CONSUMER SOVEREIGNTY IN TIMES OF DATA LOCALISATION

Monday, 24th September, 2018 | Nishith Desai Associates, 3, North Avenue, Maker Maxity, Bandra Kurla Complex, Bandra East, Mumbai

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 in association with Nishith Desai Associates to discuss and discern the contemporary challenges and benefits hinged to the issue of Data Localisation.

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.[1] The issue of Data Localisation has gained much traction from the business viability perspective and rightly so. Eventually, all costs trickle down to a consumer, and every stakeholder is a consumer too at the end of the day. The theme of the roundtable was 'Consumer Sovereignty in Times of Data Localisation', which highlighted the need for safeguarding consumer and their rights.

The discussion delved into issues like, how will we balance the interests of all the stakeholders, if Data Localisation is mandated given infrastructure constraints; and if not, what are the less restrictive and effective alternatives to the current Data Localisation regime proposed, if any, in light of adjoining issues like access to law enforcement agencies, viability of regulatory architecture and institutional uncertainties.

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 of Government Representatives, Policymakers, Civil Society and Consumer Organisations, Academia, Industry Players (Foreign and Domestic), Think Tanks, etc. Some of the eminent participants were Vijay chugh, Former RBI; Hina Rao, Economic Affairs Officer, US Consulate General; Karan Tekchandani, Analyst, Equanimity Investments; Parag Jain, former SEBI, Independent Consultant; Subramaniam Vutha, Advocate, technology Law Forum; Gowree Gokhale, Partner, Nishith Desai Associates; Amol Kulkarni, Fellow, CUTS & Head C-CIER among others.

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

Summary of the Discussion

The discussion started with a presentation by CUTS, followed with a brief round of introduction. Broadly, the session had a strong flavor of financial sector reforms, along with influence of dominant form of transaction being Business to Business, churned out insightful issues. Following are the list of issues which emanated out of the discourse:

- Privacy has now become a regulatory aspect. The bill recognises data sovereignity and consumer sovereignity, and rightly places the consumer at the centre. The bill also introduces some concepts like informational privacy, which allows the consumer to voluntary share or restrict access to its data.
- Concerns related to privacy are not being raised by the consumers but by the government due to domain related issues in accessing data by law enforcement agencies.
- Free consent has no meaning in India, even for educated people. The user avails goods and services from across the world, and so long its data is secure, the user doesn't care about the storage location.
- Two things should be looked at to begin with- whether India is an outlier and do other countries take similar action in regard to data sovereignty. India is not an outlier as there are many countries who have policies, laws, rules in this regard.
- It is fair to have a mandate to store all governemnt data within the goegraphical boundaries of the country. But the extent of this narrative should have clear boundaries. The types of industries and kinds of data falling within the same rule should be clearly reasoned and specified. Today the PSUs are confused as to whether they fall under governemnt related data mandate or not.
- On storage of payment data in India, the confusion between localisation and mirroring was due to RBI[2] not being able to take a firm stand, as the industry rushed to RBI with a proposal of mirroring. Mirroring doesn't require an entity to take decisions as regards its financial situation, sanctions from authorites, infrastructural requiremnts, etc, as opposed to localisation which would require all of the above among others. Mirroring can be done within a time span of 15-20 days.
- The government and the Law enforcement agencies at present doesn't really have issues with access to data within the geographical boundary of the country. The main intention then behind mandating localisation is most likely to target technology intermediary players, which are not

[2] RBI circular on payments data storage
https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=43574

regulated as of now, and to have a jurisdictional hook on the entities not based in India at present.

- Earlier the institutions were in the middle and the cutomer on the periphery, the situation has reversed today, and therefore the customers demand their share/incentive on their data being used to provide them services.
- The banking model of India at present is going through change. Earlier the question was who owned the customer, but today it is about who owns the data. The banks owned the former, but today the former as well as the latter is not under the sole ownership of the bank, as the data is procured and owned by other intermediary payment companies as well.
- The future holds great promise for users to get paid as well. Earlier the customer would have to pay the bank for providing services, which now gets waived off due to these intermediaries, facilatating transactions without having to pay for those services.
- The territorial process is modifying and changing in the banking domain. At present, it is designed to take commission out of its consumers and hasn't worked out an alternative model so far. For the purpose of ensuring depositors protection, the regulator intends to keep a check on the chain, wherein it selects a settlement bank, and how does the commission or omission of settlement takes place therein. The regulator is now looking at bringing payment settlement fuction under its radar, and not how the entity operates per se.
- The RBI circular on payments data storage talks only of intermediaries, which are in a no man's land. They are not supervised entities yet, and often get sandwitched when a situation crops up to lessen the cost within the value chain. The acquiring and the issuing banks have margins fixed, challenging the space of intermediaries eventually, and therefore they should voluntary demand to be regulated in this backdrop.
- The government must clearly state their intentions, what interests does the intended regulation serve, and what sort of businesses and opportunities are coming up within this space. It needs to be seen whether such regulations cater to all sections of the society, and their capacity to exercise the rights given to them. The corresponding costs and liabilities must not outweight the rights therein. We should be wary of doing things disadvantagously to a certain section of the society.
- Issues should be framed, while being informed of the needs, sensibilities and realities in the Indian context. India should not emulate other country's laws like GDPR, as it has its own history and capacity. India doesn't have the capacity to implement or enforce a complicated law as of today.

- The end result of a legal regime must be contemplated holistically by doing a cost benefit analysis. Localisation doesn't seem to give users better services. Historically, big companies that allowed users to access services globally with cheaper prices would have not entered the Indian market, had there been localisation laws in place then. Innovation would be delayed and hampered due to such hard laws, stifling the competitivenes of the market.
- The issue of localisation is envisaged to most severely hit the Small and Medium sector enterprises mainly. The big companies have the money and a large user base due to which it will have to comply. And the start ups are not yet businesses with an eye on compliance, or having proper accounting in place at that stage. So if the law hinders its growth and innovation, it would merely evade the geography. Moreover, the government usually eyes the visible players, and such start-ups are less than fifteen (15) in number in India.
- India has 1.3 billion population at present. Having said that, the big players might not include India in their intial business plans due to hard localisation laws, which would restrict consumer's access to high level services.
- There is no evidence whether the localisation and other provisions will benefit the local industry or help bolster the start up culture. The start ups are often made to comply without having to weight them in during stakeholder consultations. The large companies have to comply as it is not easy for them to turn away or difficult to comply as compared to smaller companies, which can shut shop in face of hard laws.
- The views from inter as well as intra industry dialogue must be put forth and given fair weightage to all.
- Security concerns and processes would also be affected and will have to be redesigned as data will be de-linked due to localisation, and fraud detection will be definitely hampered through the current process. Moreover, AI requires full data sets to analyse, which poses another question on governments claim of enhancing AI related industry due to localisation efforts. The situation gets more tangled up due to further division of data into different categories like personal data, sensitive personal data, critcal personal data, all having different norms.
- It is often said he who makes the rule, keeps the goal. Most rules are made in foreign jurisdictions, and we simply comply to them. It seems that India has outsourced rule making to them, while importing slog work for us.
- Information Technology (IT) Rules, 2011 emanated from Section 43A of the Information and Technology act, 2000. Several years later, there seems to be no evidnece of enforcement of the provisions therein.

Therefore, bringing in new laws, without being in sync with the reality, might make us more vulnerbale as a nation, and paradoxically endanger us.

- The proposed regime is too vague. The definitions therein are not in place and the bill seems to be iron clad.
- It is often difficult to modify laws and therefore should not be very granular in design. It should define domains, challenges, institutions involved with what issues. The law should be simple and have a co-regulatory approach having a sector specific law, wherein the concerned industry would decide whats beneficial for them.
- We are at a confluence of law, tech, policy, new forms of exercising sovereignty. The situation presents a huge opportunity and need reasoned advise to tread ahead from different stakeholders. The government needs help but is not seeking help. It is trying to achive different objectives from the same law.

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.[3]

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 FSLRC committee set up the government and the recent PSS bill, 2018 also talk of cost benefit anlaysis.

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 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. In the data economy, users are producers of data and consumers of services created through data. They need to be handheld to make India a data rich econom, if not economically rich country. As regards privacy, the rights of the consumer need to be assessed and examined keeping in mind our diversity.

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.

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