U.S. CHAMBER OF COMMERCE
U.S.-Bangladesh Working Group

ASIA INTERNET COALITION

July 10, 2020

Mr. Zunaid Ahmed Palak
Honorable State Minister
Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology
Government of the People's Republic of Bangladesh

SUB: Industry Submission on the Draft Information Privacy and Security Rules, 2019

Dear Honorable Minister,

On behalf of the Asia Internet Coalition ("AIC") and the U.S. Chamber of Commerce ("Chamber"), we are writing to express our sincere gratitude to the Government of the People's Republic of Bangladesh ("GoB"), and in particular the Information and Communication Technology Division ("ICT Division"), for its efforts to bolster the legal and regulatory regime on data privacy in Bangladesh. In particular, we welcome the initiative taken to draft the Information Privacy and Security Rules, 2019 ("Privacy Rules"), to further upgrade the regulatory framework in Bangladesh.

The AIC is an industry association comprised of leading internet and technology companies and is committed to promoting the understanding and resolution of the internet and ICT policy issues in the Asia-Pacific region. Our current members include Airbnb, Amazon, Apple, Booking.com, Expedia Group, Facebook, Google, Grab, LinkedIn, LINE, Rakuten, Twitter, and Yahoo!.

The Chamber is the world's largest business federation, representing the interests of more than three million enterprises of all sizes and sectors. The Chamber is a leading business voice on digital economy policy, including on issues of data privacy, cybersecurity, digital trade, artificial intelligence, and e-commerce. In the United States and around the world, we support sound policy frameworks that promote data protection, support economic growth, and foster innovation.

We commend the GoB's commitment to the objectives of *Digital Bangladesh*. These efforts in strengthening the legal and regulatory framework are timely and necessary, driven largely by the visionary policies and initiatives adopted and implemented by the GoB, at a time when Bangladesh is experiencing exponential growth in connectivity and digital technology. We support these efforts and would like to share private sector feedback on the draft Privacy Rules. Please find appended to this letter detailed comments and recommendations, which we request the ICT Division to consider.

We appreciate the opportunity to participate in discussions with the GoB and provide industry input into the policy-making process. We would be happy to offer our inputs and insights directly through meetings and participating in the official consultations as well.

U.S. CHAMBER OF COMMERCE
U.S.-Bangladesh Working Group

ASIA INTERNET COALITION

Please do not hesitate to have your teams contact Sid Mehra (smehra@uschamber.com) and/or the AIC Secretariat Sarthak Luthra (secretariat@aicasia.org). Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition

Nisha Biswal
Senior Vice President, South Asia
U.S. Chamber of Commerce

Enclosed:

1. Enclosure A: Detailed comments and recommendations on the draft of the Information Privacy and Security Rules, 2019

U.S. CHAMBER OF COMMERCE
U.S.-Bangladesh Working Group

ASIA INTERNET COALITION

Enclosure A

DETAILED COMMENTS AND RECOMMENDATIONS ON THE DRAFT INFORMATION PRIVACY AND SECURITY RULES, 2019

A. General Comments

The *Constitution of Bangladesh* ("**Constitution**"), adopted on November 4, 1972, guarantees the right to privacy of correspondence and other means of communication of every citizen of Bangladesh, subject to certain qualified restrictions. This provision of the Constitution codified an important right which, in an era of burgeoning data proliferation and growth in connectivity, appropriately serves as a basis for a future data protection ecosystem. Indeed, if enacted, the *Information Privacy and Security Rules*, 2019 ("**Privacy Rules**" or "**Rules**") will operate as Bangladesh's first comprehensive privacy framework.

This submission sets out the key topics in the current draft of the Privacy Rules together with recommendations based on an international benchmark of privacy laws, regulations, and standards. These include the European Union's *General Data Protection Regulation* ("**GDPR**"), Japan's *Act on the Protection of Personal Information* ("**APPI**"), the Asia-Pacific Economic Cooperation *Privacy Framework*, and the Organization for Economic Cooperation & Development's *Privacy Principles*. We refer to these together as the "**International Benchmarks**".

In general, the Privacy Rules, as written, are unable to comprehensively address contemporary data privacy concerns and would benefit from harmonization with globally accepted standards referenced in the International Benchmarks. We believe further amendments to the draft Privacy Rules are critical before these are published in the official Gazette.

Aspects of the draft Privacy Rules which are of concern include:

- Extraterritoriality provisions which create an unduly broad territorial scope;
- Narrow legal bases for cross-border data transfers and unclear relationship with existing rules governing cross-border data flows;
- Extensive use of undefined terms and expressions, which creates ambiguity and unpredictability, including the definitions of "data processor" and "sensitive personal information" which are inconsistent with International Benchmarks; and
- Unclear and duplicative provisions relating to consent and notice requirements.

In addition, the draft Privacy Rules do not clarify existing issues with Section 26 of the *Digital Security Act of 2018* ("**DSA**"), namely the expression "without lawful authority", which continues to remain undefined. In the absence of proper guidance, this provision has potential for broad interpretation and therefore should be defined subject to sufficient qualification, exceptions or exemptions so as to avoid frivolous and vexatious claims. For example, Section 26 should not extend

to collection or possession of identity information available in the public domain or where conducting any lawful trade or business.

In order to promote the growth of *Digital Bangladesh* and to participate effectively as a leading player in the global digital ecosystem, Bangladesh should create a legal framework that is aligned with global standards and best practices; provides GoB, industry and consumers the ability to operate within a clear, predictable, balanced, and stable legal environment; promotes good data governance; and enhances confidence.

B. Detailed comments and recommendations on the draft Privacy Rules

a. Extra-territoriality

Rules 3(1)(b) and (c)

The Privacy Rules are intended to apply to all those that "carry out information processing activities within the territory of Bangladesh or any place outside the borders of Bangladesh," including to those that are "not registered as a commercial entity in Bangladesh…and [do] not supply goods within Bangladesh". The extraterritorial scope of the Privacy Rules is unduly broad and effectively covers any entity worldwide that processes personal information. There is no requirement of a nexus with Bangladesh for the Rules to apply, which is unusual and inconsistent with the International Benchmarks.

While it is important to ensure the robust protection of data privacy of persons within Bangladesh, unfettered extraterritorial scope will be practically difficult to enforce, will create conflict of law issues and will not be aligned with both national and international approaches to territorial scope. The application of the Privacy Rules should be confined to data controllers and processors established within Bangladesh.

b. Definitions of "Data Regulator" and "Data Processor"

Rule 2

The terms "data regulator" and "data processor" should be defined clearly, so as to prevent any confusion about the scope of each term. There is no need to use the term "personal data regulator" separately, as it will be covered within the definition of a "information regulator." The definition of the term "organization" can also be removed as the definitions of "information regulator" and "data processor" will capture all entities. We suggest that the terms "information regulator" (also known as a "data controller") and "data processor" are defined in accordance with equivalent terms in existing data protection laws in other countries, such as the GDPR. This will ensure consistent terminology across laws of different countries and will align the Privacy Rules with International Benchmarks.

Rule 2(e)

"Data processor" is defined to include employees of a data regulator as well as "independent processor operating under any personal data regulator". However, employees that process personal data within an organization are generally considered to do so on behalf of the organization and, as such, an employee would not be classified as a "data processor" separate from the organization in question. By treating employees as data processors, the Privacy Rules would impose unnecessary direct obligations on each employee as an individual. For example, Rule 14(2) imposes a requirement for data processors to take appropriate security measures to protect the information in their custody. This, therefore, imposes direct obligations on each individual employee who handles personal information on behalf of their employer to secure the data, which is inconsistent with international practice. **Such security measures should be the responsibility of the data controller/employer. Imposing direct obligations on employees is onerous and may result in a reduced willingness for global companies to operate in Bangladesh.** Accordingly, employees should be omitted from the definition of "data processor". Further, the phrase "operating under any personal data regulator" is unclear and we suggest that this wording be aligned with the wording in Article 4 of the GDPR, which defines processors as those that "[process] personal data on behalf of the controller".

c. **Definition of Personal Information**

The definition of personal information might be framed as: "information reasonably linkable to an identifiable individual or to a device associated with an identifiable individual and does not include:

- Anonymized information
- Aggregated information
- Pseudonymized information
- Employee data
- Public information, which includes information which a person makes public
- Generated information"

d. **Processing of Sensitive Personal Information**

Rules 4, 7 and 20

The definition of "sensitive personal information" includes passwords and bank account or credit/debit card or other payment instrument details or records of financial transactions. The definition of sensitive personal information should encompass personal information which is more sensitive and of a higher risk to individual privacy and should not include, for example, passwords, and financial transaction data. Not all types of financial transaction data are always more sensitive to individual privacy.

In line with the GDPR, we recommend that Rule 20 be revised to allow for processing of sensitive personal information on such grounds other than consent, including: (i) for employment, social security and social protection purposes; (ii) where processing is necessary for the

public interest; (iii) where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; and (iv) where processing is carried out in the course of legitimate activities with appropriate safeguards by the entity.

Rule 20(1) states that sensitive personal information may not be collected or processed unless express consent is obtained via letter, fax, email, or in writing. While requiring express consent for sensitive personal information is broadly aligned with the International Benchmarks, the overly prescriptive means through which such consent must be obtained is not and creates a risk of "consent fatigue" for organizations and data subjects. In many circumstances, it may be impractical or unnecessary to obtain express consent. It should be incumbent upon the data regulator to demonstrate that the data subject has given consent and to facilitate the provision of that consent in a way which is appropriate to the service offering and the user experience.

Rule 20(3) also states that sensitive personal information collected by an entity may be 'examined' under certain circumstances. However, the meaning of 'examination' is unclear and will create significant regulatory uncertainty. The meaning and standards of examination should therefore be clarified.

Rule 20(4) requires data regulators and data processors to be responsible for ensuring that sensitive personal information is subject to enhanced security measures. However, organizations should be permitted to ensure that the manner in which consent is obtained is appropriate. Furthermore, the law should be technology-neutral to future-proof against other technologies that may not yet be available, but which may be more effective in obtaining express consent.

Rule 7 states that "each person shall have the final power to determine the method of distribution for the purpose of rule 4". It is not clear from the wording of this provision what the intention and purpose behind this rule is and whether this means that data subjects have a right to stop, or withdraw consent to, any processing of their sensitive personal information. This provision may also undermine the requirement for data subjects to give explicit consent prior to the collection or processing of their sensitive personal information, suggesting that this is not "true" consent since Rule 7 implies that organizations would otherwise determine the method of disclosure of such data. This provision should be revised to eliminate the resulting uncertainty for organizations as to whether they can rely on consent from data subjects and the extent to which an organization can disclose such data.

e. Cross-Border Transfers of Personal Information

Rule 25

Rule 25 sets out a very limited legal basis for the transfer of personal information and sensitive personal information outside of Bangladesh specifying consent as a necessary requirement for such transfer. This is far narrower than comparable privacy regimes around the world such as the GDPR and is likely to significantly impact routine operations of entities given that a requirement for "unambiguous" consent to overseas transfer of data is a very high threshold to satisfy.

The free movement of data underpins the digital economy and plays a fundamental role in ensuring data-driven growth and innovation. The effective and efficient functioning of data processing across borders is a fundamental building block in any data value chain. Allowing for cross border transfer of data is essential for aiding in international technology transfer processes and to ensure that Bangladesh's growth and potential is met from a technological standpoint. The Rules should clarify that consent is one basis for transfer but is not required for all transfers, in line with the APEC Cross Border Privacy Rules Framework and OECD Privacy Principles. Under those frameworks, data transfers are permitted as long as the data regulator remains accountable for protecting the data regardless of geographic location.

The Rules should leverage international data transfer standards and contracts to ensure interoperability with global standards (the APEC Cross-Border Privacy Rules offer a multilateral cross-border data transfer framework that Bangladesh can consider joining). An example would be Article 24 of Japan's APPI, which imposes restrictions on the transfer of personal information of Japanese citizens to third parties in foreign countries except when a third party has established a system which meets the Rules of the Commission to "continuously implement equivalent necessary measures." These regulations for implementing Article 24 specifically call out a company's APEC Cross Border Privacy Rules ("CBPR") certification as satisfying this requirement. The Rules should also include certifications as mechanisms for ensuring that data is transferred in accordance with high privacy standards. Under such an approach, a data controller that demonstrates to an independent third party certifier that it complies with specific requirements should be allowed to transfer data outside of Bangladesh without consent of the individual or by relying on another method.

Finally, while the Privacy Rules will serve as Bangladesh's first comprehensive data protection regime, there are nonetheless existing rules in place governing cross-border data transfers from Bangladesh, including at the sectoral level. We request that the relationship between the Privacy Rules and the existing data transfer regime be clarified and, where conflicting obligations arise, that they be resolved in favor of open data flows.

f. Consent and Notification ("confidential notice")

Rules 6(2), 6(3), 6(4), 8, 16, 18, 19 Schedule II

Consent: There appears to be a general obligation in Rule 6 to only collect, use or process personal information where consent has been obtained.

In Rule 18(1), there is a requirement that when "collecting information for multiple purposes, each purpose must be presented separately and consent must be given with regard to all the purposes". However, many companies process user personal information for multiple purposes, which are usually described in a user-facing privacy notice. While we assume that this Rule allows a company to describe each purpose separately and obtain one consent to all stated purposes, the wording is not clear. As

drafted, the Rule could possibly be interpreted as requiring *separate* consent for each *separate purpose,* which would not be practical.

Rule 19 also sets out what appears to be further exceptions to the consent requirement. These exceptions to consent should align with the alternative lawful bases of processing under the GDPR and should include, at a minimum, a "legitimate interest" basis of processing.

Notice: Rules 8, 16 and 18 contain overlapping requirements regarding the notice that must be provided to data subjects. Broadly, before collecting or processing personal information, organizations must provide data subjects with a "confidential notice" containing the information set out in Schedule II (both in English and in Bengali). The "confidential notice" must be unbundled and easy-to-understand. All notice requirements should be consolidated and overlapping provisions removed. Further clarification is needed around why the notice to be provided is a "confidential" notice. Additionally, the detailed requirements in Schedule II are too prescriptive and may result in notice-fatigue for data subjects given the amount of detail that must be provided in Schedule II for each collection of personal information. Streamlining this to only include the types of personal information and purposes of processing would allow organizations greater flexibility on how the notice should be presented to individuals.

g. Disclosure of Personal Information

Rules 21, 24

The Privacy Rules provide that personal information may only be disclosed to a third party where the data subject has provided written consent, where it is necessary pursuant to a contract between the recipient and data subject and where the recipient complies with the Rules. These disclosure requirements are onerous and unusual. Organizations often need to disclose personal information to service providers and other third parties to provide their products and services and to operate. This is entirely compatible with the purposes of the data processing. Further, these requirements do not align with general business practices or with International Benchmarks. The Privacy Rules should be amended to permit disclosure to third parties as long as it is compatible with the original purpose. This balances individual privacy with business efficiency.

h. Security Safeguards

Rule 14

Rule 14 imposes an obligation on data processors to implement security safeguards. While many data processors implement security safeguards in a manner consistent with industry and global best practices, it is nonetheless out of line with International Benchmarks to place specific legal obligations on data processors. Data processors do not always have control over the data or visibility over the nature, scope, and purpose of processing of such data, and are unable to ascertain the risk of harm to data subjects. Data processors are therefore not in a position to make meaningful or independent decisions about the collection, usage, processing or disclosure of personal information -

rather, their scope is generally limited to implementing the decisions of the data controller. Accordingly, any statutory obligation to implement security safeguards should be vested with the data controller. We therefore recommend that the references to data processors should be removed from Rule 14.

i. **Data Breach Notification**

Rules 13, 27, 31

There is a general requirement in Rule 13 for data subjects to be notified of the "danger/risk" of a personal information breach within seven days. There is also a requirement in Rule 27 for a data regulator and data processor to notify both the Agency and the data subjects of any general data (more broadly defined than personal information, as discussed above) breach of the same within 7 days. There is a further overlapping requirement in Rule 31 for data regulators, data processors and all third parties to notify those affected by data breaches caused by "cyber attacks" within 7 days. It is unclear if "cyber attacks" are the same as "cyber incidents" defined in Rule 2(o).

The three different provisions covering data breach notifications are overlapping and should be streamlined and consolidated for clarity. Requiring notification to data subjects and the regulator for every data breach may result in notification fatigue for data subjects and an undue administrative burden for regulators. This would de-sensitize data subjects to the impact of such breaches and would not allow the regulator to allocate appropriate responses to investigating and addressing harmful breaches. Accordingly, a minimum risk-based threshold should be introduced before a breach becomes notifiable, for example a requirement that a data breach is likely to cause serious material harm to affected individuals. It would also be beneficial to allow for more flexibility in the timeline for reporting. While timely notification is important, it is more important that organizations are able to present the facts fully and accurately and focus on breach mitigation. A prescriptive 7 day timeline may not always be appropriate – this could be too short in some cases where further investigation is required. Notification should not be required for disclosures or breaches if the data is encrypted or anonymized; does not cause or is not likely to cause any harm to the user; is a result of employee access in good faith and if the data is not further disclosed; the data is in public records.

Moreover, we note that processors may not have visibility over the nature or type of information of data regulators being processed, meaning that they would not be able to distinguish between an intentional movement of data or a security incident, let alone whether a data breach involves personal information. Finally, data processors do not have direct relationships with data subjects and would therefore not be able to meaningfully or effectively communicate matters relating to a data breach to them. Data processors should instead have the responsibility to notify data regulators of confirmed data breaches, in a reasonable timeframe in the specific circumstances, and in accordance with their contractual agreements. The responsibility of notifying the affected information provider or the relevant regulatory authorities should therefore ultimately reside with the data regulator.

j. Transition period

Rule 1(2)

The Privacy Rules are intended to come into effect immediately following publication in the official Gazette. The lack of a transition period for organizations to comply with the Privacy Rules is not practical and may result in widespread non-compliance at the start due to a lack of awareness. We note that GDPR provided companies with a two-year transition period, despite having experience with the *Data Protection Directive*, an earlier regulation in place since 1995. Consequently, the EU had the benefit of a network of experienced data protection authorities and a substantial body of legal guidance in place *before* GDPR was even enacted. In contrast, the Privacy Rules will serve as Bangladesh's first comprehensive data privacy regime, and the Government will need to invest significant time and resources to build its monitoring and enforcement capabilities. Allowing a transition period of at least two years will enable organizations and the Government to put in place systems and procedures to enable compliance with the new laws.

k. Requirement to Formulate Policies for Data

Rules 2(c) and 5

Organizations must put in place "policies for collecting, receiving, storing and managing *data*". These policies must be published on the organization's website and be available for information providers (data subjects) to access. The policies should also set out the purpose of collection and use of the data and the security measures taken to protect the data.

The policies that must be put in place appear to encompass more than just personal information. "Data" is defined separately from "personal information" in Rule 2 and means any "formally prepared information, knowledge, facts, concepts or instructions that has been processed, or is being processed, or will be processed in a computer system or computer network in any form or format, including computer printout, magnetic or optical storage media, punch cards, punch tape, or which is stored internally in a computer's memory". As such, the policies to be issued are both wider (in terms of the inclusion of non-personal information) and narrower (since they only relate to formally prepared data on a computer network or system) than usually required by other International Benchmarks. As currently drafted, there is some ambiguity as to what will constitute data (for example it is unclear whether unprocessed or raw data fall within this definition). While having general data policies is important for any organization, there is limited benefit to making these available to data subjects since non-personal information has limited privacy impact for them. This obligation should only apply in respect of "personal information", in line with the requirements of other International Benchmarks.

l. Protection of Personal Information

Rules 28 and 37

The relationship between the provisions in Rules 28 and 37 is not entirely clear. Rule 28 requires organizations to implement appropriate security measures in consultation with the Agency

and in accordance with the "manner and nature of security prescribed in government notifications". **The requirement to consult with the Digital Security Agency is onerous and would result in an undue administrative burden for both organizations and the Agency. This consultation requirement would extend the time required for a business to comply with the Rules and could impact Bangladesh's attractiveness to both local and global businesses wishing to establish privacy-compliant operations.** Furthermore, it is unclear what metrics the Agency will use to assess these measures, and the extent of the Agency's involvement in designing these measures. Further, what constitutes maintenance of "reasonable security" under Rule 37 is ambiguous and indeterminate. For instance, the concepts of "security measures", "detailed information security program" and "actual security" are not clearly described and terminology is inconsistent (variously referring to agency / company / person etc.).

The prescriptive security standards in both Rules 28 and 37 are arbitrary and increase compliance costs for organizations. For example, Rule 37 prescribes "IS / ISO / IEC 27001" as the requisite standard, but also it leaves open for the Agency to issue Standard Operating Procedure and for the GoB to set the standards and criteria from time to time, which would create compliance issues for businesses. The measures taken to protect personal data should be proportionate to the nature of the personal data and the types and purposes of processing. There is no "one-size-fits-all" solution. For example, a small store running a simple membership loyalty program cannot be expected to implement the same security controls to protect the personal data it collects as a healthcare company that deals with thousands of patient records every day.

Rule 37 also requires the "data collection and processing company" to arrange an annual audit by an auditor appointed by the GoB, with the audit report to be sent to the Agency who may issue instructions. The frequency, nature and the standard of audit is not specified. Importantly it is unclear what an audit would entail, and could potentially require the audited company to provide sensitive and confidential business information to the auditor. This obligation will be onerous for organizations and the Agency alike and should be removed.

m. **Data Subject Rights**

Rules 9, 10, 11 and 12
Access (Rule 9): Each person has a right to access their personal information and receive a copy "in accordance with Schedule II". However, Schedule II refers to the notice requirements therefore it is unclear what the intention behind this is provision and it should be removed.

Correction (Rule 10): Each person has the right to correct their personal information where it is unclear or incomplete. Amendments must be made by the data controller as prescribed by the government and completed within 60 days of the request. Given the varying structures of all organizations that will be subject to the Privacy Rules, requiring both small and larger companies to comply with the same correction process (regardless of resourcing) would not be appropriate. The 60 day timeframe is also overly prescriptive and should be more flexible. Inspiration can be taken

from Singapore's PDPA which permits a longer response time as long as the data subject is notified within 30 days of when the request will be fulfilled. Moreover, under this rule, a data processor may be required to implement a data subject's request to make amendments to their personal information where it is unclear or incomplete. However, this is a function that can only be performed by data regulators and not processors. We recommend that obligations related to this and other data subject rights rest on data controllers, not processors.

Deletion (Rule 11): The data controller must delete personal information where the purpose has been fulfilled, consent has been withdrawn, it was collected illegally, or it has been ordered by a court. There are limited exceptions. This right should be consolidated with the requirements on retention of personal information and that further exceptions to this deletion requirement be introduced.

Data portability (Rule 12): Following experiments in other jurisdictions, the GoB has proposed to grant its citizens an explicit right to data portability. It is important to ensure that its implementation does not pose risks to individuals and businesses. Any proposal related to data portability should be clearly articulated and weighed against considerations of confidentiality, intellectual property, and data security.

Rule 12 should include exceptions, if giving effect to this right would:

- disclose trade secrets or proprietary info;
- compromise privacy, security or integrity of the individual seeking to port their data and of third parties whose data might also be included;
- be infeasible on technical grounds or require disproportionate effort;
- require re-identifying or otherwise linking information that is not presently considered personal information;
- interfere with law enforcement, judicial proceedings, investigations;
- undermine efforts to guard against, detect, or investigate malicious, unlawful, or fraudulent activity or enforce contracts; or
- violate laws or the rights of others.

n. **Retention of Personal Information**

Rules 22 and 23

These provisions contain overlapping obligations relating to the retention of personal information, but broadly, they require that personal information must not be retained once the purpose has been fulfilled and must then be destroyed immediately, unless the data subject has consented to storage for a longer period of time or it is required for historical, statistical or research work. In order to align with International Benchmarks, this obligation should take a more realistic and reasonable approach by allowing for expeditious deletion of data and should incorporate further exceptions to the retention limitation requirement, such as where required for "legal and business purposes" as provided under Singapore's PDPA.

o. **'Miscellaneous' provisions - Information Gathering Powers**

Rule 38

Information regulators and processors must provide any information requested by the Agency to the body corporate / company. The draft Privacy Rules do not provide exemptions from this broad obligation, nor do they limit the permissible uses of that information once received by the Agency or otherwise provide any safeguards to ensure that data collected by the Agency under this provision is necessary and proportionate to the purpose for which it is being sought. **In the absence of any clear guidelines or safeguards on the implementation of this provision, there is ample scope for misuse, which could have adverse effect on a data regulators' and/or content creators' proprietary rights and legal obligations under the laws of other jurisdictions.** Information gathering powers of this kind also create significant conflict of laws issues. For example, U.S. companies are prohibited from complying with any data requests from Bangladeshi law enforcement, unless a U.S. court issued an order in response to a letter rogatory. In the interest of a predictable regime of law enforcement access to data, we recommend reformulating these provisions to address conflict of laws issues and to provide a rights-respecting framework for surveillance requests which draws upon international norms.

p. **'Miscellaneous' Provisions – "Good Faith" Clause**

Rule 39

Rule 39 of the draft Privacy Rules prevents legal action being taken against the GoB, the Director General of the Agency or any other person appointed by the Agency in relation to any action or process initiated under the Privacy Rules in good faith. However, an assessment of whether an action was taken in good faith is inherently subjective and fact-dependent, and can be undertaken by commencing legal proceedings. In any event, this provision cannot prevent any person aggrieved from commencing judicial review proceedings under Article 102 of the Constitution, making the provision redundant. We recommend deleting this provision in its entirety.

C. Conclusion

We commend the aim of the draft Privacy Rules and appreciate the opportunity to engage in a constructive way to develop and strengthen the rules aimed at supporting and enhancing Bangladesh's data privacy regime. We have outlined several provisions, which would benefit from additional precision and consideration through amendments to the draft Privacy Rules. Any regulatory intervention that is too onerous, or wordings that are inarticulate, or legislation inconsistent with internationally accepted standards in a global ecosystem would impede the role of online service providers in assisting communications and connectivity, driving commerce and knowledge-building, and sustaining innovation and governance. Consistent with the constitutional principles of Bangladesh, and with the objective to allow harmonious integration of Bangladesh's digital economy with the rest of the world, the suggestions and recommendations above are intended to assist the efforts of the GoB to advance data protection regulation in Bangladesh that considers global best practices in the context of local concerns.