Roundtable on Consumer Sovereignty in Times of Data Localisation
6th September 2018 | Scope Complex, Lodhi Road, New Delhi

Event Report

Introduction

With the backdrop of recent developments in the realm of Data Privacy & Protection such as the Srikrishna Committee recommendations and the Draft Personal Data Protection Bill, CUTS International organised a roundtable to discuss and discern the contemporary challenges and benefits hinged to the issue of Data Localisation[1]. Data localisation is a means to achieve data sovereignty, wherein it requires every entity involved in processing of personal data (Data Fiduciary) to store one serving copy of the personal data on a server or data centre that is located within the territory of India.[2] The theme of the roundtable was 'Consumer Sovereignty in Times of Data Localisation', which highlighted the need for safeguarding consumer and their rights. Aspects of balancing the interests of all the stakeholders, i.e. consumers, businesses and the government alike, along with deliberating the possible alternatives to the proposed Data Localisation regime were also discussed.

The event witnessed constructive discussions with diverse stakeholder groups comprising Government Representatives, Policymakers, Civil Society and Consumer Organisations, Academia, Industry Players (Foreign and Domestic), Think Tanks, Media Personnel etc. Some of the eminent participants were Usha Ramanathan, Independent researcher & expert, civil rights; G.V Srinivas, Joint Secretary, Cyber Diplomacy, Ministry of External Affairs; Nikhil Pahwa, Founder, Medianama; Prasanna, Lawyer, Supreme Court; Smriti Parsheera, Consultant, National Institute for Public Finance & Policy; Ashim Sanyal, COO, Consumer Voice among others.[3]

[1] Agenda for the roundtable can be accessed at http://www.cuts-ccier.org/pdf/Agenda-sept6-2018.pdf

[2] Section 40 of the *Personal Data Protection Bill, 2018* mandates data localisation.

[3] List of Participants of the roundtable can be accessed at http://www.cuts-ccier.org/pdf/Participants_List-sept6-2018.pdf

Summary of the Discussion

The event unfolded with a round of introductions followed by a presentation by CUTS, which set the stage for deliberations on the issue of data mirroring and localisation, from the lens of consumer sovereignty. Broadly, the discussions led to a debate on the positive and negative impact of data localisation, which were judged on various parameters.

Security risk due to vulnerability of undersea cables-

- It was advised that the same measure of analysis of security threats need to be looked into for housing data within the country as done for data moving outside. It was also mentioned that there has been no study so far which shows data localisation mandate enhances security and alleviates associated risks.

Effect on latency & cost of services-

- Although some agreed that the localisation would help reduce the latency cost in some cases, but cumulatively, the same would be overshadowed by the overall increment in costs. It was pointed out that the reduced costs are owing to the scale of options available globally. Also, at present the reliability of services and connectivity is already an issue in India. Independent Data Centres are not allowed at present to connect to NIXI (National Internet Exchange of India) which gives rise to rent seeking behaviour on behalf of Internet Service Providers (ISPs) & telecom industry. And history stands as an evidence that the cost eventually transfers to the consumer.
- It was opined that consumers do not care where their data is being stored, and were only concerned with how it is being used and protected. Moreover, it was understood to add more cost, which could eventually trickle down directly or indirectly to the consumers, and could also affect the cost & quality of services. However, credit was also given to the Bill, with respect to sparking a debate on the issue.

Access speed-

- Upon discussing whether data localisation is needed to enhance access speed, it was pointed out that there exists a parallel CDN industry (Content Delivery Network)

which behaves like a proxy internet channel. It not only enables the quality of service but also high speed delivery, quicker access to content. In this backdrop, data localisation mandate was found not only redundant but hampering the prospects of an already existing industry.

Impact on Industry-

- It was believed that mandating data localisation will raise entry barriers to the market in India and may adversely impact a variety of smaller domestic stakeholders, such as start-ups, Micro Small and Medium Enterprises (MSMEs) and other data driven industries such as software export, Information Technology Enabled Services (ITES) and Business Process Outsourcing (BPO) etc.
- The ecosystem may have disruptions in socio-economic settings due to ripple effects. It could start a trend favouring the existence of one kind of entities due to their sheer might of capital, initiating new lines of division within the industry.
- Several risks were pointed for small industry players which could have an ill effect on their functioning like, restricting their access to the use of the latest technological advances, fears of long-term adverse impact on innovation and economic growth, giving rise to rent seeking behaviour.
- It was pointed out that data localisation may fuel concerns related to digital colonialism with smaller local players being left out. This was because the large foreign companies will be able to mobilise the requisite resources to invest in setting-up their Data Centres (DCs) within India, though the same may not be possible for smaller domestic companies. The possible enhanced costs of setting-up or renting such infrastructure along with the absence of cheaper foreign cloud services may dent their business interests. However, it was also pointed out that large foreign businesses may decide not to serve India instead of getting into the hassle of data mirroring and exclusive storage (if required), thus resulting in loss to consumers.
- Data Centres being at a nascent stage in India needs careful examination and could use regulatory sandboxes to avoid creating tremors and hampering future prospects with mandating hard data localisation. The legal procedures also have to be spelled out clearly to warrant access to data in a transparent manner having regard to due process of law.

Infrastructure cost & readiness-

- India may not be ready to support large scale data centres (DC) in the country. It was opined that adequate infrastructure in terms of energy, real estate, and internet connectivity also needed to be made available for incentivising DC operators to set-up base in India. It was considered that India presently lacks the requisite infrastructure for operating and establishing data centres which would ensure fool proof security of data.

Broken Mutual Legal Assistance Treaty (MLAT) needs an alternative-

- There was consensus in admitting that the MLAT framework is broken as it has not been able to keep up with the evolving space of data protection and privacy and therefore needs to be revamped. However, it was also asserted in the same breath that this was not a substantive ground for mandating localisation without exploring other alternatives to have a jurisdictional hook on the data of the subjects within the country.

Security risks & preventing foreign surveillance-

- This was touted to be a valid ground of mandating localisation. However, counter arguments of this view with respect to the possibility of enhanced mass surveillance by the local government were made. A discourse surrounding the cyber-security issues for data protection followed, where it was advocated that a risk analysis must be conducted to determine the security risks of storing data outside the country or within the country.
- India is ranked 23rd in the UN ranking for cyber security. The fact was highlighted to question India's potential and preparedness in addressing cyber security risks while it considers housing the data within its geographical borders.
- It was also stressed that the consumers should be allowed to exercise their 'right to choice' in case of storing data with an entity/location offering the best standard of security in safeguarding the rights of the consumer. Privacy of consumers should be an important facet of doing legitimate business within this space. Inadequacy of the number of cyber-security experts in the country was also highlighted.

As per the industry, and civil society and consumer groups, data localisation is more likely to be counterproductive not only to the interest of the consumer but to the whole society. The argument also extended to question the basis of mandating data localisation as it does not meet the objectives, as stated in the recommendations. It neither addresses the issue of safeguarding privacy nor does it add value in enhancing security.

The Bill doesn't address or settle the issue of personal data being seen as a tradable asset. It was emphasised that privacy has been defined as fundamental right, and not as a property by the Puttaswamy judgement hence it could not be traded. Moreover, the Bill sets the standards for conducting business in relation to various kinds and forms of data, making the assumption that data is a resource. And in the name of data security, it omits to address the core issues and digresses towards hard mandates having irreversible ramifications. The need to analyse the interaction between data privacy and data localisation was highlighted.

Issues pertaining to the disabling regulatory frameworks governing DC operators were also discussed. This led to extant debates on whether businesses should be forced to localised data, or be let free to choose the most cost effective and technically efficient geography to store data. Therefore, the government needs to make some regulatory changes, if the bill was to be passed in its current form.

Talking in favour of data localisation, few suggested that the Srikrishna Committee has been very sensitive towards securing consumer's data, as it seeks to empower common consumers.

Key Takeaways

The key takeaway from the discussions was to make the regulation making process more balanced and pro-active, instead of being merely a reactive one. Regulations can have varied and divergent impacts on different stakeholders, and it is thus necessary to ensure that in the process of achieving its objectives, the costs imposed by regulation on stakeholders do not outweigh its benefits.

It was felt that the committee has opted for a populist method to achieve data sovereignty, without exploring other and possibly better alternatives suited to Indian democracy. The bill ought to have taken the least restrictive and viable path to achieve the desired outcome.

Aspects of improving the ease of doing business of data driven businesses, in terms of infrastructure and regulatory frameworks, coupled with incentives to operate in the

country and incubating domestic data driven innovative start-ups will need more attention. An evaluated approach has to be taken for evolving specifics in each industry and data type rather than simplistically mandating data mirroring and localisation.

Moreover, assumptions and fear ought to be replaced with evidence based research from various perspectives- economical as well as civil liberties. Fears pertaining to mass surveillance in the garb of governance need to be addressed systematically. While the need of ensuring access to data for law enforcement agencies is genuine, doing so along with evaluating the risks to data privacy could help assuage the fear.

Surveillance reforms with adequate checks and balances, inclusive of independent oversight is the need of the hour in this backdrop. There needs to be a legal basis, coupled with the principles of necessary and proportionality for infringing the privacy of an individual.[4]

Way Forward

The observation of the committee must be treated as a recommendation, i.e. *India would have to carefully balance possible enforcement benefits of localisation with the costs involved in mandating such a policy in law*. Accordingly, undertaking Regulatory Impact Assessments (RIA) or Cost-Benefit Analysis (CBA) of the proposed data mirroring mandate becomes imperative in order to map its impact on various stakeholders before its enactment.

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 decentralisation. Further, the welfare state needs to be the pioneer of following gold standard of protecting and ensuring the right to privacy of its citizens.

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.

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 organisations spread across the country while placing the user/consumer interest at the center of the discourse. The workshop(s) 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 Data Protection Bill to the Government of India.

******

[4] The *Puttaswamy judgment* lays down three principles, which need to be followed in order to infringe the privacy of an individual.