Bill Blowup

#1/2019

CUTS International

Draft Personal Data Protection Bill 2018

In the light of Supreme Court of India's Puttaswamy Judgement declaring the right to privacy as a fundamental right, the Ministry of Electronics and Information Technology (MeitY) had constituted a Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (the committee) to draft a proposed legislation, with the objective of protecting personal data as an essential facet of informational privacy. Accordingly, the committee drafted the Draft Personal Data Protection Bill 2018 (the bill), which has been handed over to Shri Ravi Shankar Prasad, Hon'ble Minister of Electronics and Information Technology, but is yet to be introduced in the Parliament. The Bill was released in public domain and comments were invited from interesting stakeholders.

Consumer Unity and Trust Society (CUTS) has already submitted its comments on the bill to MeitY, based on primary and secondary research (Attached as an annexures). A few pertinent issues requiring special attention have been highlighted in this document.

The Bill at a Glance

Highlights

- Provides data principals the right to data portability.
- Mandates data fiduciaries to take reasonable steps to maintain transparency regarding its general practices related to processing personal data.
- Mandates data fiduciaries to put in place proper procedures and effective mechanisms to address grievances of data principals efficiently and in a speedy manner.
- Differentiates between personal data and sensitive personal data.
- Mandates data fiduciaries to provide the data principal with relevant information, no later than at the time of collection of the personal data or, if the data is not collected from the data principal, as soon as is reasonably practicable.
- Mandates purpose limitation, i.e. personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for.
- Provides for setting up a Data Protection Authority (DPA).

Lowlights

- Value of non-automated and/ or offline data is no less than data shared online, however, the right to data portability is not applicable on the same.
- Misses upon making data fiduciaries responsible for raising awareness and providing adequate data protection tools to data principals.
- Grievance redress mechanism in the Bill falls short of ensuring transparency and accountability, a clear time frame for resolving complaints at every step of the process.
- Consumer perspective not considered while establishing 'identifiability'.
- Issue of consent and notice fatigue have not been addressed adequately.
- Data Localisation/ mirroring mandated without any Cost-Benefit Analysis (CBA). The observation of the Committee was not 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.*
- The adjudicating wing within the proposed DPA is intended to be quasi-judicial body, while the Central government, which is a part of the executive, will prescribe the operation, segregation, independence and neutrality of the wing.

INSIDE

➥ *See 'Action Points' on Page 5*

Introduction

The expansion of Digital Economy is blurring the line between real and virtual world[1], since consumers today spend increasing amount of time online, for accessing information and public services, transacting business, enjoying social life, availing financial services, etc. In doing so, they generate enormous amount of personal data[2], hence concerns about privacy and data protection have naturally come to the fore.

The recent landmark judgement[3] of the Supreme Court that recognises the "right to privacy" (including information privacy) as a fundamental right, stated that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution".[4] Notably, the judgement also clarified that like most other fundamental rights, the right to privacy is not an absolute right. Subject to the satisfaction of the 'just, fair and reasonableness' test, a person's privacy interests can be overridden by competing state and individual interests.[5]

However, unlike many other countries, India presently does not have an enacted data protection law. Though the government had brought the 'Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011'[6], the same were considered to be inadequate for data and privacy protection in the wake of recent cyber challenges.'[7] In light of the above, the government had constituted a committee to make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a Draft Data Protection Bill.[8]

The committee came out with a report titled 'A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians', along with a draft bill. At the same time various sectoral regulations, such as those applicable on ePharmacies, Fintech sector, eCommerce, etc have also been implemented, or have been conceptualised, which complement, and/or overlap with the draft bill.

Though drafting of the bill is welcome step, and contains various highlights as pointed out above; it does fall short in certain aspects, which require it to be revisited. These have been highlighted in this Bill Blowup, along with appropriate recommendations to address them.

Discussion

Consumer Grievance Redress Mechanism: Although only a marginal number of survey respondents perceived to have experienced violation of privacy and data breach, only half of them went on to report the violation to seek redressal. However, the redress mechanism provided under the bill are plagued by various challenges.

The Bill should have a clear time frame for resolving complaints at every step of the process. Although a 30-day period has been marked for resolving the complaint at the data fiduciary level, no time frame has been stipulated for disposing the complaint from the level of the Data Protection Authority and onwards. Also, no action has been proposed against the data fiduciary, in case of not resolving the complaint within the 30-day time period.

It is recommended that the processes adopted by the Data Protection Authority are simple and comprehensible to enable a data principal to take up its own matter. The regulator should also provide regular updates to complainants on the progress of their complaint through a communication channel of their preference.

Differentiating between Personal Data and Sensitive Personal Data: Laudably, the bill separately defines 'personal data' and 'sensitive personal data'[9]. However, the definition of personal data may be subject to varying interpretation resulting in vagueness. It might be useful to provide some examples to elaborate on concepts mentioned in the definition, such as 'identifiability'. In this regard, it will also be important to consider consumer perception with respect to different kinds of data, i.e., the test for establishing 'identifiability' should include a consumer perspective.

Data Portability: The Bill restricts the right to data portability to data processed through automated means. As revealed in CUTS survey, in many instances, data is collected through non-automated means and offline means, such as by doctors through prescriptions, etc. Consequently, the right to data portability (comprising right of retrieval and transfer to other data fiduciaries) should also be extended to such non-automated data processing. Furthermore, the scope of the said provision may also be extended to data collected through offline means.

Notice and Consent Fatigue: Our survey highlighted that at present, a very limited number of users were reading privacy policies. Among those who were reading, most of them did not understand them. The main reasons for not reading the

privacy policies relate to length, language and terminology, among others.

The Bill has rightly laid down important requirements for a valid consent – free, specific, informed, clear and capable of being withdrawn. However, it needs to be realised that this might be difficult given varied socio-economic, education, occupation and demographic factors in a diverse country like India.

Consent should signify informed choice, which might not be the case for consumers at present while accepting notices and privacy policies. This is evident through the lengthy and incomprehensible language of such notices and policies, full of legal jargons. Going forward, businesses should not be allowed to use consent notices and privacy policies as a means to shrug away their liability. Rather the essence behind privacy policies and data collection disclosure must be to educate the consumer about the business' data use practices. In case practices that exist today continue, the objective of specifying principles of consent, as mentioned above, might be lost.

In addition to addressing the issue of privacy policies and user capacity, the concerns with respect to consent and notice fatigue also need to be addressed. It has been observed, that privacy policies are displayed at inconvenient times, which conflicts with the consumers' on-going actions, thereby being accepted without any thought. Added to this, even businesses are to lose on account of consent fatigue, since they run the risk of losing new consumers, who do not take the time to accept an exhaustive privacy policy. It becomes important to understand the implications of the exhaustive list of information to be furnished to data principals (as per the bill); if it is presented in its current form it may lead to consent and notice fatigue.

Need for Adopting Data Protection Tools and Privacy Enhancing Measures: CUTS survey[10] findings showed, that although most consumers were aware of their privacy rights, not many took measures to enhance their privacy or use tools (such as incognito mode, cookie blockers, antivirus, etc.) to protect their data. Common reasons for non-usage of such tools were noted to be lack of awareness, and the perception about their ineffectiveness in protecting data. Difficulty in usage was also flagged by many in this regard. There is, therefore, a need for spreading awareness about the available data protection tools, along with making them more effective and usable. If such tools are best in class, data fiduciaries[11] should be made responsible to educate consumers about their effectiveness, utility and importance, by clearing any misconceptions about them.

Data Localisation: The bill mandates every data fiduciary to store at least one serving copy of personal data on a server or data centre located in India. As per the industry, and civil society and consumer groups, data localisation is more likely to be counterproductive, and it does not meet the objectives, as stated in the Bill. It neither addresses the issue of safeguarding privacy nor does it add value in enhancing security.

Security risks and preventing foreign surveillance seems 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 also need to be kept in mind. Furthermore, India is ranked 23rd among 165 nations in the UN ranking for cyber security index. This fact questions India's potential, and preparedness in addressing cyber security risks while it considers housing the data within its geographical borders. Inadequacy of the number of cyber-security experts in the country also needs to be highlighted in this regard.

It needs to be pointed out that data localisation may fuel concerns related to digital colonialism with smaller local players being left out. This is because, 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.

Most debates on the issue of transfer of personal data outside India, data mirroring and data localisation have happened from the perspective of businesses and government. Consumer perspective on this issue, despite being important, has been mostly ignored. The impact of data localisation on consumers, remains to be checked with respect to various parameters such as data privacy, quality of service, availability of service, innovation, etc.

Data Protection Authority: The adjudicating wing within the Data Protection Authority (DPA) is intended to be quasi-judicial body, while the Central government, which is a part of the executive, will prescribe the operation, segregation, independence and neutrality of the wing. There may be instances where the government itself is a party to a dispute, thereby leading to a conflict of interest. There is, therefore, a need to amend the Bill to make the adjudicating wing truly independent.

Conclusion

- It is recommended, that awareness and capacity building workshops for consumers must be undertaken, in order to enhance the uptake of data protection tools, with support from well-established and credible consumer organisations. Other aspects requiring consumer attention such as knowledge regarding the amount and kind of data shared by them, i.e., scope of data collection and processing by data fiduciaries, etc may also be covered in such workshops. The Bill may mandate such responsibilities on data fiduciaries (considering their level of interaction with consumer's personal data), by incorporating relevant provisions in the said section.
- The Bill could borrow a leaf from the recent Consumer Protection Bill, 2018, which assigns 21 days to decide the admissibility of the complaint from the date, on which the complaint was filed. And if it is not decided within 21 days, the complaint is deemed to be accepted. The Bill could also have explored alternate dispute redress mechanisms, such as mediation and credible and experienced consumer organisations like CUTS can act as a mediator between data principal and data fiduciaries.[12] The redress mechanism should be made accessible, simple to use and should not prove to be burdensome for the consumer. It should offer them multiple channels to register complaints, such as toll-free calling lines, central online portal, email, letter, fax and even in person.
- The test for establishing 'identifiability' should include consumer perspective, i.e., the select range of personal identifiers should be informed by the perception of consumers, and mentioned in the Bill. Also, the use of sole criteria of 'identifiability' for defining personal data needs to be revisited, and other aspects such as perceived sensitivity, or intimacy of data must also be considered. There might also be merit in defining the scope of 'personal data' and 'sensitive personal data' based on consumers perceived risk of misuse, which is not necessarily similar to the 'identifiability criteria'.
- Any rights being given to data principals, such as the right to data portability, must be extended to data collected by all three service providers, i.e., online businesses, offline businesses and the government. In other words, rights pertaining to data collected through automated means, must also be extended to offline data and data processed through non-automated means. While there may be questions with respect to implementability of such provisions, the value of offline data is no less than data shared online. Capacity building, awareness generation and advocacy can help in bridging the existing constraints of implementation of such a provision.
- Notices and privacy policies should be simple, easy to understand and technology should be used to address any doubts that users may have. The users should also be in a position to compare consent notices, privacy policies and practices of different data fiduciaries on indicators like length, availability in different languages, and use of legal language. Relevant information should be publicly available on the web site of the proposed DPA. Also, data auditors might assess the user friendliness of privacy policies, while undertaking audits and providing data trust scores to data fiduciaries.

CUTS' recommends the inclusion of an 'Executive Summary' in privacy policies. In other words, the most important information required at the time of notice for consumers must be formulated in a more participative manner, by taking the views of consumers through primary interaction with them, and creating a feedback loop, in order to gauge their understanding of policy. An approach adopted in the financial sector wherein Most Important Terms and Conditions are highlighted upfront in bold and bigger font size may be adopted. A human-centred design approach can be formulated in this regard, and infographics/ privacy labels may also be designed in this regard.

- 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 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. Furthermore, regulation-making process should be 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. Moreover, assumptions and fear ought to be replaced with evidence-based research from various perspectives – economic, social as well as civil liberties.

Action Points

- Awareness and capacity building workshops for consumers must be undertaken, in order to enhance the uptake of data protection tools, with support from well-established and credible consumer organisations.
- Explore alternate dispute redress mechanisms, such as mediation and credible and experienced consumer organisations can act as a mediator between data principal and data fiduciaries.
- The test for establishing 'identifiability' should include consumer perspective.
- Any rights being given to data principals, such as the right to data portability, must be extended to data collected by all three service providers, i.e., online businesses, offline businesses and the government.
- Notices and privacy policies should be simple, easy to understand and technology should be used to address any doubts that users may have.
- Undertaking Regulatory Impact Assessment (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.

Endnotes

1 *Forbes Article - Augmented Reality: Blurring The Lines Between The Real And Virtual Worlds - published on April 11, 2016 is accessible at https://www.forbes.com/sites/mahindracomviva/2016/04/11/augmented-reality-blurring-the-lines-between-the-real-and-virtual-worlds/#50211a6de015*

2 ***"Personal data"** means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information. Draft Personal Data Protection Bill 2018*

3 *Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others; SC WP(C) No. 494 of 2012 – judgement delivered on August 24, 2017*

4 *Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others; SC WP(C) No. 494 of 2012 – judgement delivered on August 24, 2017*

5 *https://medium.com/indrastra/an-analysis-of-puttaswamy-the-supreme-courts-privacy-verdict-53d97d0b3fc6*

6 *http://meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf*

7 *Mondaq Article – Data Protection Laws in India: The Road Ahead – published on July 1, 2015 is accessible at http://www.mondaq.com/india/x/408602/data+protection/DATA+PROTECTION+LAWS+IN+INDIA+THE+ROAD+AHEAD*

8 *Economic Times Article – Justice BN Srikrishna to head committee to draft data protection framework – published on August 2, 2017 is accessible at http://tech.economictimes.indiatimes.com/news/corporate/justice-bn-srikrishna-to-head-committee-to-draft-data-protection-framework/59870627*

9 ***"Sensitive Personal Data"** means personal data revealing, related to, or constituting, as may be applicable— (i) passwords; (ii) financial data; (iii) health data; (iv) official identifier; (v) sex life; (vi) sexual orientation; (vii) biometric data; (viii) genetic data; (ix) transgender status; (x) intersex status; (xi) caste or tribe; (xii) religious or political belief or affiliation; or (xiii) any other category of data specified by the Authority under section 22. Draft Personal Data Protection Bill 2018.*

10 *CUTS had commissioned a user perception survey pertaining to data privacy and user welfare in India. The objective of the survey was to gauge perception and experience of users with respect to privacy, purpose of data collection, usage of data collected, strategies for data protection, data breach, among others, in relation to data collected by online and offline service providers, as well as the government. A total of 2,400 respondents (10 per cent of whom were non-internet users) were interviewed across six states (one from each region – north, south, east, west, central and northeast) of the country. The sample was distributed between urban, peri-urban and rural areas, with adequate representation of respondents with different education levels, occupations, genders and age groups.*

11 ***"Data fiduciary"** means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data. Draft Personal Data Protection Bill 2018.*

12 *http://www.cuts-international.org/cart/Grahak_Suvidha_Kendra.htm*

For viewing other Bill Blowups, please visit our website: www.parfore.in

© CUTS, 2019. This document is produced by CUTS and is a brief for Parliamentarians in understanding new legislation and enhancing the quality of the debates so that better laws are enacted. Readers are encouraged to quote or reproduce material from this paper for their own use, but as copyright holder, CUTS' requests due acknowledgement and a copy of the publication.

This paper has been researched and written by Sidharth Narayan, of and for CUTS International, D-217, Bhaskar Marg, Jaipur 302016, India. Ph. 91.141.2282821, Fx. 91.141.2282485, E-mail: cuts@cuts.org, website: www.cuts-international.org

Also at Delhi, Kolkata and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland); and Washington DC (USA)