8(4) of the BDSA, or the DSA could be provided with such authority by a legal amendment.

However, there is also a need to build in provisions for checks and balances, a scope for assessment of the legality of the blocking order, and the possibility of review and appeal. In relation to the same, we recommend the following:

a. Blocking orders must be issued only where there is a valid court/judicial finding that the content in questions violates Bangladeshi law (with evidence and reasoning sufficient to document the legal basis of the order);
b. Blocking orders must be resorted to only where there is no alternative method/recourse available to remove access to the content; and

c. Blocking orders must be in writing, reasoned, and be narrowly scoped to specific URLs or content.
d. Where applicable, the time period for which the content should be restricted, should be indicated.

A social media service provider should not be held liable for any non-compliance if the order in question does not follow these procedural safeguards and due process requirements.

D. Intermediary Liability

Section 38 of the BDSA seeks to introduce the concept of intermediary liability. Intermediary liability is a core principle of the global Internet as we know it today, incorporated into the digital laws of almost every country. An enabling regulatory framework in this regard is crucial, given the major contributions made by intermediaries in elevating the role of the internet as a primary channel for the exchange of information, ideas, trade and commerce.
The guiding principles that are globally followed in this regard are encapsulated in the Manila Principles which broadly state that:

a. Intermediaries should be shielded from liability for third party content;
b. Requests for imposition of restrictions on content must be clear, unambiguous and follow due process of law, and they must comply with the tests of necessity and proportionality;
c. Laws providing for content restriction must also follow due process of law; and
d. Transparency and accountability must be built into the process of requesting content to be taken down or blocked.

Section 38 of the BDSA states that intermediaries will avoid liability under the BDSA and any of the provisions thereunder for facilitating passage of information or data which would otherwise amount to an offence, if it is proven that the concerned violation was committed without their knowledge or that they had taken all measures to prevent the occurrence of the offence.

There are several key concerns with this framing of the law, and they fall short of the guidelines offered by the Manilla Principles in several key respects. The key issues with framing of the provision are highlighted below:

a. The framing of this safe harbour is inadequate as it *only applies to offences and contraventions under the BDSA itself*. It does not apply to other civil, criminal, or regulatory frameworks which may operate to regulate content and create liability. For an intermediary liability protection to be effective, it must account for liability from all forms of regulatory frameworks and not merely liability arising under the BDSA itself.

b. In addition, there is a need for greater clarity in relation to the safe harbour provisions relating to knowledge and precautionary measures – which are loosely framed and may require intermediaries to proactively remove content in the absence of a valid request from an independent authority. The failure to include the requirement for independent adjudication of the legality of content will result in harmful effects for speech as private

sector efforts to remove content based on abusive requests – something which, despite reasonable protections, will invariably result in legal/lawful content being mistakenly removed.

c. The law in its present form could be interpreted in such a manner as to entirely subvert the intention of limiting intermediary liability. Intermediaries are exempt from liability usually because they do not actively monitor all content that is communicated through their platforms. If the law fixes "knowledge" as a criteria for fixing liability, this makes it difficult to determine whether the law is implicitly placing a responsibility of actively monitoring all content on the intermediary, to assess what is legal content and what is not (please note that this has to be read in light of the fact that even posting content that "annoying" or "insulting" or "offensive" is illegal under the BDSA).

   Constant monitoring as regards content is often unfeasible from a technical perspective, as well as a violation of the right to freedom of speech and privacy of users.

d. The law also places a burden on the intermediary to prove that there was no knowledge and that "all possible steps to stop the commission of an offence" had been taken. This is a very subjective standard and a high burden of proof. The idea of intermediary liability being limited means that the *default* assumption is that the service provider was not liable as long as they did not modify the content in any way and merely provided a platform. Therefore the present wording of this provision entirely subverts the concept on intermediary liability as it is understood in most other legal jurisdictions of the world.

We recommend that the provision be edited to bring it in line with the global standards enumerated above, and remove the ambiguities highlighted herein.

E. Other Notable Provisions

- **Lack of procedural safeguards in investigation:** The investigative powers provided under the BDSA, particularly in Sections 41 and 43, are wide ranging, including scope for confiscation, collection of data, information and traffic data from 'any person' – without providing procedural safeguards as to how such information access requests should be structured and responded to. Further, Section 46 which provides for 'help in investigation' simply states that the investigation officer who conducts any inquiry may request any information or assistance and the service provider will be 'bound to' help the officer.

  In the interest of a predictable regime of law enforcement access to data, we recommend removing these provisions and replacing them with clear procedures mentioning who can request what level of information, scope for review and response, nexus between investigation and information sought, and appropriate security measures applicable to information sought.

  Any order of the investigative authority should be in writing, backed by judicial authorisation, contain a reasoned request, and there should be safeguards to ensure that

this provision is not utilised in ways that go against the spirit of citizen privacy and freedom of business and commerce.

- **Extra-Territorial Application**: Section 4(1) of the BDSA states that if any person commits any offence under the BDSA outside Bangladesh, which, if committed in Bangladesh would have been punishable under BDSA, then the BDSA shall be applicable to it in the same manner as if such offence had been committed in Bangladesh.

  This provides for complete extra territorial application, with no linkage at all to Bangladesh. In this context, the scope for prosecution has been made too wide. Ideally, the scope of the provision should be limited to a situation where computers from Bangladesh are used to commit the offence, or are otherwise involved, or if the offence is committed from within Bangladesh. In this connection, the relationship between Section 4(2) and 4(1) would need to be appropriately clarified.

- **Abetment**: The law does not provide any definition of what constitutes abetment, while affixing liability at par with the principal offence. This, read with the diminished limitation of intermediary liability, and very vague statements of offences, could result in undue burdens on companies that provide platforms for users to upload and create content.

F. Conclusion

In conclusion, while the aim of the law is commendable, there are several provisions that would greatly benefit from additional clarity through rules and regulations, or amendments where necessary. Any regulatory intervention that is too onerous or restrictive will impede the role of the internet in assisting communications, knowledge-building, governance, innovation and commerce. Guiding principles to keep in view while regulating content online, are as follows:

"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 in dependent 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." (UN Special Rapporteur on Promotion and Protection of the Right to Freedom of Opinion and Expression)

In keeping with the aim of harmonious integration of the Bangladeshi digital economy with the rest of the world's, we have provided inputs that should help bring these laws into step with global best practices, while continuing to address the specific concerns of the Bangladeshi Government. We remain committed to assisting the Government in ensuring a balanced framework for digital security in Bangladesh and are happy to discuss our comments in further detail.