Government of India
Ministry of Electronics & Information Technology (MeitY)

19.01.2018

The Government of India has constituted an Expert Committee under the Chairmanship of Justice B.N. Srikrishna, Former Judge, Supreme Court of India comprising members from the Government, academia, and industry to identify and study the key issues relating to data protection in India; make specific suggestions on principles underlying a data protection framework in India; and to suggest a data protection bill.

The Expert Committee has put out a White Paper on a data protection framework for India and has sought comments from the public. Submissions of responses to the White Paper will be received till 31 January 2018, preferably through the website https://innovate.mygov.in/data-protection-in-India/.

In this regard, MeitY has also decided to conduct stakeholders' consultation meetings in various cities. The third stakeholders' consultation meeting was held at the Indian Institute of Science on 13 January 2018 in Bangalore. Several key stakeholders, such as startups, civil society organisations, industry representatives, law firms and citizens were present at this consultation, where they shared their views and opinions in relation to the various issues raised in the White Paper.

Some of the concerns raised by the participants are as follows:

A. Scope and Exemptions

1. Categories of Data

- Personal data is normally the one by which a natural person is identifiable, reasonably identifiable or highly identifiable. At present, the personal data that is captured through various laws includes demographic data and biometric data. However, with the evolution of data science, new categories of data such as psychometric data, device identity data and access control data, which are also personal data, are emerging. These need to be defined in the law. Further, with machine learning, yet newer categories of data that constitute personal data may emerge.
- There is a need for a strong data classification framework. Dynamic classification should be adopted. Further, security levels need to be defined on the basis of the nature of data.
- The level of sensitivity of data must be the standard for classification of data. Data may be classified as Level I, Level II and Level III. Such classification should be the basis on which policy on access to data, guidelines for impact assessment etc. can be determined.
- Some recommended categories of data: personally identifiable information, sensitive personal information, personal information, anonymised information, pseudonymised information, aggregated information, etc. must all be defined.
- Sensitive personal data may be defined using a non-exhaustive list. Some types of data which were discussed as sensitive personal include biological data, biometric and health data.
- There were diverging views on financial data. While some argued that financial data needs to be specifically protected, some were of the opinion that financial data should not be included in the category of sensitive personal data.

- Data on the energy consumed may be included as personal data since it is highly sensitive in nature. On the basis of the energy data from a household or building, one can gauge when it is unoccupied thus rendering the same vulnerable to thefts, etc.
- The law must account for aggregated/amalgamated data.

2. Entities

- The entities, data controller and data processor, need to be clearly defined in the law to delineate the kind of activities they can perform as well as liability to be imposed on them. Further, accountability must primarily lie with the data controller.
- Liability must be determined on the basis of who is the first receiver of data. Irrespective of where and to whom the data travels down the chain, the first receiver i.e. data controller must be held liable.
- The principle of consent must be applicable to data processors as well.

3. Notice and Consent

- Guidelines should be developed on what constitutes a privacy notice.
- Notice and consent may be improved through tools such as colour coding, pictorial representation, etc.
- The onus on ensuring that the terms and conditions are accessible to the common person must be on the service provider.
- At present there is an illusion of choice. Thus, the Data Protection law must make it clear as to what constitutes as an adequate notice. All barriers to exercise of choice and consent must be tackled.
- Thinking about child's consent is essential. The internet must be made accessible to children and while developing a provision on child's consent one must be mindful. The law must not be overly prescriptive or paternalistic, and a child's autonomy – subject to certain exceptions, must be preserved.
- Emphasis on child's consent was raised in context of children being denied ration because of Aadhaar glitches.

4. Cross Border Flow of Data

- At present, restrictions exist for cross-border flow of data. The law must regulate and permit cross border flow of data.

5. Exemptions

- There should not be blanket exemption. They must be carefully crafted. There may be an exemption from certain privacy principles but not all, depending on the nature of the exemption.
- Some recommended exemptions: employer-employee relationship, research in public interest, public emergency such as natural disasters, etc.

6. Concept of Community Data and Collective Redressal

- The concept of community data was raised at the consultation. It was discussed at three levels.
  - First, it needs to be determined if a community has rights over its data?
  - Second, data for governance i.e. the right of a public authority to access data that may belong to a community.
  - Finally, cross-border flow of data. Once data crosses borders, one ceases to have rights over it. The concept of 'community data' would ensure that people (India as a community) continue to

have rights over such data even when it crosses borders irrespective of how many levels of processing it has been subject to.

- It was pointed out that the concept of community ownership will also prevent corporates from delegitimising rights of people over the data that such corporates have collected and use.
- The concept of community ownership will also permit collective redressal (class action suits). It was pointed out that in a nation where enforcement of the law by an individual is generally a challenge, the law must permit collective redressal – similar to Article 82 of the EU GDPR.

B. Privacy Principles

1. Accountability Principle

- Emphasis was placed on the accountability principle. It was argued that while consent is important, it is not always the solution – especially in the age of big data. Thus, the controller must be made accountable, even when collection and use is on the basis of consent.

C. Regulation and Enforcement

1. Model of Regulation

- The law should not be prescriptive in nature and should allow for a principles-based approach. There should be regulator which is adequately equipped with statutory powers, which at the same time is flexible.
- There must be historical continuity. Section 43A of IT Act 2000 puts in place a co-regulatory model wherein the self-regulatory bodies come up with self-regulatory standards that are thereafter approved and notified by the Government. Such a model should ideally continue.
- A relevant model is the ASCII model wherein the industry and the regulator develop a model of regulation together.
- There were competing observations on the competence of regulator. While someone argued that the regulator with a technical spine must be established, on the other hand it was proposed that the regulator must not handle technical issues. Further, it was proposed that instead of a data protection authority, a data authority must be established. Such an authority would perform the traditional functions of a regulator while also handling the technical issues that exist in a digital economy.
- Harm based model of regulation should be explored.
- An entity similar to the banking ombudsman may be introduced.

2. Breach Notification

- What constitutes a breach must be made clear in the law. Guidelines must exist to this effect.
- Breach should be limited to access (confidentiality of data) and modification (integrity of data) and not include availability of data.
- The concept of breach notification must be carefully thought out. First, there must not exist an obligation to immediately notify a breach because not all prima facie breaches are actual breaches. Instead, there could be a model wherein the controller notifies the breach immediately to the authority, and thereafter seeks permission to investigate such breach within a certain timeline before informing the public of such breach. The authority must determine whether such timeline is reasonable or not.
- The Government must develop a broadcast platform wherein breaches are notified.

- In case of a breach, the first response of the controller must be to secure the data. The law must incentivize controllers to secure data. Further, the material risk standard i.e. risk of material harm must be made applicable for breach notification.
- Arbitrary timelines must not be fixed for breach notification. The controller must have adequate time to investigate.

3. Audits and Privacy Impact Assessment

- The kind of audits and privacy impact assessment for an entity must depend on the nature of data they are processing.
- Guidelines on audits and privacy impact assessments must be provided otherwise compliance becomes a challenge.
- Instead of audits, the law must be obligation-heavy wherein clear penalties are prescribed for non-compliance.
- Public infrastructure must be publicly auditable.

4. Penalties

- While the penalty model works for Non-State actors, it may not work for State actors. Such a regime would be largely ineffectual against violations by the Government. An alternative regime for the Government must be developed in light of this.
- Penalties and liabilities must be clear in the law.

5. Offences

- Aggregated data even if anonymised can lead to re-identification. Thus, re-identification must be made an offence.

D. Compliance

- The issue of compliance with multiple legislations was raised. Further, the law needs to clarify about what happens when personal data is handed to a foreign entity.
- It was suggested that there could be staged compliance - starting off with a policy document before requiring compliance with a full-fledged data protection law.
- Rules for compliance must be slabbed for entities based on categorization - on the basis of revenue, or other criteria such as nature of data collected and used.

E. Other relevant issues

- The law must be based on a dignity framework and use of de-humanising words such as "data subject" must be avoided.
- Modern Artificial Intelligence based on deep learning technique is the future. Data Protection law must adequately account for such technology. Further, the law must encourage innovation.
- A new cadre of professionals such as data privacy consultants must be introduced and promoted. Since the common person may not be able to understand or navigate the law to protect his privacy – there must be professionals who can advise him on how to do so.
- Privacy by Design is important and the law must provide for it. The white paper does not address it adequately. Example of Aadhaar was given where privacy by design has not been applied.
- There needs to be a framework that prescribes how data infrastructure is governed.
- Concerns were expressed that the consultation is not broad-based and only four metropolitan cities had been chosen. The consultation must extend to other non-metropolitan cities such as towns, villages etc., so that it is democratic and adequately representative.