24 April 2019

To
Mr. Mahendra Man Gurung
Secretary, Ministry of Information and Communications
The Government of Nepal

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

On behalf of the Asia Internet Coalition (AIC) and its members, I am writing to express our sincere gratitude to the Ministry of Information and Communications, Government of Nepal, for the opportunity to submit comments on the amended Information Technology Bill, 2018 ("IT Bill"). We would also like to reiterate that this submission is in continuity to the earlier submission made by AIC on 6 February 2019 (Link to earlier submission).

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 IT Bill as amended proposes to introduce some important principles of the 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 is adequately reflected, and to facilitate the continuing spurt of growth of new and innovative information technology services in Nepal, we submit our concerns and recommendations with regard to the provisions of the proposed IT Bill.

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 Bill. Importantly, we would also be happy to offer our inputs and insights on industry best practices, directly through meetings and discussions, which the Ministry plans to hold.

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.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition | www.aicasia.org

Detailed Comments and Recommendations – Information Technology Bill, 2018

I. REPRESENTATION ON THE INFORMATION TECHNOLOGY BILL, 2075 (2018)

As technology is developing rapidly across the world, countries have felt the need to understand these developments and respond to them, in order to regulate their development in a way that benefits the digital economy. In light of the advantages of technological integration among different countries, the Government of Nepal has felt the need for a progressive and updated law on information technology. Accordingly, the new Information Technology Bill, 2075 (***IT Bill***) has been drafted to replace the erstwhile Electronic Transaction Act, 2006 and provide a comprehensive framework for information technology, cyber security, data protection, and intermediary liability.

The IT Bill seeks to address the rise of digitisation in Nepal, by recognising the legal validity of electronic records, electronic contracts and electronic signatures. The provisions relating to the digitalisation of public services and creating websites for all government agencies and public entities are also commendable.

However, we would like to take this opportunity to share some concerns in respect of certain provisions of the IT Bill. In this representation, we have highlighted legal provisions that could hamper the growth of the digital economy in Nepal, and have provided comments that may help in aligning the stated objectives of the proposed legislation with the actual provisions. To this end, we have provided a tabular presentation for the specific provisions that we believe should be reviewed.

As a path-breaking legislation, this IT Bill will have a tremendous impact on the industry of Nepal, and we are deeply committed to seeing that the impacts act as a positive force that will promote and guide information technology practices and digital development in the country.

II. ANALYSIS AND COMMENTS ON KEY PROVISIONS OF IT BILL

a. Lack of procedural safeguards

The IT Bill empowers investigating agencies to access and collect traffic data and intercept content data. The authorisation for the same is given by the quasi-judicial body formed under the IT Bill, that is, the Information Technology court (***court***). Under these provisions, the court orders the access, collection or interception of specified data based on its satisfaction that the data is reasonably required for a criminal investigation. However, these provisions do not provide adequate safeguards and due process for interception / data access requests, etc.

Firstly, there is no provision for data protection requirements to be followed by the law enforcement agencies who access the collected data.

The IT Bill should prescribe the following safeguards in order to protect the collected data:

- Judicial pre-authorisation of all data access / search / seizure provisions – including for monitoring traffic data;
- Non-disclosure of collected data to unauthorised bodies or to the public;

- Destruction of the records relating to such data after a specified period of time, and
- Data protection measures by the involved agencies in order to protect the privacy of the individuals whose data has been collected.

- The due process for data requests should allow a solution for conflicts with other laws the service provide is subject to. For example, the Australian law proposed such provisions.

Secondly, there is no provision for notification to the individual whose data is being collected. While this may be necessary in order to maintain the sanctity of the criminal investigation, the IT Bill should direct the court to consider whether the notification to such individual is viable or not.

b. Establishment of license / registration regime

The IT Bill prescribes registration and / or licensing for various services, such as registration of social networks, license for running a data center or a cloud service, etc. Such compliance obligations are highly onerous for businesses as well as individuals. Licenses and registration requirements will create barriers to the conduct of business in key sectors of the digital ecosystem, which will slow down the process of digital growth in Nepal.

A similarly onerous provision is the pre-approval for using passwords and software or electronic devices which are very challenging for enforceability, as digitally connected individuals may set multiple passwords and use multiple electronic devices.

While public interest dictates some level of regulation as necessary in the area of information technology, it is unclear which public purpose is being addressed by the above-mentioned provisions. In fact, such obligations would have an extremely stultifying impact on the digital industry.

c. Intermediary Liability

We observe that the IT Bill seeks to define "service providers" and "social networks" separately, and impose specifically onerous obligations on both. These obligations are not in line with global best practices. While the Bill seems to adhere to the principle of limiting liability which is desirable for promoting a thriving digital economy, it falls short of the principles of specificity and unambiguity.

We therefore recommend:

- Clearer principles governing intermediaries (some are presently falling into both the categories of "service providers" and "social network" and have obligations in respect of both)
- Exemption from liability whenever the intermediary acts as a neutral channel of communication and does not modify content. 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. These should not amount to "selecting" user and losing safe harbour.
- Adequate due process safeguards have not been built into takedown requirements. 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.
- Requests for content of communications, should be limited to where available, i.e. acknowledgement of end-to-end encryption.

An intermediary should not be held liable for any non-compliance if the order in question does not follow these procedural safeguards and due process requirements.

- In the present iteration of the IT Bill, liability is not exempted where the provider is "**aware** the information, data or the link that infringes the provision of existing law" (emphasis added) which could be interpreted in such a manner as to entirely subvert the intention of limiting intermediary liability. Since it is not possible, in the absence of a judicial determination, for a private party to be "aware" that any content is unlawful, we recommend building in a requirement of judicial order being passed in order for an entity to be considered "aware" of illegality of content.

- The offence of "abetment" which runs through various penal provisions including the provisions limiting intermediary liability, are 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. We have recommended limiting liability in all cases where an intermediary does not actively initiate transmission of communication.

d. Vagueness in cyber offence / provisions

The IT Bill creates a framework for cyber security in the country by prescribing cyber-crimes such as cyber terrorism and publishing / display etc. of obscene materials. The IT Bill states that publishing content constituting disrespect of labour, acts against morality and ethics, messages meant to tease or discourage constitute cyber offences. However, none of these terms have been defined, and it is highly challenging to develop objective judicial thresholds for content that could legally be held to be 'discouraging', 'disrespectful to labour', etc. The provision on cyber bullying, though well-intentioned in light of the instances of online harassment, make acts that "tease, derogate, discourage, defame or scold anybody" a cyber-crime. Similar to the above, these terms have been given no definition or standards in order to adjudicate as to the actions that would be grave enough to constitute punishable offences.

It is crucial that a predictable legal regime for cyber offences should be developed – which clearly specifies what constitutes offences, who is liable for the same, specifies clear standards for abetment and assistance in a way that does not subvert intermediary liability.

III. TABULAR PRESENTATION OF THE SPECIFIC PROVISIONS THAT WE SUGGEST FOR REVIEW

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
Definitions	Service providers / social networks are defined differently.	We recommend defining a single category of intermediary as a body that provides a channel of communication or a platform for hosting content and limiting liability whenever any	The overlapping requirements applicable to service providers and social networks may be onerous for certain categories of

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
		communication is not directly initiated by such a party.	intermediaries to comply with, and also give rise to procedural inconsistencies.
Missing Definitions	There are several key terms that are not defined in the law, including: a. Open Standard b. Data Subject c. Information Technology Instruments d. Data Processor e. Warehouse Operator	We recommend adding definitions to all terms used in the law in order to ensure effective implementation and remove ambiguities in interpretation.	
12. Information not to be inserted, changed, deleted or suppressed	No one can exhibit any unauthentic electronic information as authentic or insert, modify, delete or suppress the electronic information making it legible or understandable or illegible or not understandable for legal purpose or cause to do so.	No one shall knowingly represent any false information as authentic or insert, modify, delete or suppress the electronic information making it legible or understandable or illegible or not understandable for legal purpose or cause to do so. Provided that any liability under this section on body corporates shall be subject to Section 89.	In the absence of a definition of "exhibit", this provision risks undermining intermediary liability. Relevant changes have been suggested to mitigate such liability.
47 Submission of private key to the Controller	(1) If the Controller thinks, in order to protect the sovereignty or integrity of Nepal, to maintain the friendly relations with friendly countries, to maintain the law and order, to prevent from committing of any offence under the laws prevailing, and or in other conditions as prescribed, necessary to issue an order to any subscriber to submit the private key to him/her specifying reason there for, such a subscriber shall immediately deposit the private key to the Controller.	Recommend deletion. Alternately, we recommend narrowly defining the grounds on which this can be done, and specifically requiring pre-authorisation from a judicial body. Further, recommend putting in adequate safeguards so that this provision is not misused by the Controller or the office of the Controller.	This provision is broadly worded and does not contain any procedural safeguards, which may lead to compromise of digital documents if this provision is misused.
64	(1) Certain information technology instruments	We recommend defining the terms in this provision such as	The term "information technology instruments"

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
Goods with permitted standard only be imported and distributed	shall be imported and distributed that only meets prescribed standard. (2) Whatsoever written in Subsection (1), prescribed instruments can only be used after the Permission. (3) Procedure of approval based on the standard, quality of the goods, longevity and security and the other issues related to the e-waste management shall be as prescribed.	"information technology instruments" and "information technology related goods" as these definitions being clear is critical to a predictable regime for importation of digital products. Further, recommend inserting the language "or exceeds" in clause 64 (1) after the words "…that only meets…" so that the government may prescribe the base standard, and anything above the base standard should be automatically permitted.	and "information technology related goods" has not been defined in the IT Bill. In this event, there is a lack of clarity over the scope of this term, and which goods could be included under it. Other suitable changes for streamlining importation and distribution of goods have been mentioned.
65 Instruments shall not be used without permission	Under this Chapter, no one shall use or provide others to use the information technology related goods without Permission or more than period of time than permitted		
66 Instruments that does not meet the prescribed standard shall not be imported or traded	Under this Chapter, no one shall import or trade information technology related goods without Permission		
67 No collection of Personal Information	(1) Personal information of individuals remained in electronic form shall not be collected except otherwise provided by law. (2) Data Subject should be compulsorily informed the purpose of collection of the information when there is necessity of such collection.	We recommend defining terms like "personal information" and "data subject" and reframing Subsection (1) to harmonise the data collection norms with Nepal's Individual Privacy Act, 2075. The responsibility of informing the data subject should also be clarified – if the onus is on the data processor, this should also be defined. We recommend that sub-section (4) be changed to:	1. Data collection on the basis of consent should be the default norm, and not a blanket ban on personal data collection unless otherwise authorised. 2. Legal necessity (that is, any obligation to retain data under any law in force in

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
	(3) Any personal information stored in Information Technology System shall not be used, transmit or exchanged other than the purpose given to the data subject before collection of such information. Provided, this provision shall not restrict using or transmitting or exchanging the information with the permission of the data subject or other law in effect. (4) Personal information collected or stored under the law for specific purpose shall be destroyed within thirty days after the purpose or use of the information is served and the data subject be sufficiently assured about the destruction of such information.	"The data processor may store personal data for as long as may be reasonably necessary for the purpose for which it was collected or processed." Separately, we recommend that the Bill clarify that the term "personal information" is used in a manner consistent with its definition in Nepal's Individual Privacy Act, 2075.	any of the countries in which a data collector operates) should be an absolute exception to the data deletion obligation. 3. 30 days is an extremely short time frame and should be reconsidered in line with global best practices – ideally this should be a flexible time frame depending on business practices and legal necessity. 4. The term "personal information", used in this section has not been defined in this Act. In order to ensure consistency and ease of implementation of the Information Technology law, the definition of "personal information" in the Individual Privacy Act should be applied to this statute as well.
68 (1) Information Security shall be guaranteed	Data processor, data warehouse operator or service provider shall maintain the privacy and integrity of the information remained in digital form during the exchange, processing and storage of the information in digital form.	Recommend defining data processor and warehouse operator. We also recommend defining the terms "continuity" and "information" in a manner that is clear and consistent with Nepal's Individual Privacy Act, 2075. Further, this issue may be better addressed under a privacy law.	These entities have not been defined, thus it is unclear which of them must comply with the provision. If this is a cross reference to any other law dealing with privacy, the references should be clarified.

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
68 (3) Information security should be guaranteed	Government, public, financial or health institution should secure prescribed information while processing, transferring or storing in a way such information shall not be trafficked to the cross-border jurisdiction.	Recommend deletion. We recommend that this clause be amended to state: "Government, public, financial or health institution shall process, transfer and store the prescribed information securely." In the alternate, critical categories of data for localisation should be specified.	The term "prescribed information" does not appear to be defined in the statute. In order to ensure consistency and ease of implementation of this legislation, this term should be defined and/or cross-referenced to its definition in the Individual Privacy Act. This provision appears to introduce a localisation requirement. It should be noted that localisation is a measure that significantly impedes ease of doing business, prevents opportunities for innovations and collaboration, and often increases costs for consumers. In light of the several globally acknowledged problems with localisation, such measures where implemented tend to be restricted to a very narrowly defined critical category of data, if imposed at all, following a cost benefit analysis. The broad localisation provision imposed in this law should be reconsidered.
70 Security audit to be done	Government, public, financial institution or an institution that uses health related information should compulsorily conduct annual security audit of the information technology system.	Recommend defining. "health related information."	The term "health related information" has not been defined. Such a definition is imperative in order to provide clarity on which institutions must comply with this provision. It is also unclear if "institution" includes

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
			private parties such as intermediaries.
71 Provision Regarding operation of data center and cloud service 73 Data center or cloud service not be run without license:	Any person or Institution desirous to operate a data center or cloud service within the territory of Nepal should obtain a license from the Department after submission of an application in prescribed form. Pursuant to this Act no one shall run data center or cloud service without license	Recommend deletion.	The requirement of a license in order to run a data center or cloud service is onerous and may prove to be a barrier to business. It appears that the conditions of license are also not clarified which is further cause for concern.
81 Pre-approval required for use of certain devices	(1) Before the use of following devices pre-approval shall be taken from the Ministry: (a) Any software, electronic system or electronic devices designed to protect the electronic system or can be used for offensive acts, (b) Any kind of passwords, or access codes or data that enable partial or full access upon the electronic system or data.	Recommend deletion.	The range of electronic devices covered by this is broad enough to make this provision impractical in the present day – it is both lacking in rationale and being difficult to monitor the implementation of.
83 Provision relating to cyber bullying	Nobody shall continuously harass, tease, derogate, discourage, defame or scold anybody using electronic system	Recommend linking this provision to specific offences under Nepal's penal laws.	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. The provision creates penalty for acts such as "teasing" and "discouraging", while the provision does not specify the elements which would constitute such acts. Many kinds of content could be considered to be

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
			"teasing" or "discouraging" or "scolding", based on the sensitivities of different people. It would be exceedingly challenging to develop judicial thresholds for offences of this nature.
84 Provision relating to cyber terrorism	Nobody shall, using Information System, undermine the national security, sovereignty, territorial integrity, nationality or national unity, independence, dignity, provincial relationship or obstruct or cause adverse effect to the security of the nation or data system.	Recommend linking this provision to specific offences under Nepal's penal laws.	A penalty provisions should ideally be more specific in terms of the act it seeks to penalise – such broad and overarching provisions would have a stifling effect on free speech and be hard to monitor for enforcement purposes.
87 Provision relating not to induce	Nobody shall induce anyone in the electronic system or using the electronic system with the intention to sexually exploit or to fraud or doing any act prohibited by the law or propose, incite or meet or provoke or establish online relation.	Recommend changing to: "Nobody shall use electronic systems to sexually harass or fraud or to act in contravention to any law." [Recommend adding cross references to penal provisions if applicable.]	The purport of this provision is unclear, as it is based on the provoking or establishing of "online relation", which has not been explained.
88 Not to misuse of electronic system	(2) Nobody shall use electronic system to encourage or incite acts that creates racial discrimination or untouchability, or disrespect upon any profession.	Nobody shall use electronic medium to encourage or incite acts that creates racial discrimination or untouchability, in relation to any of the acts specified in the [Caste-based Discrimination and Untouchability Law].	The term "disrespect upon profession" is unclear – if the reference is being made to offences under Nepal's Caste-based Discrimination and Untouchability Law, then a cross reference to the specific provision of the law may be recommended.
89 Service Provider shall not liable	(1) Notwithstanding any provision in other laws in effect, Service providers are not liable, in following situation, for any criminal liability that arises from any fact or	Notwithstanding any provision in other laws in effect, Service Providers are not liable, in following situation, for any criminal liability arises from any fact or particulars only because they	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

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
	particulars only because they provided access to such information or data or link. (b) If the Service Provider has not transmitted the information, data or link by its own, not selected the user by its own and the Service Provider did not select or altered the information its own; Provided, the 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.	provided access to such information or data or link. If the Service Provider has not initiated the transmission of the information, data or link by its own, and the Service Provider did not modify the content on its own; Provided, the Service Provider's liability is not exempted where the provider fails to take action regarding the specified content after being ~~is~~ made aware the information, data or the link that infringes the provision of existing law by way of a court order or by an order by an officer not below the rank of [Joint Secretary].	by users, options selected by users, or patterns of behaviour detected by algorithms. It is unclear whether this would imply that the user has been "selected" by the algorithm. In order to remove this ambiguity, the provision should simply clarify that no liability for unlawful third-party content shall accrue to an intermediary who merely hosts and does not modify the content. Further, the threshold of "awareness" has not been defined – in some jurisdictions, awareness of illegality can only take place through a court order specifying which content is illegal. This should be built into the law as a procedural safeguard. It would also be problematic to have references to abetment and assistance without mentioning what these terms would imply – thus, these references should be removed and the provision on intermediary liability should be brought in line with global best practices.
90 Data to be preserved	The Service Provider has to preserve the data relating to the service they provide for specific time and in specific form as prescribed by law.	The Service Provider has to preserve the data relating to the users of the service they provide for specific time and in specific form as prescribed by law.	The intention behind this clause is unclear. Does that bill contemplate storing data relating to the service or data relating to the users

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
			who use the service or both? Further, recommend differentiating the different types or kinds of data that is required to be stored and the period each kind of data is required to be stored. For example: financial data, user profile, uploaded content, etc.
91 Registration and Regulation of Social Networks	(1) Any person desirous to run social network has to register at the Department pursuant to this Act.	Recommend deletion Alternatively, we recommend that this provision be amended to state that any person who runs a social network must abide by the terms of this law and all other laws for the time being in force.	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. Further, the definition of "social networks" is extremely broad and does not cover 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

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
			proposed legal regime, and its implementation.
92 Direction may be given	The Department may direct the Social Network Provider to remove the contents or information immediately when the Department believes that such content is communicated or being communicated that could be declared offensive pursuant to this Act.	The Department may direct the Social Network Provider to take action regarding the contents or information immediately when the Department believes that such content is communicated or being communicated that is declared offensive pursuant to this Act, provided that the request is valid in law, is issued pursuant to a reasoned judicial order, and specifically identifies the content sought to be taken down.	The power given to the Department requires adequate due process safeguards and a review process in order to ensure that it is exercised in a manner that is fair, just and transparent. Currently, the IT Bill does not envisage any such safeguards.
94 Not to Published in Social Network	(1) No one shall perform or cause to perform the following acts in the Social Network. - Inciting the racial discrimination or untouchability, disrespecting the labour, inciting criminal activities, encourage to disrupt peace and order or publishing or transmitting any content prohibited to publish or broadcast by the prevailing law or doing or causing to do any act against public moral - Communicating any message with the intention of teasing, misleading, insulting, discouraging, threatening, creating hatred and enmity, or confusing the receiver - Without any evidence, performing any act that is realized as curse or disrespect pursuant to the prevailing law with the intention of defaming someone	We recommend linking this provision to existing/specified offences in Nepali law, rather than creating new offences that are unclear in scope, especially in terms of vague phrases such as "disrespecting the labour" and "teasing", "discouraging", "confusing" etc.	This provision is unclear in scope, especially in terms of vague phrases such as "disrespecting the labour" and "teasing", "discouraging", "confusing" etc. Similar provisions have been read down for being too broad and vague in other jurisdictions, such as in India in the case of *Shreya Singhla vs. UOI* where it was held that such broad, overarching terms impinge on freedom of speech. This clause should also be in line with the Manila Principles, and the liability of intermediaries and social networks should be limited against third party content. Social networks must be liable only to the extent proportional, and clearly mandated by law.
97	Anyone who abets someone to commit any offence pursuant to this	Anyone who abets someone to commit any offence pursuant to this Act or attempt to commit such	

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
Abetment of the Offence	Act or attempt to commit such offence or party in conspiracy, he is liable for the equal punishment as applied to the principle offender.	offence or party in conspiracy, he is liable for the equal punishment as applied to the principle offender, subject to Section 89.	We have recommended modifications to ensure that intermediary liability provisions are not subverted by lack of clarity on what constitutes abetment.
98 Punishment to the Aid	Anyone who provides aid to the principle offender or provides support in any other way shall be liable for half of the punishment sentenced to the principle offender.	Anyone who provides aid to the principle offender or provides support in any other way shall be liable for half of the punishment sentenced to the principle offender. subject to Section 89.	
107 Search and seizure	If an Investigating Officer undertaking the search and seizure, pursuant to Sub-section (1) has reasonable grounds that the information searched is stored in another electronic system or the part of it is in another system within its jurisdiction, or in another system legally accessible from the system initially acquired, then the Investigating Officer may extend the search and seizure immediately to that system and can have access to the system.	We recommend adding procedural safeguards to avoid misuse. For instance, the following safeguard could be added: Where any Investigating Officer extends search and seizure to any place not permitted by the Court under sub-section (1) of this section, such Investigating Officer must inform in writing to the Court about the reasonable grounds based on which the search and seizure was extended, and obtain the permission of the Court within a period of 7 working days, and if the permission of the Court is not obtained within 7 working days, any information gathered from the search or seizure of any electronic equipment or information or any other such material must be erased.	As search warrants tend to be specific to a place, this provision is prone to misuse without adequate safeguards being put in place.
111 Access to Traffic Data	(1) If the court is satisfied that the traffic data associated with a specified communication is required for the purpose of a criminal investigation, the court, on the basis of affidavit, may give permission to the investigation officer to access the traffic data associated with a specified communication.	The term "traffic data" should be defined – and the safeguards in Section 107 should be included in this provision too. Further, it may be recommended to add that such information will only be used for the purposes of investigation and impose restrictions on disclosure and deletion requirements in line with privacy laws / criminal procedure in Nepal.	There is no definition of traffic data, or any clarity on what "traffic data associated with a specified communication" pertains to. We recommend defining the terms, including adequate due process safeguards, and also instituting data protection requirements post-collection such as requirement of data

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
112 Collection of traffic data	(1) If the court is satisfied in regard to prima facie evidence that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the court shall, by giving written notice to a person who has control of such traffic data, shall order the follows: (a) collect or record traffic data associated with a specified communication during a specified period in real time; and (b) permit and assist an investigation officer to collect or record that data in real time. (2) If the court, in regard to prima facie evidence, is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the court shall give permission to an Investigating Officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means in real time.		deletion and restriction on disclosure.
113 Interception of content data	(1) If the court is satisfied in regard to prima facie evidence that content data of any communication is required for the purpose of a criminal investigation, the court	Content data should be defined – and procedural safeguards in relation to the same should be built in.	The concerns relating to lack of definition, safeguards and data protection requirements as applicable in respect of traffic data also apply

SECTION	EXISTING PROVISION	PROPOSED PROVISION	RATIONALE
	shall order to collect or record content data associated with specified communication transmitted by means of an electronic system in real time through the application of technical means or shall order to permit or assist the authorized officer for such act.		in respect of content data.

In light of the above analysis, we request that the specified provision be reviewed and reconsidered, and be revised in the manner suggested, in order to ensure that the IT Bill serves the purpose that it aims to serve, which is of ensuring public safety and trust, while allowing business to grow.

- ***End of Submission***