6 February 2019

To
Mr. Laxmi Prasad Yadav
The Director General
Ministry of Communication and Information Technology
Department of Information Technology
The Government of Nepal

Subject: Industry Submission on the Draft Information Technology Bill, 2075 (2018), Nepal

On behalf of the Asia Internet Coalition (AIC) and its members, I am writing to express our sincere gratitude to the Government of Nepal, for the opportunity to submit comments on the Information Technology Act, 2018 ("IT Act"). Headquartered in Singapore, AIC is an industry association comprised of leading internet and technology companies in the Asia Pacific region and with an objective to promote the understanding and resolution of Internet and ICT policy issues in the region. Our current members are AirBnB, Amazon, Apple, Expedia Group, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Oath).

AIC welcomes the attempts by the Government of Nepal to introduce a comprehensive information technology legislation. We believe that the Information Technology Act, 2018 ("IT Act") proposes to introduce some important principles of law that would go a long way in bringing the legal regime of Nepal at par with global best practices. However, in order to ensure that the stated aim of the law are adequately reflected in the word of the law, and to facilitate the continuing spurt of growth of new and innovative information technology services in Nepal, we have highlighted a few concerns with regard to the provisions of the proposed IT Act.

As such, please find appended to this letter detailed comments and recommendations, which we would like to respectfully request the government to consider when reviewing the IT Act.

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. Importantly, we would also be happy to offer our inputs and insights on industry best practices, directly through meetings and discussions.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC) | https://www.aicasia.org

ASIA INTERNET COALITION

Detailed Comments and Recommendations – Information Technology Act, 2018

1. Data Retention Limitation

Section 57 (4) of the IT Act states that: Personal information collected or stored under the law for specific purpose shall be destroyed within 30 days after the purpose or use of the information is completed.

The law imposes an arbitrary time limit of 30 days after which data collected for a specific purpose would have to be destroyed. It is not clear how this strict time limit of 30 days has been arrived at.

There are several key consumer harms that can arise out of such a strict limitation. Some of these are highlighted below:

a. The underlying assumption behind this provision is that data is collected for a single, or multiple well defined, discrete purposes, which are served within a specified time period. In the modern data economy, this is very rarely the case. A few examples will make this clear.

- For service providers in the financial services sector, record keeping is necessary for not only completing the transaction that the customer is seeking to execute, but also for several other purposes such as processing refunds (which may take longer than 30 days), fraud detection, identifying global patterns of fraudulent transactions to improve the security of the services, and so on.
- For social media service providers who monetize data for advertisement revenue, there is a need for processing and analysis of data to identify patterns, which may be impacted by a strict data retention limitation.
- For cross border service providers, the multiplicity of data retention laws that they need to comply with makes it very important to have flexibility in terms of determining how long any data should be stored within their system.
- For possible future litigation purposes, it may be important to store data for a period longer than 30 days.

b. Legal necessity has not been offered as an exception to the data retention limitation provision. There may be many reasons to retain data – to give an example, it may necessary for tax and accounting purposes, or even for the purposes of law enforcement access or future litigation. In the absence of a clear exception clause, there may be unnecessary legal uncertainty created by the possibility of multiple overlapping data retention / data deletion obligations.

In light of these, as long as a consent and necessity-based privacy regime is in place, it may be unnecessary to legally impose a specific number of days by way of a data retention limitation. Thus, we recommend the following changes:

a. The data retention obligation should be reconsidered in its entirety.

b. Even if such a provision were to come into place, 30 days is an extremely short time frame and should be reconsidered in line with global best practices.

   For example, the EU GDPR states that the period for which the personal data is stored should be limited, and that the relevant time limits should be established by the data controller. The data may be periodically reviewed in order to ensure compliance with the data retention policy that has been arrived at by the organization in charge of the data.

c. Further, data may be stored in de-identified form by the organization in charge of the data, and any processing done pursuant to such de-identification should not require deletion as per this provision.

d. Legal necessity (that is, any obligation to retain data under any law in force in any of the countries in which a data collector operates) should be an absolute exception to the data deletion obligation.

2. Intermediary Liability

Section 68(1) of the IT Act states: "*service providers are not liable for…criminal liability [that] arises from any fact or particulars only because they provided access to such information or data or link.*"

One of the conditions for this is that the service provider has "*not selected the user by its own and the Service Provider did not select or altered the information its own*."

The service provider is also obligated to remove any information "*directed by a public agency or tribunal to remove or disable declaring the content as unlawful*."

A proviso to this section states that "*Service Provider's liability is not exempted where the provider is aware the information, data or the link that infringes the provision of existing law or the service provider acts as an abettor of a crime and do assistance to commit such crime*."

This provision seeks to govern the legal liability of intermediaries, and limit it to exclude liability for mere access to content. The concept of limiting intermediary liability is based on global best practices, as the policies governing liability of intermediaries can have a tangible impact on several fundamental freedoms of users, such as the freedom of speech, expression and right to privacy. Therefore, it is commendable that this principle is sought to be included in law.

The guiding principles that are globally followed in this regard are 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
d. Transparency and accountability must be built into the process of requesting content to be taken down or blocked. (Please note that Section 70 provides for blocking orders, and these procedural safeguards would also be relevant in that context.)

While the draft law seeks to import the principle of limiting liability which is desirable for promoting a thriving digital economy, it falls short of the principles of specificity and unambiguity. As it presently stands, the provision would be clearer if the abovementioned principles were built into the law more explicitly. In this regard, our suggestions are as follows:

a. The term "selected the user on its own" is unclear. Several social media platforms target content to specific segments of users based on information provided by users, options selected by users, or patterns of behavior detected by algorithms. Whether the act of providing targeted content based on choice, requirements etc. of the user, would imply that the user has been "selected" by the algorithm, is unclear. In order to remove this ambiguity, we recommend rephrasing this provision such as to remove any reference to "selection." The provision should simply clarify that no liability for unlawful third-party content shall accrue to an intermediary who does not modify the content.
b. Adequate due process safeguards have not been built into the sub-clause (c). Orders for the restriction of content must build in procedural safeguards such as, *inter alia*:
    - Provide a determination that the content is unlawful in the jurisdiction.
    - Indicate the identifier and description of the unlawful content.
    - Provide evidence and reasoning sufficient to document the legal basis of the order.
    - Where applicable, indicate the time period for which the content should be restricted.

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.

c. The phrase "liability is not exempted where the provider is **aware** the information, data or the link that infringes the provision of existing law" (emphasis added) is a broad, overarching provision which – in the absence of any clarification – 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 introduces "awareness" (which is a vague and unspecific term) as a criteria for fixing liability, this makes it difficult to determine whether the law is implicitly placing a responsibility of monitoring all content on the intermediary.

Further, it is not possible, in the absence of a judicial determination, for a private party to be "aware" that any content is unlawful. This introduces a burden of constant monitoring and adjudication as regards content, which 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 offence of "abetment" is also highly unclear. While merely providing access to a link is not likely to be considered as abetment, it is unclear what kind of activities of intermediaries would come under this ambit.

Therefore, while it is commendable that this principle has been introduced in law, we believe that it would serve its stated purpose better if it is modified to incorporate the above suggestions. Furthermore, due process in relation to blocking and takedown orders would make the blocking orders under Section 70 more transparent.

3. Registration Requirements

Section 70 of the IT Act states that social network operators "may" require registration, and unregistered operations "may" be prohibited.

The proposed provisions by the use of the word "may", creates uncertainty with respect to the manner in which the provision will be implemented. Specifically, it is not clear under what circumstances the registration will be required by the Government and what considerations will be taken into account for proposing such registration requirements. Given that the operations of a social network operator could potentially be shut down in the absence of registration, the costs and benefits of the provision need to be carefully analyzed.

In our assessment, the provision as it stands now suffers from the following problems:

a. "Social networks" is not a distinct class. Platforms offering very different services may include some features of social networks. For example, gaming apps integrate messaging features between users, while food discovery apps may allow users to post reviews and engage with other users. In this scenario, making registration mandatory for an ambiguous category of platforms will lead to unpredictability in the proposed legal regime, and its implementation.

b. The conditions for registration are not clearly specified and it is unclear which social networks, under what circumstances, would require registration. This leads to unnecessary ambiguity in the legal regime.

c. Usually, a registration requirement is based on a need for tracking the number and quality of essential services such as healthcare, or when an exclusive right is being provided by the government, as is the case with telecom service providers. There is no rationale for imposing a registration requirement on social media services – and in the absence of such rationale, a registration requirement is likely to increase the cost of compliance and hamper flexibility of operations of such social network operators, particularly as this industry is still young and has many start-ups.

d. A model of self-regulation based on an assessment of the kind of services provided by information technology companies may be a better regulatory fit than a prescriptive approach which seeks to define a category of service providers and register / regulate them as a class. This is particularly crucial since we are presently seeing an unprecedented spurt of development of new services, consolidation of different kinds of services, and fast paced innovation in the ways of providing familiar services such that they are consumed differently. Any legal provision that seeks to regulate the emerging online service industry on the basis of hard and fast categorizations and registration processes, may risk quick obsolescence.

4. Offences and Punishment

Some of the offences and corresponding punishment envisaged under the law are unclear and may give rise to an unpredictable legal regime. Some of these are highlighted below.

Section 78 of the IT Act states: "*Where anyone breaks the privacy of someone else's private information that is in electronic form, as per the offence the person shall be liable to the punishment…*"

The scope of the offence of "breaking the privacy" is unclear as it is worded broadly, and the necessity of this overarching provision is unclear, since all the specific obligations under this proposed law are already addressed through a corresponding penal provision. There is no prescribed set of steps that must be followed to ensure privacy specifically, and this is a general obligation that is complied with by all entities that process personal data. Thus, this vaguely worded offence – "breaking of privacy" – is ambiguous and hence will result in uncertainty in the manner in which the legislation is interpreted and implemented.

It is important to ensure that penal provisions identify the specific violations and harms that the law seeks to address. A broad provision such as this, which could potentially be interpreted in

many different ways, could constrain innovation by making companies hesitant to invest in innovative methods of processing data and delivering services. The concept of "privacy" is broad enough that any compliances for "breaking privacy" would be hard to outline. Thus, this provision should be removed as such broad language is prone to misinterpretation, and could potentially lead to a harsh and unpredictable legal regime.

Section 87 of the IT Act states: "(1) *Where someone teases, misleads, insults, discourages, threatens, creates hatred and enmity, creates difficulty to a person or an institution or with the intention of confusing the receiver, sends or cause to send information via social media or any other electronic medium, as per the severity of offence the person shall be liable to the punishment with a fine not exceeding five lakh rupees or one year of imprisonment or both.*

(2) *Where by using social media or any other electronic media someone seriously disrupts the sovereignty of Nepal, integrity or good relation between different caste, ethnicity, religion or creed or breaks peace and security or encourages the massacre or causes to act so, as per the severity of offence the person shall be liable to the punishment with a fine five to ten lakh rupees or five to ten years of imprisonment or both*."

The penal provision is broadly and vaguely worded in a manner that makes it very difficult to comply with, without having a chilling effect on all speech. This provision, without appropriate checks and balances grounded in due process of law, is likely to give rise to the potential of being used to issue takedown notices or blocking orders, to the detriment of users as well as social network service providers who are hosting content.

Read with the other provisions of this proposed IT Act that mandate taking down content when the social media service provider is "aware" of illegality of content, and given that this provision makes a broad swathe of content potentially illegal, this would tend to create a highly uncertain regulatory regime where social media service providers may be expected to police speech to err on the safe side of the law.

In this instance, the provision creates penalty for acts such as "teasing" and "confusing", while the provision does not specify the elements which would constitute such acts. Many kinds of content could be considered to be "teasing", "insulting" or "creating difficulty", based on the sensitivities of different people. It would be exceedingly challenging to develop judicial thresholds for offences of this nature.

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 remove this provision and alternatively, make it more pointed in order to refer to specific kind of content. Any reference to "creating difficulty" should be removed in the interest of making the law specific and understandable.

98. Abetting for offence: Where someone abets anyone for any offence pursuant to this act or announces to commit such offence or be involved in conspiracy, such person shall be liable to the punishment equals to the punishment condemned to the main convict.

99. Punishment to matiyar: Someone who supports for committing offence pursuant to this act or supporting to do so via any other way shall be liable to half of the punishment condemned to the main convict.

The interrelationship between Sections 98 and 99 is unclear as they seem to be referencing the same offence while mentioning different penalties. Assuming that "abetment" and "support" are two separate and specific offences, this needs to be clarified in the drafting of the provisions, which is presently unclear.

The punishment of "half" the punishment is also unclear as laws provide for punishment in a range and depend on judicial determination. Prescribing "half" the punishment as that of the "main convict" will lead to confusion if there are multiple main convicts with multiple sentences. This provision also does not adequately provide for judicial determination of sentence based on the degree of wrong committed and will be prone to creation of conflicting judicial precedents.

Further, in light of the fact that most of the offences that we have highlighted above are drafted in vague and non-specific language, it would be inadvisable to have such harsh penalties for "abetment" and "support" – as this could lead to wrongful convictions or unpredictability in legal regimes where the main offence is inadequately defined.

It should be noted in this context that abetment of offence, in addition to being punishable, is also a ground for refusing exemption of liability to intermediaries. Therefore, there is an urgent need to make the scope of the offence clearer, since it could lead to a legal regime that is not conducive to an innovative digital economy.

End of Submission