ANNEXURE-I

COAI

RSM/COAI/2018/191
October 10, 2018

Joint Secretary
Ministry of Electronics and Information Technology (MeitY)
Room No. 4016, Electronics Niketan,
6, CGO Complex,
Lodhi Road, New Delhi – 110003

Subject: COAI's Inputs on draft "The Personal Data Protection Bill 2018"

Dear Sir,

1. This is in reference to the notification issued by MeitY on August 14, 2018, requesting comments of general public on the "Draft Personal Data Protection Bill 2018"; and the subsequent extensions for submission of comments granted till October 10, 2018. Our response is enclosed.

2. Kindly note that the enclosed response is being submitted on behalf of the core members of COAI which include M/s Bharti Airtel Limited, M/s Reliance Jio Infocomm Limited and M/s Vodafone Idea Limited.

3. Our Associate Members namely IBM, Facebook, Google, Amazon, Ericsson etc. have divergent opinions with our Core Members with respect to Section 40 and 41 of the draft bill i.e. "Restriction on Cross-Border Transfer of Personal Data" and "Conditions for Cross-Border Transfer of Personal Data" respectively, and they will make their independent submissions to the Ministry.

4. We hope the Government of India will consider our submissions favorably, while finalizing "The Personal Data Protection Bill 2018".

Regards,
For **Cellular Operators Association of India**

Rajan S. Mathews

Rajan S. Mathews
Director General

Copy To:

1. **Shri Ajay Prakash Sawhney, Secretary**, Ministry of Electronics and Information Technology, Electronics Niketan, 6, CGO Complex, Lodhi Road, New Delhi – 110003

14, Bhai Veer Singh Marg, New Delhi – 110 001
tel: +91-11-23349275 fax: +91-11-23349276 email: contact@coai.in website: www.coai.in

COAI INPUTS ON THE "THE PERSONAL DATA PROTECTION BILL, 2018"

At the outset, we sincerely appreciate and thank you for the opportunity provided to us to present our inputs on the Draft "Personal Data Protection Bill, 2018" ("Bill") drafted by the Group of Experts chaired by Justice (Retd) BN Srikrishna.

This response is being submitted on behalf of the core members of COAI which include M/s Bharti Airtel Limited, M/s Reliance Jio Infocomm Limited and M/s Vodafone Idea Limited. We welcome the Draft "The Personal Data Protection Bill, 2018", which has been drafted with an intent to keep the personal data of citizen secure and protected. The framework proposed by the committee incorporates numerous provisions that lay emphasis on demonstration of accountability and re-establishing trust between entities and end consumers in the digital ecosystem.

Kindly note that our Associate Members namely IBM, Facebook, Google, Amazon, Ericsson etc. have divergent opinions with our Core Members with respect to Section 40 and 41 of the draft bill i.e. "Restriction on Cross-Border Transfer of Personal Data" and "Conditions for Cross-Border Transfer of Personal Data" respectively, and they will make their independent submissions to the Ministry.

We would like to submit that although the draft bill has been formulated post detailed deliberations and extensive consultation processes, however there are certain provisions defined in the bill which may cause impediments to businesses and therefore need to be clarified/relooked at. We believe that addressing these impediments will aid in ensuring a balanced approach to data protection regulation, which will harmonise the interests of citizens and businesses at large, in the larger interest of the Nation. Certain aspects of the present draft are likely to cause disproportionate harm to consumer or business interests without a corresponding benefit, particularly by way of increased compliance and overhead costs for stakeholders.

We would also like to highlight that the telecom sector is highly regulated, being governed by a number of guidelines relating to protection of user data. There are however, different players in the Information Communication Technologies (ICTs) ecosystem who are not subject to the same regulatory restrictions/oversight, thus placing at risk the data protection and privacy rights of Indians.

The absence of a horizontal data protection framework across all digital entities gives rise to an uneven regulation as different data fiduciaries are subject to different rules with regard to privacy and data protection. This inequity is most visible in the treatment of telecom service providers and OTT Communication service providers. Whilst the former are subject to license conditions prohibiting sending of user information outside India, the OTT Communications service providers, offering identical services are subject to no such restriction. There is a risk to the end objective and also all laws and regulations being rendered futile if one set of service providers are able to transfer data outside the country with little jurisdiction of the local authorities/ regulators, whilst the other set are subject to strict restrictions with heavy penalties for non-compliance. The only way

to fully protect the interests of consumers and national security will be through firm laws that are ubiquitously applicable to all digital entities as has been done in several countries already.

Lastly, an effective data protection framework requires enforcement by an able and qualified regulatory authority, which is independent and empowered. In our view, the structure and functioning of the Data Protection Authority could be altered in small ways so as to result in a more certain, predictable, and effective framework.

We would like to submit our concerns and suggestions on the following clauses/issues highlighted in the draft Personal Data Protection Bill 2018. We also seek your leave to make further /additional submissions in the matter after assessment of the impact, if any, of the Aadhaar judgment on the Draft Bill (recently issued by the Supreme Court on 26th September 2018):

A. Definition of Personal Data and Anonymised Data

The definition of personal data should be practical and risk-based. It should not include all data that is capable of re-identification by a person or set of persons, but data for which a fiduciary or processor is reasonably likely to have and use the means to be able to identify the data principal. It may be noted that this distinction was there in the IT Act, which defined "**Personal information**" as any information that relates to a natural person, which, either directly or indirectly, **in combination with other information available or likely to be available with a body corporate**, is capable of identifying such person.

We submit that the definition of personal data in the IT Act read with SPDI Rules has spurned multiplicity of differences and disputes in interpretation. We believe that if the Draft Bill is to meet its object of addressing data protection and data privacy in a definitive and effective manner, **it will be critical for the Draft Bill to resolve the ambiguities in interpretation of what constitutes personal data** by going beyond a mere description of a set of generic and non-exhaustive characteristics (which, in the Draft Bill, are similar to the IT Act read with SPDI Rules) and stipulating an objective and verifiable method of determination. To that extent it is requested that the definition be made precise and clear.

Further, de-identified data should not be considered as personal data and should be considered as anonymised data. We believe that anonymization/anonymised data should include de-identified data similar to the definitions in GDPR, for a practical and balanced implementation of the bill that meets the requirements of data fiduciaries and data principals.

The word "irreversible" should be deleted from the definition of anonymisation. For identifying the ambit of "personal data" – a standard similar to Recital 26 of the GDPR should be employed, which clarifies that "to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." The test of reasonability can linked to "objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". The Draft Bill could also take an approach to de-identification that is similar to the

Health Insurance Portability and Accountability Act ("HIPAA") which states that, when specific identifiers that been removed from the data, it can be regarded as de-identified. Such data should not be included within the ambit of personal data.

We submit that data should be considered anonymized or de-identified if the likelihood of re-identification (with reference to technical possibility and practicability) is below certain thresholds. The Bill departs from international standards in its treatment of de-identified data by according it the same level of protection and concomitant obligations as other personal data, which should not be the case. Further, the definition of anonymization should include references to 'reasonableness' or 'risk-based approach' to managing the risk of re-identification instead of focusing on the process and end – state of the data.

B. Definition of Sensitive Personal Data or Information (SPDI)

The Bill has expanded the list of SPDI and has added ambiguous categories such as behavioural patterns. This will lead to compliance challenges for businesses and strongly discourage innovation. The list should be shortened for ease of compliance and should only include categories of data that carry special risks in relation to discrimination and abuse of fundamental rights. Even the GDPR, which is widely regarded as one of the most comprehensive data protection laws of our time, has a narrower list of SPDI as compared to the current Bill. Further, the definition should be exhaustive to avoid any ambiguity.

Further, in this case also the accountability of the data fiduciary should be confined to only such data or information as provided to the data fiduciary by the data principal for providing the Service.

W.r.t official identifiers, these are regularly processed by data fiduciaries. If these are to be included, the list/universe of official identifiers should be made known to avoid any ambiguities.

The Bill should also include a clearer definition of what processing of SPDI would mean, i.e. explicit collection and processing of specific categories of data and not merely potential inference of SPDI. Safeguards for processing of SPDI are best identified by industry through contextual self-regulation and assessment of harms/risks.

Instead of regulatory prescription, the law should allow wider grounds for processing of sensitive data. Processing for employment related purposes should be a valid ground for processing sensitive personal data. The bill has provided this basis only for processing personal data and we recommend it should be extended to include Sensitive personal data.

In view of the above, we recommend the followings:

(i) The list of SPDI data should be shortened for ease of compliance - even the GDPR, which is widely regarded as one of the most comprehensive data protection laws of in current scenario, has a narrower list of SPD as compared to Draft Bill. We recommend that this list be exclusively given in the law, the Draft Bill.

(ii) Instead of regulatory prescription, the law should allow wider grounds for processing of sensitive data. In general, processing of sensitive information should be allowed where appropriate safeguards for the security and privacy of the information are in place, where the data subject is adequately informed about the collection and use of the sensitive data prior to sharing of data and has legitimate options to refrain from sharing the data, or where adequate de-identification, subject to sufficient technical and organizational measures preventing re-identification, is employed.

Other comments w.r.t Section 3 (Definitions) :
W.r.t sub-section (21), the definition of harm includes
(vi) any discriminatory treatment.

However, it is very subjective - an action which may be discriminatory for an individual may not be discriminatory for other, which could result in unnecessary claims. Hence, this should be dropped.

(viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal

However, this broad definition of "harm" could have a deleterious impact on everyone using machine learning and Artificial Intelligence (AI) in the social context and hence, should be dropped.

C. Notice

Section 8(1) (g) poses an operational challenge which requires the data fiduciary to give information of 'the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared' as the list of such entities/individuals may be voluminous particularly on account of out-sourcing of various parts of the business activities to multiple entities. Hence, it should be modified to exclude the names of the individuals or entities-instead.

D. Consent

Section 12 mandates that for consent to be valid it must inter alia be capable of being easily withdrawn. While it is vitally important to ensure that the Data Principal has the ability to withdraw consent for processing of its data, this should not be made a condition precedent for the validity of consent. The ease or difficulty of withdrawal of consent does not in any way influence or induce the Data Principal to provide consent where it does not want to. Provided the Data Principal's consent is free, informed, specific and clear, there is no need to invalidate the consent just because the capability of withdrawal is not easy enough. The right of withdrawal of consent can be protected without making it a pre-condition for consent. The test of easiness also brings a lot of subjectivity into the question of consent. It is suggested that the section 12(2)(e) should be removed and instead we propose that the right to withdrawal of consent should be included in Section 29 of the Bill, which deals with policies and measures to be undertaken by Data Fiduciary.

This will ensure that the Data Fiduciary is still obligated to ensure ease of withdrawal of consent without negating consent altogether just because the capability of withdrawal is not easy enough.

The Bill states that personal data ("PD") can be processed with consent from the data principal or for specific purposes set out in the Bill in Sections 13 to 17. One of these bases is for "reasonable purposes" that will be specified by the DPA at some point in the future. Additionally, "explicit consent" is the main basis on which sensitive personal data ("SPD") can be processed, with only limited exceptions to the same. As submitted above, the scope of the term "sensitive personal data" is broader than other comparable privacy regimes, such as the European Unions' General Data Protection Regulation ("GDPR") and covers passwords, official identification data, and financial data, which means that under the Bill processing these types of data is much more restricted than comparable privacy regimes. Moreover, the Authority has discretion to add new categories to this definition to which the restrictions on processing will apply, whereas under the GDPR only defined categories of information are considered "sensitive". The scope of exceptions to explicit consent for processing sensitive personal data are narrower than under the GDPR. It is unclear why this position has been taken under the Bill. With reference to the same we strongly recommend the following:

(i) We believe that the Bill should contain clear bases for processing personal data that would be considered "reasonable purposes". It should allow for the inclusion of a specific ground permitting data processing on the grounds of **contractual necessity**. Further, the reasonable purposes exception must be included as an equal ground for processing of sensitive personal data to enable better security and fraud detection, among other consumer benefits, and it should not be a residual ground or require the approval of the Data Protection Authority.

(ii) We note that some of the activities listed under Section 17 (2)[1] fall in the realm of necessary activities of data fiduciaries – to carve them out as a separate category, which will only be allowed basis DPA's specific instructions, will create operational issues for many data fiduciaries. For e.g. prevention & detection of any unlawful activity, mergers & acquisitions, network & information security, credit scoring, recovery of debt etc. Hence, such activities should be excluded from Section 17 (2). Further, processing of publicly available personal data [Section 17(2)(g)] should not be regulated. Thus, 'reasonable purpose' should be judged by the data fiduciaries, in line with global standards

(iii) There are several social and economic benefits that can be derived from big data analytics. The Privacy bill should not hamper such innovation. Privacy provisions should only apply to identifiable data being shared with third parties without user consent.

(iv) In addition, the Bill should also allow the DPA to specify further basis for processing in future regulations as technology develops. For example, under GDPR alternative legal basis (other than consent) for processing personal data are clearly set out in Article 6, such as where processing is necessary for the performance of a contract to which the data subject is a party or where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. All legal bases for collecting, using

[1] prevention and detection of any unlawful activity including fraud; whistle blowing; mergers and acquisitions; network and information security; credit scoring; recovery of debt; processing of publicly available personal data.

and disclosing personal data should be treated equally instead of relying on consent as the primary ground for processing personal data.

(v) Further, in order to ensure that the protection of individual privacy rights is balanced with other legitimate business and public interests, we recommend the scope of the definition of "sensitive personal data" be amended and the exceptions to explicit consent be expanded to include all the bases. The GDPR definitions can act as benchmark here.

(vi) By way of this omission (i.e. grounds of contractual necessity), the Bill creates a need for the data fiduciary to repeatedly obtain consent from the data principal for every step of the processing activity. Obtaining consent at all points of data collection and processing or obtaining direct and positive consent all the time, is at times either impossible, impractical or unnecessary. As long as the processing of the data does not deviate from the original purpose, repeated consent requirements should not be imposed. Individuals can be overwhelmed if constantly presented with privacy choices and requests to collect data. This needs to be clearly addressed in the Bill (as raised in point [ii]). As long as the consent has been obtained as per the provisions of the Indian Contract Act, the bill should not impose any additional obligations or restrictions which will potentially affect the rights of the data fiduciaries and lead to inconvenience to the individuals.

E. Excessive Delegated Legislation

The draft Bill has many instances of delegated legislation either to the DPA or the Central Government. The most concerning instances are as follows:

i) Standard contractual clauses
ii) "Guardian" data fiduciaries
iii) "Significant" data fiduciaries
iv) Codes of Practices
v) Anonymization standards
vi) Limit for exemption from Act for small entities
vii) Qualifications of Adjudicating Officers

As can be observed, all the above-mentioned powers have been delegated without providing either the DPA or the Central Government with statutory guidance on how to regulate these areas. The danger with such broad delegation is that the executive authorities cannot be expected to derive the true legislative intent of the law and identify the exact nuisance to be prevented. The overarching powers in favour of the DPA are excessive and unwarranted. The disproportionately broad powers vested in the DPA would effectively allow it to implement an entirely different framework of obligations for data fiduciaries and data processors by the simple act of issuing directions or codes of conduct without seeking submissions from industry representatives and other stakeholders and without following usual legislative processes or the principles of natural justice. As a result, data fiduciaries and data processors will face significant uncertainty in managing their compliance with the law and this uncertainty will likely lead to inconsistencies and

have a negative impact on data principals as a whole. They may exceed the scope of the law or even distort its intentions. We strongly recommend that the broad discretion of the DPA be replaced with transparent and clear provisions contained in the Bill or in implementing regulations that are passed in accordance with the legislative process. We suggest that such statutory guidance /framework may be enunciated in the preamble giving the purpose and intent of the Act.

We submit that the Draft Bill should incorporate and provide for the sector regulators, and where there is no sectoral regulator, the relevant ministry, to play the role of prescribing the specific parameters applicable for matters such as consent, notice, individual participation rights, definition of personal data and the like, in the specific context and in consideration of unique factors that may impact such relevant industry. We reiterate that such involvement not only co-opts the sector regulator/ministry in playing an active role in assisting the Authority, but also strengthens the regulatory oversight of such sector regulator/ministry, thereby creating a strong mesh of interacting and interoperable regulatory framework.

F. CONSENT FOR MINORS

Where children's data is processed by data fiduciaries, the Bill imposes special requirements to incorporate 'appropriate' mechanisms for age verification and parental consent. The Bill also creates a category of 'guardian data fiduciaries', as notified by the DPA where a data fiduciary operates commercial websites or online services directed at children or processes large volumes of personal data of children (Section 23). Guardian data fiduciaries are barred from profiling, tracking, or behavioural monitoring of, or targeted advertising directed at, children and undertaking processing personal data that can cause significant harm to the child. 'Child' is defined under the Bill as a data principal below the age of 18 years (Section 2(9)).

We believe that mandating age-verification procedures and a blanket limit of 18 years of age, the Draft Bill has ignored the varying maturity levels of children at various age groups which may result in excluding a large swathe of the Indian youth population, which forms a bulk of internet users, from participating in the digital economy.

Given the onerous burden of compliance to these provisions, several businesses may choose to opt out of providing child-focussed services and services targeted to any users suspected to be below 18 years of age as also this will negatively impact any business which includes the possibility of participation by persons below the age of 18 years. This will preclude access to valuable sources of learning and communication for a large part of the population that would otherwise stand to gain from such access.

It is also pertinent to note that while the definition of child as a person below 18 years has been retained in the Bill in deference to the age of consent for contract as per the Indian Contract Act, 1872 read with the Indian Majority Act, 1875, the Committee has explicitly acknowledged that "from the perspective of the full, autonomous development of the child, the age of 18 may appear too high." (Page 44 of the Report) recognising that mandating 18 years will not be reasonable in

light of the varied nature of online activity. This is also in line with the observations of the Delhi High Court in the case K.N. Govindacharya v. Union of India [W.P. (C) 3672/2012] where the Court recognised the general practice of mandating 13 years as the lower (age) limit in the case of social media. Additionally, EU GDPR Article 8, requires parental consent for children below age of 16 years, allowing member states to provide by law a lower age for consent, provided it is not below 13 years.

Thus while parental/guardian approval should be required in relation to collection of personal data from children below the age of 13 years, children between the ages of 13 and 18 years may be permitted and empowered to make decisions about their data in relation to activities in ordinary course. As maturity levels are not always coexistent with age, each circumstance of collection from a child must be analysed based on the entirety of circumstances.

In addition, mandating age-verification by itself is an insufficient solution, because many businesses may – out of abundant caution – choose to stop servicing children or any users suspected to be children under a specific age. This will exclude large parts of the internet for use by children – including valuable sources of information, learning, and communication.

Instead, the Draft Bill must manifest an approach which recognises that age-verification mechanisms can only be implemented through 'all possible reasonable steps' by Data Fiduciaries. Entities who take all reasonable steps to ascertain and verify age must be exempt from any liability for the processing of child data. At the same time, where an entity has specific knowledge or reason to believe that a user is underage, they may be obligated to discontinue servicing them.

Our recommendations with respect to this issue are as below:

(i) It is thus recommended that the Bill should not mandate an age limit of 18 years in the data protection law and leave it to be interpreted based on the context of such activity. Alternatively, a 'carve-out' could be effectuated from the age of majority legislation for purposes of personal data processing of children between the ages of 13 years and above, in tune with principled considerations around the object of processing as is done in most data protection legislations around the world. Such a carve-out would be additionally supported by the overriding effect of the data protection law over any inconsistency vis-à-vis with the provisions of any other law as mandated by Section 110 of the Bill.

(ii) With these concerns in mind, we urge the Ministry to adopt a nuanced approach to the age of processing and to adopt a mechanism whereby the 'reasonable efforts' of Data Fiduciaries to verify age are recognised. Failure to include such a condition so will exclude large number of children from accessing the internet in India.

G. Data Principal Rights

The draft Bill provides many rights to data principals in order to ensure their right to privacy and autonomy. These include right to access, correction, data portability etc.

Section 24 allows data principals to obtain from the data fiduciary a brief summary of their personal data processed by the data fiduciary. Section 26 provides data principals the right to receive personal data from the data fiduciary which (i) has been generated in the course of provision of services or use of goods by the data fiduciary, or (ii) forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained. These provisions seem to include derived and processed data in their ambit. This means that the data that is a result of processing, which might form part of the intellectual property of the data fiduciary, will also be required to be shared with the data principal. This measure will thus violate the legal right of the data fiduciaries, and there is a need for further exploration of how the rights of data principals and data fiduciaries can be harmonized.

We recommend that derived and processed data should be excluded from the scope of the right to data portability.

There is a strong need to strike a balance between the data principal and the intellectual property that is created by the data fiduciary.

Section 27 provides data principals the right to be forgotten, the availability of which is to be determined by adjudicating officers. It is likely that the number of requests for this right will be very high and the officers will be inundated by a huge number of applications. It is unclear whether the DPA will have sufficient manpower and resources to process these many applications, given that the adjudicating officers have a number of functions.

In view of the above, we recommend that

i). The data principal should be able to obtain from the data fiduciary, only such data that has been provided by him/her.

ii). The right to be forgotten should be applied narrowly, where retention of such data by the fiduciary may cause likely harm to the data principal.

H. Transparency and Accountability Measures

In Chapter VII, the Draft Bill prescribes various transparency and accountability measures for data fiduciaries to implement. While these measures are rightly oriented towards addressing the power deficit between data fiduciaries and data principals, the Ministry must re-evaluate each of these measures to provide additional clarity on the specific compliances required to be undertaken. For instance, Section 29 of the Draft Bill requires data fiduciaries to implement policies to ensure Privacy by Design, however, no further information regarding the specific scope of this requirement is mentioned in the bill.

While several of the transparency measures are clear, many do not provide any indication of the compliance requirements associated thereto. For instance, sub-section (g) of Section 29 provides that “the interest of the data principal is accounted for at every stage of processing of personal

data". However, there is no clarity regarding the practical implementation of the same. In the event of such ambiguities, the enforcement of the required transparency measures will remain consequentially piecemeal.

Therefore, the Government must consider rationalising the obligations contained in this Clause by either prescribing a safe-harbour for entities implementing efforts to a 'reasonable' level, or further clarify the obligations contained under these and other provisions of Chapter VII.

W.r.t Section 30(2) (Transparency), regarding the obligation of the data fiduciary to notify the data principal of important operations in the processing of personal data through periodic notifications, since there exist other checks and balances in the various parts of the bill, the need to notify the data principals may be dropped, to reduce operational and compliance costs.

W.r.t Section 33 (2), the cost of engaging a data auditor should not be passed onto the data fiduciary. As a general comment, we also note that the words 'data auditor' and 'independent data auditor' are inter-changeably used – these may be clarified & harmonised.

W.r.t Section 39 (Grievance redressal), the time limit of 30 days for resolution of a complaint is too stringent and should be reasonably extendable by another 30 days in case the data fiduciary requires more time to resolve the complaint.

I. Differential Regulation of Data Fiduciaries

The Draft Bill creates a new category of data fiduciaries which are subject to differential systems of regulation – such as significant data fiduciaries and guardian data fiduciaries (in relation to child data), to be notified by the DPA. This differential basis of regulation has following issues:

i) Instead of focussing on concepts such as harm and risk, the criteria takes into account factors such as volume of data processing, turnover, and deployment of new technologies. In other words, entities which undertake innovation and deploy new technologies are penalised by the imposition of additional compliance requirements.

ii) Such an approach causes serious harm to India's ambitions to emerge as a hub of innovation and technology. Instead, the proposed framework should aim to incentivise and to facilitate to the maximum extent possible and only intervene where articulated harm to any specific party results.

iii) The obligations of trust score and data protection impact assessments on significant data fiduciaries might be better suited to be put in place by the entities themselves, so that they meld the interests of consumers of data as well business.

iv) Therefore, the Government should reconsider this application to classification. The purpose of the law would be better addressed with a uniform approach to compliance, with scope for intervention by the regulator only in cases where articulated harm results.

Recommendations:

(i) There should not be separate categories of data fiduciaries. The law should be uniformly applicable on all data fiduciaries without any categorization/sub-classification. The proposed framework should be uniformly applicable to data fiduciaries with an aim to incentivise and to facilitate to the maximum extent possible. It should only intervene where articulated harm to any specific party results. For instance, the introduction of reduced penalties or a safe harbour to encourage implementation of security measures would go a long way towards bringing about a culture of compliance.

(ii) The proposed framework should exclude irrelevant considerations such as deployment of new technologies and turnover, from the criteria for determining significant data fiduciaries.

J. Penalties

The present iteration of the Draft Bill adopts an unreasonable and arbitrary approach towards penalties for violations under the proposed regime. Notably, penalties may extend to as high as 4% of worldwide turnover of an entity in default in addition to criminal liability for certain offences. While it is important to have a robust enforcement framework, it is critical that this framework does not penalise beyond the actual harm done and stifle business and innovation for fear of penal sanctions. Any such effect will result in entities choosing other jurisdictions over India.

The issues related to the penalties proposed by the draft Bill are:

i) By linking penal sanctions to 'worldwide' revenue, the Draft Bill also adopts an irrelevant consideration in place of the actual harm that any non-compliance may have caused to an entity. For this reason, the current approach may also fall foul of constitutional safeguards which require penalties to be 'proportionate' and linked to the extent of the guilty conduct and harm caused.

ii) As the Supreme Court of India has, for example, stated in the Competition Act context:

> "…*It should be noted that any penal law imposing punishment is made for general good of the society. As a part of equitable consideration,* ***we should strive to only punish those who deserve it and to the extent of their guilt.*** *Further it is well established by this Court that the principle of proportionality requires the* ***fine imposed must not exceed what is appropriate and necessary for attaining the object pursued****…*."[2]

The penalties are proposed to be calculated on the basis of 'Total Worldwide Turnover' of the company, and not limited to the revenue which is generated in India or the actual harm that any non-compliance may have caused to data principal. It is inappropriate to include

[2] Civil Appeal No. 2480 of 2014 (Decided on May 08, 2017; Supreme Court of India)

worldwide turnover as a consideration in the levying of penalties for non-compliances under the proposed framework. Rather an approach which would entail fixing a cap on penalties or have penalties which are 'proportionate' to the basis of actual harm caused due to any non-compliance, would be more balanced and relevant approach.

iii) The provisions related to the imprisonment are draconian in nature and are not reflected in modern progressive data protection legislations such as GDPR. They may be misused to unduly threaten employees and individuals at all levels including senior management of the companies with personal liability.

iv) Implicating businesses and their management in legal proceedings would lead to a dip in the company's ability to carry out significant research and innovation activities leading to a fall in the country's overall innovation capabilities.

v) Chapter XIII dealing with the criminal offences may be considered for complete omission. We believe that criminal liability should only be triggered in extreme / limited situations involving criminal (including fraudulent) intent (e.g. illegal sale of personal data to third party for profit without consent) or where there is a direct and serious violation of explicit direction issued by the DPA to a particular data fiduciary. However, it would be desirable to invoke the extant legislative provisions to deal with such offences rather than criminal consequences under the Data Protection legislation.

vi) Section 36 provides for appointment of a Data Protection Officer to carry out various data protection functions. As per Section 95 (offences by companies), in the presence of data protection officer (who is to be appointed as per the proposed bill), in case of any alleged offence by companies, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence, which would mean that the entire board of the company could potentially be made responsible/liable for the breach which should not be the case. This needs to be harmonized and clarified to limit the liability to the accountable persons only.

vii) There is a need to have a parallel development of enforcement of laws, where unscrupulous people taking technological advantage, commit data theft no matter how robust the systems and processes are. In the event there is sufficient due diligence and checks and balances have been deployed by the data fiduciary/processor, they cannot be unnecessarily penalized. In the absence of mens rea, the recommended penal provisions in the bill having implications of personal liability are un-justified.

viii) W.r.t Section 75 (4) and (5) (Compensation), the Compensation should be granted on the basis of principles of **actual** loss suffered.

ix) In Section 75 (5), it is not clear why each data fiduciary or data processor may be ordered to pay the entire compensation even if they may not be entirely liable. The liability and the

mandate to compensate should be based on the extent of liability that is cast on the offending party.

K. Data Protection Authority

The move towards establishing a dedicated Data Protection Authority (DPA) is important and will go a long way towards ensuring that individual rights are recognised, and personal data is only processed responsibly by all stakeholders. However, for this result to occur, it must be ensured that the DPA is suitably focussed on its role, is sufficiently empowered, and possesses the requisite technical expertise to address the issues which may arise before it. Within this context, there is potential for the DPA as conceptualised under the Draft Bill to be improved and reinforced in line with proven global practices. The present structure of the DPA has some critical problems:

i) Empowerment: The independence of a body can be judged by its level of control over its finances and its composition. The independence of the DPA may be compromised by its dependence on the Government for finances in the form of grants and appointment of chairperson and members.

ii) **Expertise:** The DPA is a powerful body and has many powers, including setting standards for anonymization, preparing the Codes of Practice, approving intra-group schemes et al.

iii) **Centralisation of powers:** The DPA is vested with broad, overarching powers to discharge quasi-executive, quasi-legislative and quasi-judicial functions. While there is a large mandate provided to the DPA, its limited institutional capacity and judicial checks may lead to draconian use of power by the regulator. In this context, separation of powers by way of separate divisions or entities may help. For instance, there should be separate regulatory, supervisory and adjudicatory divisions.

The Draft Bill provides that the members of the DPA should have specialised knowledge of, and while the qualifications of the chairperson and members of the DPA include the need to have specialised knowledge of, and at least 10 years of professional experience in, relevant areas (Clause 50(4)), the Bill does not provide similar requirements for the appointment of its officers, employees, consultants and experts. A requirement to ensure that such officers also possess a similar level of qualifications will ensure that the DPA makes reasoned decisions based on a sound understanding of all relevant technical factors.

Further, the bill provides for a separate 'Adjudication Wing' of the DPA (Clause 68), whose Officers are required to be persons of ability, integrity and standing, and must have specialized knowledge of, and not less than seven years' professional experience in the fields of constitutional law, cyber and internet laws, information technology law and policy, data protection and related subjects. However, 'judicial experience' has not been mandated as a requisite qualification for such Officers, despite the fact that they make judicial determinations about the rights and liabilities of data principals and data fiduciaries, and whose orders/decisions are appealable to the Appellate Authority (Clause 84(2)).

iv) While Section 67 provides for a coordination mechanism between DPA and other regulators, however, it lacks guidance on the detailed process to be used and for resolution of conflicts if and when they arise.

In view of the above, we recommend that:

(i) the Government should consider providing **financial autonomy to the DPA** and also provide detailed eligibility criteria for the members and Chairperson, and other officers, employees, consultants, and experts in the statute itself. These changes will make the body independent and empowered.

(ii) While the DPA would approve standard contractual clauses or intra-group schemes, it would be best for DPA to recognize similar approvals granted under the EU GDPR (e.g. SCCs, BCRs) or APEC (i.e. CBPR and PRP) as sufficient. This would significantly reduce the bureaucratic burden on the DPA as also would ensure greater global harmonization thereby enhancing the efficiency and effectiveness of such frameworks.

(iii) Gradually evolving the DPA's roles and responsibilities over time instead of overwhelming it with responsibility is the best way to ensure it can effectively fulfil its role. The DPA should focus on building a conducive ecosystem through digital literacy, awareness, providing guidance to start-ups and industry players etc. rather than taking on the role of a law-prescribing enforcement body. Further, in order to better prioritise the DPA's resources, reporting obligations should be limited to highest risk issues instead of the current broad reporting mandates.

(iv) Different sectors of the industry utilise different types of data and depending on their sensitivity, industry privacy practices are best developed specifically for such sector. With legal recognition of self-regulation this can be achieved with self-regulatory organisations defining the process and codes of practice. Such an approach also marks continuity from the existing framework, under Rules 8(3) and 8(4) of the IT Act, Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011.

(v) Checks and balances may be imposed on the functioning of the DPA by prescribing due process within the Bill, along with requiring transparency in its functioning. Due process to be followed by the DPA may include expressly providing the parameters that need to be considered by the DPA for discharging any statutory function within the Bill, including imposing penalties. Ensuring there are rigorous standards for the officers and Chairman of the DPA will increase both the credibility of the organisation as well as ensure effective enforcement of the Bill.

(vi) The DPA should have the power to conduct investigations in the form of data audits, but there should not be a general obligation for fiduciaries to undertake annual audits conducted by registered auditors. This is neither targeted, nor does it reflect the way data protection programmes are often managed globally.

(vii) W.r.t Section 50 (composition and qualification for appointment of members), it would be necessary to examine if the tests laid down in *R Gandhi* Case (from Madras HC & subsequently SC on composition of NCLT/NCLAT) and *Brahm Dutt* Case (in SC on composition of CCI/COMPAT) are being satisfied/met during such appointments.

(viii) W.r.t Section 66 (Search & seizure), unfettered Search & Seizure powers cannot be granted to the Authority without judicial oversight. Such requests were made by introducing Amendment Bills in other statutes (like Competition Act) but were not approved and passed. Such clause is prone to misuse and hence should be restricted by inserting appropriate clauses which require Authority to get necessary Orders from Courts of competent jurisdiction to initiate any Search & Seizure.

L. Grounds of Processing

Under the current Draft, Chapter III details the various grounds on which the processing of personal data may be carried out by a Data Fiduciary. These include consent, Government purposes, compliance with court orders, employment purposes, and other reasonable purposes to be notified. The primary objection to these provisions is as follows:

i) While the provided factors are all valid grounds of processing personal data, there is a **notable omission of processing for the purposes of contract** (or 'contractual necessity'). This ground is important in the modern data economy to prevent disruption of goods and services by the need to repeatedly procure consent for processing from users. Under this ground, where a user enters into a contract, the Data Fiduciary may process data as may be required or relevant for purposes of the contract.

ii) The absence of such a ground significantly complicates the conduct of business online – without addressing a countervailing harm or perceived harm, and additionally takes away user autonomy as enshrined in the Indian Contract Act, 1872. Within this context, the lack of inclusion of such a ground for personal data processing is surprising and significantly out of step with global best practices contained in foreign frameworks. Retaining such an approach will complicate business, result in consent fatigue for users, and disrupt the online economy – while at the same time undermining user autonomy to enter into contracts as they see fit.

iii) While data processing for employment related purposes is a valid ground for processing personal data, this is missing from the grounds for processing of sensitive personal data. Given that Passwords, Financial data, Health data are sensitive personal data, there is a need to recognize processing for employment related purposes as a valid ground for processing of sensitive personal data as well.

M. Data Protection Impact Assessment

There is an assumption within Section 33 that processing that involves "new technologies" inherently carries a risk of significant harm to data principal and, therefore, a Data Protection

Impact Assessment (DPIA) is required in all such instances before any processing can be undertaken. On the contrary, there is no evidence to suggest that new technologies carry such a risk. Implementing a statutory requirement for reviewing the DPIA with the regulator could delay the adoption and growth of new technologies in India. If there is to be a DPIA, we are of the view that, it should only be conducted if there is an assessed risk of serious harm under the general intent of Section 33, and not because of the technology that may be used for the processing.

In addition, this provision could hamper large companies from setting up centers of innovations in India and impact the home-grown startup ecosystem. Section 33, therefore, should be technology neutral and focus on the risk of harm.

Further, there should not be a mandatory DPIA [Section 33 (2)] for any category of data fiduciaries, unless there is an assessed risk of serious harm in a particular case. Even if there is an assessed risk of harm, Section 33 (4) (submission of Data Protection impact assessment) should be made applicable only w.r.t Section 33 (2).

N. Notification Requirements and Purpose Limitations

The Bill incorporates certain 'principles' for processing of personal data, such as 'collection limitation' on the basis of data that is necessary for processing (Section 6) and 'purpose limitation' in that 'personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected.

The Bill also provides stringent criteria for the provision of notice to the data principal while collecting data, and the content of such notice. (Section 8). It burdens data fiduciaries with the obligation to ensure that personal data processed is complete, accurate, not misleading and updated, having regard to the purposes for which it is processed. (Section 9). Further, the data fiduciary may retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed and must undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession. Our recommendations are as below:

(i) This is a highly restrictive approach that burdens the data fiduciary with an unwelcome and undesirable (burden of) interpretation as well as compliance based on vague, broad and inherently subjective terms. The Bill does not provide any specific guidance for the interpretation of these criteria. Vague and ambiguous statutory language will result not only in the objective of the Bill or enactment being open to subversion but also lead to contradictory interpretations increasing avoidable business risk and exposure and consequent litigation.

(ii) Mandating such broad criteria is likely to compromise numerous business models which have contributed to making the internet a domain for knowledge-sharing and commerce, as it puts them on the defensive for taking subjective calls on processing.

(iii) From a user perspective as well, foisting upon the data fiduciary the duty to "take calls" regarding the interpretation of these terms deprives the user from exercising direct agency over the circumstances in which she would want her data to be processed.

(iv) Given that (clear, free, informed, specific) 'consent' (also capable of being withdrawn) is the primary ground for processing of data, which gives primacy to the user to determine when her data should be processed, this provides adequate legal basis and consequently there is no further requirement for a regulatory framework allowing for subjective determinations to be made regarding processing.

(v) Section 9 casts an obligation on the Data fiduciaries to ensure the data is updated/ re-validated for accuracy before sharing with other data processors/fiduciaries. This requires the Data fiduciaries to maintain data integrity of the personal data residing at all entities' ends (including Cross border, where applicable). It is not pragmatic/ feasible and instead, the onus should be on the Data principals as mentioned in SPDI 2011 rules.

(vi) These regulatory restrictions would negate the growing role of Big Data processing as well as Government initiatives under Digital India which rely on processing large amounts of data for service delivery and public interest. Thus, we propose modification of the collection and use limitation clauses, and doing away with Section 12(3) of the Draft Bill.

(vii) While the record-keeping obligation under Clause 34 may be used to demonstrate compliance, Clause 34 (2) provides that the data fiduciary shall maintain records "in such form as specified by the authority". This specifically restricts the flexibility of organisations to devise their own compliant forms of record keeping. Given that the law shall be applicable equally to all, it shall be unfair to have one common standard imposed by the DPA. Instead, records should be kept in a manner that allows them to be produced to the DPA on request, consistent with Clause 11(2). But the manner of form of records should be left to the discretion of the data fiduciary. We therefore recommend deleting this section.

O. Extra-territoriality

The Bill applies to data processors and data fiduciaries established outside of India if the processing is:

(i) in connection with any business carried on in India; or
(ii) systematic offering of goods and services to Data Principals in India; or
(iii) any activity which involves profiling of Data Principals within India.

For clarification and to ensure that this extra-territoriality is consistent with GDPR, the third limb should be qualified with "as far as the profiling is with respect to the data principal's activities within India". Moreover, the Bill should clarify whether the Bill is intended to apply to data processors established in India that are processing personal data of non-Indian individuals under a contract

with a non-Indian data fiduciary as Clause 104 of the Bill implies that the scope of the Bill covers this scenario unless the Central Government grants an exception.

P. Transfer of Personal Data outside India

The Draft Bill requires all data fiduciaries should ensure that at least one serving copy of personal data is stored on a server or data centre located in India and that categories of personal data notified as critical personal data shall only be processed in a server or data centre located in India.

The need for balance of national sensitivities /interests/security and ensuring economic opportunities is also recognized by the Committee, noting that such flows [of data across borders] cannot be unfettered, and certain obligations need to be imposed on data fiduciaries who wish to transfer personal data outside India; further that India's national interests may require local storage and processing of personal data.

The issue of addressing concerns pertaining to the national security and consumer privacy are paramount. There are two aspects, namely, different players in the Information Communication Technologies (ICTs) ecosystem collect, process and store data in servers outside the geographical boundaries of India without any restrictions, whereas certain companies in the ICT space are required to ensure that the data is retained in India. This leads to a situation where the same data can be treated differently basis the categorization of the service provider. The data being taken out of the country also places at risk the data protection and privacy rights of Indians. This results in undue judicial delays even in case of regular enquiries leading to effective dilution of powers of the law enforcement agencies (LEAs). At the consumer level, this gives a sense of insecurity to the consumers, as the protection of their sensitive data cannot be ensured within the existing framework.

The absence of a horizontal data protection framework across all digital entities also gives rise to an uneven regulation as different data fiduciaries are subject to different rules with regard to privacy and data protection. This inequity is most visible in the treatment of telecom service providers and OTT Communication service providers. Whilst the former are subject to license conditions prohibiting sending of user information outside India, the OTT Communications service providers, offering identical services are subject to no such restriction.

COAI has been raising the issue of 'Same Service, Same Rule' relating to the Over-The-Top (OTT) Communication services, so as to address glaring licensing, regulatory and security arbitrage. We are of the firm view that bringing OTT players offering any kind of communication or messaging services through applications under the Indian licensing regime is also essential for addressing various security concerns, maintaining data records/ logs and ensuring security, safety and privacy of the consumer data, as also envisaged under the Draft Bill.

There is a risk of all the laws and regulations being rendered futile if one set of service providers are able to transfer data outside the country with little jurisdiction of the local authorities/ regulators, whilst the other set are subject to strict restrictions with heavy penalties for non-compliance. There

are several service providers today who do not even have a presence in India and yet are able to freely transfer data outside the country. The only way to fully protect the interests of consumers and national security will be through firm laws that are ubiquitously applicable to all digital entities as has been done in several countries already.

In view of the above:

(i) We support the provision in the draft data protection Bill that provides for one copy personal data be stored on a server or data centre located in India and more stringent safeguards for critical personal data to be processed only in a server or data centre located in India.

(ii) We submit that we are in alignment with the Draft Bill which has in-fact adopted a well-reasoned classification of data categories that require data localization in India.

(iii) We believe that any data which is potentially critical to nation's interest or is sensitive customer information, must always be retained within the country to ensure that it is kept secure at all times, is accessible to the authorities should the need arise and cannot be misused by someone else. At a time, when the digital services industry is at an inflexion point, we cannot afford to let consumers think that their data is not secure as this will critically hamper the growth of the industry.

(iv) Further, other regulators such as the Reserve Bank of India and the Telecom Regulatory Authority of India have also mandated localization of certain categories of data for which many applicable businesses are already complying or will comply in the near future. Since there are several online portals which despite having negligible physical presence in the country have a large consumer base, data localization will help Indian authorities to keep a check over such businesses.

(v) Mandating localized hosting of critical personal data in India and requiring one copy of the data to be stored in India would not only strengthen the national security and lead to a sense of assurance for the consumers, but will also allow for efficacious monitoring and enforcement as it would give them access to judicial remedies in case the situation demands whilst ensuring a free and fair digital economy, unlike in the current scenario.

(vi) Specific and narrow restrictions are necessary to protect sovereign interests. Many jurisprudences like Indonesia, South Africa etc. have provisions pertaining to local hosting of well-defined categories of data thereby indicating increasing adoption of additional safeguards by different nations in the interest of national security and industry. In fact, we understand that China has proposed an additional draft law requiring any foreign owned entity to certify that any data taken out of China's borders will not impact national security or interests. Thus, Data localization and restrictions on cross-border flow are globally recognized and are being increasingly practiced by several countries to safeguard their national interests including countries like China, Russia and EU. It is also an evident fact that all these economies have thriving companies in the digital space. Hence the assumption of hardship to Indian start-ups and SMEs etc. may be exaggerated.

(vii) The provisions in the draft Bill will also promote India based cloud technologies and promote investment in India as it will create strong reciprocal demands from other jurisdictions. This will in fact promote development of cloud technologies in India thus not only enabling local entrepreneurs but will also support 'Digital India' programme as well. It will result in job and skill creation in India. Given the scale of the Indian opportunity, the large global cloud players will be keen to invest in India and create local capabilities, thereby benefitting all the stakeholders within the framework of a free and fair eco-system.

(viii) Moreover, unrestricted free flow of data across the borders without any safeguards is not advisable with the growth of data specific crimes, cybercrimes and cyber terrorism. In fact, from the global developments it is obvious that the onus of preventing misuse of personal data is upon us. Data security and primacy of data privacy will be the defining contours of global trade in the coming years. India will in fact benefit from strong data protection and privacy framework, as it will make Indian companies stronger and more competitive in the changing global trade perspectives.

(ix) In this regard, it is pertinent to note that, India is a preferred location of global capability centres (GCC) across industry segments, with increasing investment and employment generation, and, we believe that this preference will only increase with the adoption of a strong data protection and privacy framework, growth of Indian cloud companies and adoption of 'Host in India'. The safeguards in the Data Privacy bill will help strengthen the regulatory certainty and will promote stable and long term investments in the country.

(x) These safeguards besides protecting the national interests will also provide the primary jurisdiction to investigate data breach cases to Indian authorities. This will make enforcement of the new data protection law easy as the enforcement authority will not have to depend on its relations with foreign nations, MLATs etc. to determine the liability of the wrongdoers. Further, by mandating global entities to store data locally, the Indian economy will be strengthened, as data localization will ensure that foreign players operating in the Indian market will have local presence. This in turn, will generate employment opportunities in India.

(xi) The growth and sophistication of data specific crimes, cybercrimes and cyber terrorism is an unwanted by-product of the free flow of data and it makes it imperative that we should take all possible steps to prevent misuse of personal data and data localization is one significant step in that direction.

Q. Critical Personal Data

Critical personal data has not been defined nor has any criteria been set for determining which data will be treated as critical personal data – this should be defined to lend predictability.

R. Personal Data Breach Notification

The Bill prescribes that data fiduciaries inform the DPA in the event of any data breach relating to any personal data processed by the data fiduciary, which is likely to cause harm to any data principal. This provision operates on a very low threshold, and is likely to inundate the DPA with numerous notifications that may have little impact on any data principal. Additionally, this may create a delay in the few cases where the impact is significant, resulting in continued harm to the data principals.

Section 32 places the onus only on the data fiduciary w.r.t personal data breach whereas the breach may have been at data processor's end. This Section, read with Section 11 (accountability) seems to indicate that the entire accountability and liability will be only on the data fiduciaries. We recommend that the entire bill needs to bring the data processor into the accountability, liability and breach framework. Data processor should be liable and accountable if the breach has occurred at the data processor's end. As a general recommendation, we find that the draft bill in many places puts the onus only on the data fiduciary and no onus has been placed on the data processor – this situation needs to be corrected to provide for broad rules/guidelines governing the relationship between data fiduciary and the data processor.

Recommendations:

(i) We recommend that this provision be modified to state that breaches should be notified to the DPA if there is a real risk of significant material harm to principals. We would suggest that there should be ample clarity on the applicable standard in assessing the risk of **impact** or degree of harm (e.g. Australian approach – only when "a reasonable person would conclude that the access, disclosure, or loss is likely to result in serious harm to any of the individuals to whom the information relates").

(ii) Also, the timeline for notification should only begin when the responsible team within the fiduciary is aware of the breach and has a sense of its general significance -- and not when the breach occurs.

S. Offences

W.r.t Section 93 (offences to be cognizable and non-bailable), the offences should not be treated as cognizable and non-bailable, especially when the financial penalty limits are proposed to be implemented. This should therefore be made at least bailable and compoundable. Sec 77B of IT Act should be referred.

T. Accountability and Liability of Data Processor and Data Fiduciary

We note that the liability of data processor seems to be much lesser (than that of data fiduciary). Further, in certain cases Data Fiduciary may be held liable for breaches by Data Processor. Section 11 (Accountability) is silent on the accountability of the data processor. It is proposed that

the accountability of the Data Processor should also be clarified so as to attribute proper liability to correct defaulter. This position may be corrected in the all relevant sections of the bill.

U. Data Trust Scores

While data audits by competent third parties play an important role in validation, probe and review of the real practices with respect to the extant standards, policies and regulations, the proposal for "data trust score based on ratings" proposed in Section 35 seems overly burdensome, especially considering that such rating would itself be based on the criteria specified by the Data Protection Authority. It would not be out of place to mention that such a construct would be predicated on a myriad of factors and is likely to vary across sectors and business context, making a 'one-size-fits-all' scoring mechanism inefficient, as the results (i.e. individual data fiduciaries' scores) would be neither comparable, nor therefore really meaningful.

Further, the data trust scores by data auditors may suffer from subjectivity in the absence of benchmarks for consideration by the data auditors. Data trust scores based on codes of practice by the Data Protection Authority ("DPA" / "Authority") may not reflect the comprehensive set of measures to provide additional safeguards due to the dynamic nature of data management practices. Additionally, data is controlled/ processed by millions of entities across the world. Establishing a systematic process of regulation mandated allocation of trust scores is both unfeasible and impractical. It also runs the risk of the user receiving incomplete or inaccurate information due to the sheer fragmentation with respect to availability and access to user information.

Recommendations:

(i) The data trust score mechanism should not be part of any legislative mandate and the Authority should not be burdened with such additional tasks.

V. Overriding effect of this Act.

The draft Bill provides that [save as otherwise expressly provided under this Act], the provisions of this Act shall have an overriding effect to the extent that such provisions are inconsistent with any other law for the time being in force or any instrument having effect by virtue of any such law.

The telecom license carries certain provision with regard to data protection and security. Further, telecom operators are subject to various obligations:

(a) Obligations imposed by the Unified License Agreement ('ULA') on the licensee, pertaining to data and information viz.
- Types of information that are collected is prescribed by DoT (Cl 39.17 of ULA),
- to take necessary steps to safeguard the privacy and confidentiality of the information so collected from the subscribers (Cl37.2 of ULA),

- to maintain records of commercial, call detail records (CDR) , exchange detail , IP details , for a stipulated period of 1 year. (Cl39.20 of ULA),
- Non-disclosure of the customer information's unless there is consent for such disclosure and disclosure is in accordance with such consent. (Cl 37.2 of ULA.

(b) TRAI regulations such as Telecom Commercial Communication Preference Regulations regarding the unsolicited calls by enabling the customers to register with his/her service provider as Do Not Disturb (DND) customers.

(c) Obligation to facilitate the Government to carry out interception in case of exigencies and in the interest of national security. This was a result of amendment inserting Rule 419 A in the Indian Telegraph Rules, 1951 which mandates that the discretion for interception of any message or class of messages under section 5 of the Telegraph Act shall not be issued except by an order made by the designated government officials in writing.

These provisions should be aligned with the provisions of the Data Protection Bill especially to get parity with the OTT Communication players. Alternatively, these should be deleted from the license and only the provisions of the Bill should be applicable.

W. Timeframe for implementation

The transition provisions in the present iteration of the Draft Bill allow for 18 months for compliance from the notification of the Act. The DPA is expected to be notified within 3 months and then the codes of practice, standards and other rules would be issued and notified, after due consultation no later than 12 months. Assuming the DPA notifies standards and codes within 3 months of its formation, this effectively gives at most 9 months, and perhaps as less as 6 months for the transition. Considering the extensive consultation and preparation that will be needed subsequent to the notification of all compliance requirements, there is need to extend this duration.

We suggest that at least 30 months (2.5 years) should be given for implementation, from the date the Act is notified – in this timeframe, the first year should be where the DPA issues all the guidelines, codes of practice, security standards etc, against which necessary technical infrastructure creation, and compliance can be readied by the data fiduciaries and data processors in the subsequent 1.5 years.

Conclusion

It is key that the law be outcome-driven and focus on building the necessary ecosystem, rather than exclusively focusing on regulating data processing. In the interest of innovation and competition, it is of utmost essence that a framework of accountability through self and co-regulation be propagated.

Within the above context, the draft Bill is a significant step in the creation of a data protection framework in India. On the basis of the above-mentioned grounds, it can be seen that certain

aspects of the Bill are not most suitable for maintaining individual rights and promoting business innovation simultaneously. These provisions must be modified so as to achieve the goals of Digital India and aid the country in emerging as a technology power. There is a need to differentiate between privacy, confidentiality and security – each one of these are different and the proposed data protection bill should be finalized keeping the requirement of privacy at the forefront.