Towards A Regulated Data Economy: Getting The Implementation Right

26th September, 2018 | Electronics & Computer Software Export Promotion Council (ESC)
155, Okhla Industrial Estate Phase 3 Rd, Okhla Phase III, Okhla Industrial Area, New Delhi-110020

EVENT REPORT

Introduction

The Personal Data Protection Bill, 2018 (hereinafter referred to as the "Bill") is the first step towards designing an over-arching framework for securing the informational privacy of the citizens of India. At present, the sharing of personal data is loosely governed by the Information Technology Rules, 2011. The Bill although earnestly envisages, but makes a half-hearted attempt in rightly addressing the concerns and issues therein. Identifying the loopholes with respect to privacy in the backdrop of evolving digital landscape coupled with existing regulatory capacities and constraints, requires in depth consultation with stakeholders, which has been given a miss.

CUTS International in association with The Dialogue organised a roundtable titled 'Towards A Regulated Data Economy: Getting The Implementation Right', to develop an insight into the key aspects of the Bill, along with an assessment of its scope, intent and implementability.

The functionality of the Bill requires a holistic analysis as it assigns variable rights and duties upon the stakeholders in furtherance of its objective to foster the relationship of trust. The new paradigm seeks to balance itself on the plank of trust and binds stakeholders in a fiduciary relationship in order to safeguard privacy. Further, the institutional constraints within the digital ecosystem at present, which the Bill seeks to address, need to be assessed in light of existing regulatory capacities and constraints therein.

The roundtable witnessed participation from law enforcement, government stakeholders, internet companies, public policy think tanks and global business strategy firms. Eminent Speakers included Mr. Varun Kapoor IPS, (ADGP) Director, PRTS Indore; Gautam Vohra, Hike; Kazim Rizvi, The Dialogue; Adnan Ansari, Associate Principal, Albright Stonebridge Group; Charu Chadha, Facebook; Pranav Mehra, Snapdeal; Divya Dwivedi, Policy Head, UKIBC; Tridivesh Singh Maini, Assistant Professor, Jindal University; Anubhuti Bhrany, Govt Relations Head – HP; DK Sarin, ESC India; Rahul Sharma, IAPP.

The Roundtable discussed and discerned the fundamentals of data driven ecosystem, intent and aspirations of the stakeholders' vis-a-vie the proposed legal framework, regulatory and institutional architecture, and implementability thereof. It invited views and suggestions from multi-stakeholder community and will incorporate them in our submissions to the Government (MeitY).

Summary of the Discussion

The stakeholder consultation was divided into two sessions. The first session **"Rights & Responsibilities of Data Principal, Obligations of Data Fiduciary, and User Rights"** focused on:

- Consent architecture
- Grievance redressal mechanism
- Enhanced personal entitlements - User rights

Whereas the second session **"Regulatory architecture & Institutional uncertainties"** focused on:

- Data Protection Authority/ Data audits/ Data Protection Officer
- Governance and surveillance
- Data Ethics- A marriage of Privacy and Data Protection
- Data Localization

Session 1: Rights & Responsibilities of Data Principal, Obligations of Data Fiduciary, User Rights

Newer emerging technologies such as blockchain and AI presents newer challenges and changing realities and facets having a corresponding impact on the consumer's perception on data economy and digital economy. It was deliberated that the Bill ought to have the flexibility to deal with such dynamic changes and be able to keep up with the technology.

- **Consent Architecture**

Touching upon the consent architecture, fundamental questions were raised as regards to its functionality and implementability. It was pointed out that there is confusion in relation to the stage at which the consent should be required from the data principals. Whether it's the data collection stage or before processing data needs clarity. It was indicated that there was lack of clarity on the scope of processing as well, as the language of the Bill includes collection within its meaning.

Moreover, there is no certainty as to who will bear the cost of maintaining the data infrastructure ultimately. It needs to be assessed whether it will trickle down to data principals.

It was asserted that the duties emanating from the rights bestowed upon the consumer should not overburden them. Also, the consent framework, which is extremely elaborate, granular & multi-level in design, should seek to balance the rights and duties of the stakeholders

It was outlined by the industry that consent forms are being designed keeping user's interface and user experience in mind. Pictorial and graphical presentation could be used to walk through the privacy settings, which engages users more constructively in understanding the context. Also, the

language of privacy setting should be simplified keeping in mind the socio-economic and cultural context of the user.

The implications of equating consent forms with a product raises the liability of a data fiduciary, and might lead to rise in cost of services was also discussed.

The consultants voiced their opinion in the context of consent and product liability. It was pointed out that the onus of taking consent should not be shifted to the user at any given point because if the technology overburdens the user, they give it up. Organizations should be more open and transparent with their policies. And the Bill should be in vernacular languages and vernacular consent forms would help cater to different kind of consumers.

Another important detail that came out from the discussions was maintaining valid consent throughout the user's interaction with a product or service. The point was substantiated by taking a case of a user purchasing an item from an e-commerce website. First, they might choose to type their preference in a search engine which takes them to the website of their liking. After scanning through the items, they choose to select the ones they like and click on "Buy Now". The e-commerce website then redirects the user to a payment portal after which the user is redirected back to the website. In this process, there is also an access of the logistic chain partner. The situation demands to have clearly defined consent throughout this entire chain of process. For a data fiduciary, there should be a clear outline on how many features and third-parties are built in to create a new product.

This would also facilitate an organization to be more open and transparent with their policies. Additionally, users should also be notified of any further data analytics usage by the organization. An organization should induce transparency and visibility as to when is the product/service using a user's consent and for what purpose and extent was noted as an important facet.

- **Product Liability**

It was pointed out that equating a consent form with a product creates liability on data fiduciary at all times, while holding on to the data of the data principal. Consequently, the data fiduciary will continue to have liability for any harm caused to the data principal on account of the data being given to him. This further enhances the liability imposed on the data fiduciaries for it has to ensure that the consent is properly obtained. The presence of pre-ticked boxes, non-appearance of the notice at the required time, or the use of the data for purposes not reasonably expected by the data principals are some of the harms outlined by the bill and need to be taken care of while seeking consent.

It was opined by the industries that this framework will not only increase the cost on the business, but also the user. Voices were heard in support of awareness generation drives on behalf of data

fiduciaries among its users about consent, product liabilities and privacy. This will again add to the costs, which might pass down to users.

- **Grievance redressal mechanism**

It was pointed out that the grievance redressal mechanism was one of the ways for the individuals to exercise their rights. And it was unanimously agreed that the Data fiduciaries must adhere to grievance redressal mechanisms for managing complaints. And in case of breach, the data principal should be notified within a time frame with due reasons for the breach, and the immediate actions taken by the data fiduciary in remedying the breach.

There were concerns as to whether the grievance redressal framework allowed a consumer to directly engage in the process without seeking the help of a lawyer which creates an additional cost and burden on the user.

It was highlighted that institutions like Grahak Suvidha Kendra (Consumer redressal centres), need to be established which help lessen the burdens on consumer courts. A consumer can approach the Kendra which can make them aware about their rights and help navigate the grievances redressal mechanism thereby enhancing the efficiency of the right to redress

It was also pointed out that a grievance redressal mechanism should be accessible to people through various channels like helpline numbers, chat-bots, emails, etc being few examples. Grievance redressal system should be accessible to people. A correct mechanism and process pipeline has to be identified.

Moreover, it was noted that the citizens often view tech products with suspicion. They feel they are not the 'users of the product', they are the 'product' and that their data is being sold. Therefore proper grievance redressal will increase trust factor. Some inspiration could be taken from the mechanisms under the Consumer Protection Act, wherein consumer courts have the rights of civil courts but are not necessarily bound by their procedures.

- **Enhanced personal entitlements - User rights**

It was pointed out that the user rights come with an added economical cost and legal consequences upon the data principal as well as data fiduciary. The right to withdraw needs to be understood before exercising it as it could attract costs and legal consequences upon either or both parties involved in the transaction.

It was also noted that the right to data portability can barely be functional in the current market structure, and the same would need to be incentivized by the government to be operational in future.

Session 2: Regulatory architecture & Institutional uncertainties

There were points raised regarding the functionalities of The Data Protection Authority of India and how government will ensure its transparency. It was added that the DPA should have a separate wing for adjudication and administration. The current structure is way too centralized in nature, which needs segregation for better functionality.

- **Data Protection Authority/ Data audits/ Data Protection Officer**

Many concerns were raised as to whether a DPA in India would ensure fair inclusion of interests of different stakeholders, in order to design provisions informed by practical challenges. Such a measure would also foster shared ownership and enhance voluntary compliance. It was highlighted that transparency in the functioning of DPA is paramount to develop trust within this ecosystem ensure its independence.

Monitoring cross-border transfer of personal data is one of the functions of the proposed Data Protection Authority of India (DPA). Such monitoring of cross-border transfers of personal data would be time consuming and might hit the pace of businesses. The DPA while performing the twin function of monitoring and adjudication might be overburdened, and therefore a capacity assessment of the body should be done. It was suggested that having regional offices of DPA in this respect might help Moreover, the roles and responsibilities of the Data Protection Officers (or equivalent thereof) to be appointed by the data fiduciaries were discussed. Lack of clarity on accountability of such DPOs was highlighted. Concerns with data audits and data trust scores were also pointed out. It was mentioned that such scores could remain subjective and unclear and might not be the best mechanism to inform users of the data protection tools employed by data fiduciaries.

It was pointed out that lessons could be learnt from other jurisdictions like Singapore where the government has announced the Data Protection Trustmark (DPTM) scheme, under which Singapore-based firms will be able to get officially certified for their data protection measures. The certification will assure clients or consumers that their personal data is being securely handled. The company will be judged based on four principles developed by the Personal Data Protection Commission (PDPC): governance and transparency, management of personal data, care of personal data, and individuals' rights. The challenges of having a trust score based system were discussed, along with deliberations on what alternative mechanisms would work in a country like India.

Outcome from these discussions also entailed resources to be spent by a significant Data fiduciary on maintaining a DPO and the extent of accountability of the DPO in case of a default mistake. And therefore the Bill must also clarify the role and responsibilities of DPO as it reports directly to the DPA and does not fall in the hierarchy of a typical organizational structure. It was suggested that cues could be taken from EU-GDPR, where the role of a DPO is mandated to be segregated from a

compliance officer. The DPO should act as a facilitator between a data fiduciary, the DPA and most importantly, the end consumer/user.

Evidently, the discussion trickled down to the issue whether the body of DPO should be made mandatory. Drawing an analogy with the professional or a compliance body like company secretaries, it was noted that there is a possibility that the DPOs might develop into a professional body, like in the case of insolvency officers. The point raised a question whether an independent body status should be assigned to the collective DPOs.

- **Localization**

It was noted that even if the data is localized and stored within the domestic territories, the issue of access to data would still remain unless due process of law allows speedier access to such data.

It was opined that although, there are data investigation processes already in place, vital data that pertains to the security of life and property to the citizens may be stored locally, but the costs will be significant that may be borne by the user. Other data (data not vital to national importance) should have mechanisms in place to facilitate data access by the governments, whether through a mutual legal assistance treaty (MLATS) or an association of countries participating in free-flow of data. The issue of equivalence between EU GDPR and the Bill was raised along with the need to develop an understanding on the points of divergences and similarities between the two legislations.

It was added that a bottom up approach would make more sense instead of going top bottom. For example, Telangana has an opposing view of data localization. Allowing the states, districts, SMEs and startups decide their respective data localization requirements would be a good step. It was pointed out that Cooperative federalism should not only be practiced in domestic issues but also in foreign issues and policies. Identifying important local stakeholders is a key to sustainable solutions..

Key Takeaways

It was felt that the committee has rushed into designing a data protection framework, without exploring other and possibly better alternatives suited to Indian democracy. An evaluated approach has to be taken for evolving specifics in each industry and data type by consulting key stakeholders. Aspects of improving the ease of doing business, in terms of infrastructure and regulatory constraints and capacities, coupled with incentives to operate in the country will need more attention and detailing.

Although access to data by the law enforcement agencies is genuine, doing so along with evaluating the risks to data privacy could help assuage the fear. Additionally, surveillance reforms with adequate checks and balances, along with an independent oversight should be put in place. There needs to be

a legal basis, coupled with the principles of necessary and proportionality for infringing the privacy of an individual.

Way Forward

The bill marks a positive step in the direction of securing and enhancing data privacy of its citizens but it is far from achieving its intended objective of free and fair digital economy. The bill needs to put in place strong pillars of transparency, accountability, and decentralization. The welfare state needs to be the pioneer of following gold standard of protecting and ensuring the right to privacy of its citizens.

Further, the regulator should ideally take a principles based approach and have a risk-based supervision in place informed by pragmatism. Moreover, due to information asymmetry, the regulators should use a pyramidal bottom up strategy, incorporating an ex-ante analysis of harm and risks, with respect to consumers, as eventually every other stakeholder is also a consumer at the end of the day in some capacity. Accordingly, undertaking Regulatory Impact Assessments (RIA) or Cost-Benefit Analysis (CBA) of the proposed mandate becomes imperative in order to map its impact on various stakeholders before its enactment.

Moving forward CUTS wishes to conduct an informative/educative workshop(s) on different set of issues regarding the developments made on the front of data protection & privacy in the coming months. It would serve the purpose of informing and building capacity of the Consumer and Civil society organizations spread across the country while placing the user/consumer interest at the center of the discourse. The workshop would help enhance and evolve the body of knowledge existing within the data privacy and protection network. And in addition to the above, it would also be productive in churning out actionable and practical tools of engagement models, methods and mechanisms, which could be further utilized to aid the users/consumers to become more empowered in the on-going development of the data privacy & protection.

The learnings and takeaways of the discussions of the event may be incorporated by the participants in framing their responses and comments on the draft bill to the Srikrishna Committee.

****