SFLC.IN
K-9, Second Floor, Birbal Road,
Jangpura Extension,
New Delhi-110014
(tel): +91-11-43587126
www.sflc.in

August 25, 2019

To,
The Ministry of Electronics and Information Technology,
New Delhi,
India.

[*Via electronic distribution*]

Sir,
Re: Follow-up Comments on the Consultation on Draft Personal Data Protection Bill, 2018

SFLC.in is a New Delhi based not-for-profit organization that brings together lawyers, policy analysts, technologists and students to protect freedom in the digital world. We promote innovation and open access to knowledge by helping developers make great Free and Open Source Software (FOSS), protect digital civil liberties by providing pro-bono legal advice, and help policymakers make informed and just decisions with the use and adoption of technology.

Our comments on the Follow-up Comments on the Consultation on the Draft Personal Data Protection Bill, 2018 are attached below.

We were surprised to learn that a follow-up consultation is being conducted with comments being sought from a select few participants. Sir, considering the importance of this bill and the fact that the first round of consultation was held with the public, we expect the entire process to be transparent and open to participation by all stakeholders. Conducting a follow-up consultation with a limited set of participants sets a dangerous precedent for the future of public policy in India. We urge you to refrain from holding such a private consultation in future, and ask you to open up these questions to be answered by all stakeholders with a longer timeline to respond to the questions.

With Regards,
Sundar Krishnan,
Executive Director,
SFLC.in

Does the draft Bill impose adequate obligations on the data fiduciary?

The data breach notification obligation under the draft Bill is insufficient as it shifts the responsibility for assessing the potential damage from the data fiduciary to Data Protection Authority of India (DPAI). Under Article 33 of the GDPR, for example, data controllers are required to notify the supervisory authority within 72 hours of a breach, and under Article 34 of the GDPR, data controllers are required to notify the data subjects without undue delay when the breach "is likely to result in a high risk to the rights and freedoms of natural persons". In its current state, the draft Bill does not consider the fact that many forms of harms to data principals can be mitigated if the data principals are immediately made aware of a breach. A delay will be caused by the intermediate step of first notifying DPAI, and then waiting for DPAI to reach that particular breach notification, followed by time required for DPAI to adjudge the significance of that breach and whether data principals deserve to know that their data has been breached. The data fiduciary knows the significance of the data in their custody. In some situations, the delay between the data fiduciary realising that a breach has taken place, and the DPAI telling the data fiduciary to notify the data principals can be long enough to give time to the miscreants to use that information to the detriment of the data principals. This delay, if avoided, could result in protective steps from data principals. For example, if a data breach regarding debit card information takes place, there is no need to wait for the DPAI to first assess the situation and determine whether the data principals deserve to be notified. While DPAI should have the power to issue a direction to the data fiduciary to obligate them to inform the data principal for any breach that has occurred, the data principal itself should have an obligation to inform data principals when the breach has a high risk.

While the Srikrishna Committee Report recommends placing an obligation on the data fiduciaries to provide enough granularity so that access to services is not barred "without necessarily consenting to all or nothing", the draft Bill does not incorporate this suggestion. Without this clause, any consent given by a data principal to monopolistic service providers, dominant service providers or unique service providers would be entirely meaningless.

If a request is made under the right to be forgotten, it should be passed on by the data fiduciary to all other entities that have been provided a copy of that data. The right to be forgotten is insufficient as the draft Bill does not provide a way for data principals to request for deletion of their data. If their data is being held in trust by the data fiduciary, it is only natural for them to be able to request for their data to no longer be held in trust.

The draft bill proposes that all personal data needs to be stored in India whereas significant number of feedback received suggests that restriction on cross border flow of data may be limited to sensitive or critical personal data. Do you feel it is necessary to mandate storage of all types of personal data in India?

In our opinion, it is not necessary to restrict the storage of any category of data within India. The storage of a very narrowly defined category of data such as state secrets could be restricted to India. A detailed study is required on the economical, environmental and opportunity costs associated with storing data within India before taking such a step.

Many developing nations look towards India as a role model for creating their own laws and frameworks. The perceived benefits of storing data locally, i.e. generating new jobs, may potentially be offset by an associated increase in the opportunity cost for Indian entrepreneurs that wish to expand their businesses to other countries, only to be faced with data localization costs in those countries.

Additionally, as we submitted in our comments to the draft Personal Data Protection Bill, 2018 under the heading "Economic Impact of Data Localisation", studies have shown that data localization results in a net negative to the GDP.

Alternative methods to achieve lawful access to data can be developed, as the Internet connects devices across the globe, and any data stored anywhere in the world can be accessed remotely through the Internet. Our first priority should be to fix the MLAT process. This is already happening through global developments like Budapest Convention and other international efforts to standardize digital privacy and data sharing.

The role, scope, powers and authority of the regulator proposed – Data Protection Authority of India (DPA)?

In order to remain consistent with the other answers in this submission and our prior submission on this draft Bill, we have used the term 'DPAI' to refer to the Data Protection Authority of India.

While we have submitted detailed comments on this in our comments for the earlier consultation on the draft Bill, we believe that it is necessary to mention that since the authority is meant to have an oversight on every government and non-government entity that deals with personal data, it must be allowed to operate freely. The draft Bill has diluted the role, scope, powers and authority in favour of retaining powers in the hands of the central government. We must realize that DPAI is meant to have the highest level of expertise in this matter, with oversight over all entities that deal with personal data. In order to be effective in its mandate, DPAI needs to be to have full control and oversight without interference from the government. Many clauses in the Bill defer to the government for the final decision, while we believe that the Authority should have the power to decide on issues such as whether or not another country has sufficient protection for personal data. For more details, please refer to our prior submission on this issue.

What could be the contours of a policy that should govern non-Personal Data such as community data, anonymized data, e-commerce data etc.?

The question presumes that such a policy should exist and leaves no room for reasonable arguments against such a policy. The Ministry must keep an open mind about the very need for such a policy.

On one hand, the draft Bill suggests that data fiduciaries hold data in trust, i.e. they are not the owners of the data. The data still belongs to individuals. If that is the case, as it should be, then no concept of community data can arise from personal data as individuals cannot be forced to give up that which is theirs, except in the form of purely collective anonymized data from which individual entries cannot be retrieved. As long as individual entries can be retrieved, it will remain possible to re-identify that data. For more details, please refer to our original submission on this issue.

Could there be a case for mandating free access to such non personal data such as community data, anonymized data, e-commerce data etc.?

While a case can be made for free and open access to collective anonymized data for research and reporting, the same cannot be said for any form of 'community data' or 'e-commerce data'. These forms of data are derived from personal data without sufficient safeguards for the protection of individuals. The government cannot legally enable private profiteering at the cost of the Right to

Privacy of individuals. Any such clause will be subject to challenge before the Supreme Court of India as a violation of the Right to Privacy.

Should the DPA also be the regulator in respect of all non- personal data?

No comments.

Any other related matter.

The timeline for the Bill to come into force once it has been enacted is too short. EU's GDPR provided two years from 2016 to 2018 to comply with the law, and many companies still struggled with its implementation. Data protection covers a wide variety of activities in a data-related business. The draft Bill provides data fiduciaries as little as 6 months from the time when the DPAI may finalize the compliance requirements for data fiduciaries.

We believe that criminal provisions in the Bill should not include any form of imprisonment, as we have witnessed the misuse of Section 124A of the Indian Penal Code and Section 66A of the Information Technology Act, 2000.

This consultation should have taken place in the form of a public consultation open to all stakeholders. A secret process with selective participants is harmful to the democratic nature of our country no matter what the consultation is about. The issue is compounded by the fact that this is a crucial issue for the future of the rights of people and the economy of the country. All stages of this process need to be open to public. We hope that the Ministry will be more transparent and open with the process in future.