Bill Blowup

#1/2020

CUTS International

The Personal Data Protection Bill 2019

In the judgement of K.S. Puttaswamy vs. Union of India, 2017, the Supreme Court of India (SC) recognised 'right to privacy' as a fundamental right. The Government of India (GoI) had formed a committee to study various issues relating to data protection, which proposed the draft Personal Data Protection Bill 2018 (draft bill). After a round of public consultation, The Personal Data Protection Bill, 2019 (bill) was introduced in Lok Sabha on December 11, 2019, with certain key changes to the previous draft. The same has been referred to a Joint Select Committee of both houses of Parliament for review. The objective of the bill is to 'provide for the protection of the privacy of individuals relating to their personal data', among other incidental issues.

The Bill at a Glance

Highlights

- The bill grants various rights to consumers, such as data portability, correction & erasure of personal data, right to be forgotten & grievance redress.
- Differentiates between personal & sensitive personal data. · Mandates notice requirements, purpose limitation & transparency regarding processing personal data on service providers.
- Bill provides for setting up a Data Protection Authority (DPA).
- DPA has been empowered to create a 'sandbox' to encourage innovation.
- A new concept of consent managers has been introduced.

Lowlights

- Implementation, awareness & capacity building issues remain unaddressed for effective exercise of rights given to consumers.
- Missed making significant data fiduciaries responsible for providing appropriate data protection tools to consumers.
- Blanket exemptions given to the GoI from the provisions of the bill, for processing personal data under various circumstances.
- Consumer perspective not considered while establishing 'identifiability' for the purpose of determining personal data.
- Issues of consent & notice fatigue not addressed adequately.
- GoI, in consultation with DPA, can direct service providers to provide anonymised and/or non-personal data for select purposes. · Details pertaining to 'sandbox' remain unknown & ambiguous.
- The bill now provides for allowing consumers of social media intermediaries to voluntarily verify their accounts.
- Data localisation though minmised but remains for sensitive and critical personal data.

Action Points

- Awareness & capacity building workshops for consumers must be undertaken, to enhance the uptake of data protection tools.
- Scope of data portability should be determined: which data & whose data can be ported, along with privacy issues arising from portability.
- Cost Benefit Analysis, or impact assessment studies from a consumer &/or competition perspective must be undertaken on select provisions, to ensure optimal regulations.
- Independence and accountabilty of DPA must be ensured.
- Notices and privacy policies should be simple, & easy to understand for consumers. Executive summaries may be prepared, and Privacy Labels should be adopted.
- Harsh provisions such as data localisation should be removed, and less intrusive ways of ensuring Law Enforcement Agencies (LEAs) access to data need to be explored.
- Explore alternate dispute redress mechanisms for consumers.
- Greater accountability should be mandated on the GoI, and the exemptions must be pruned down while accommodating for compliance with the principles of the Puttaswamy judgement.
- Regulatory overreach of the bill must be avoided, so as to not strive to attain government objectives that are beyond the scope of the bill.
- Joint Select Committee of Parliament must hold extensive & inclusive stakeholders' consultations.

INSIDE

Introduction

The landmark judgement[1] of the Supreme Court of India 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 of India". 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.[2]

Around the same time, the GoI constituted the Retired Justice Srikrishna committee to draft specific suggestions for its consideration on principles to be considered for data protection in India and prepare a draft Personal Data Protection Bill 2018.[3]

After deliberation on the draft Bill, the GoI recently introduced a revised Personal Data Protection Bill 2019[4] in the *Lok Sabha*. The same has been referred to a Joint Select Committee of both house of Parliament for their review.[5] Also, parallelly, various sectoral data related regulations, such as those applicable to ePharmacies, Fintech sector, eCommerce, etc. have also been implemented, or have been conceptualised, certain provisions of which overlap with the bill.

Though the bill is a welcome step, and contains relevant provisions as mentioned above; it does fall short in certain aspects, which needs to be deliberated upon and revised appropriately. These have been highlighted in this Bill Blow-up, along with appropriate recommendations to address them.

Consumer perception of personal and sensitive personal data

Laudably, the bill separately defines 'personal data' and 'sensitive personal data.'[6] Furthermore, personal data now explicitly encompasses online & offline data and has been broadened to include inferences drawn from personal data for the purpose of profiling, thereby, granting protection to a larger set of data.

However, the definition of personal data may be subject to varying interpretations resulting in vagueness, especially with respect to 'identifiability'. It might be useful to provide some examples to elaborate on such concepts mentioned in the definition. In this regard, it will also be important to consider consumer (data principal) perception with respect to different kinds of data, i.e. the test for establishing 'identifiability' should include a consumer perception.

Furthermore, CUTS implemented a consumer perception survey[7] and found that different users (based on gender, age, years of using internet etc.) perceive different information differently. Therefore, 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 coverage of 'personal data' and 'sensitive personal data' based on consumer's perceived risk of misuse, which is not necessarily similar to the 'identifiability criteria'.

Furthermore, passwords have been excluded from the ambit of sensitive personal data, which may not be in the best interest of the consumers and thus, should be included in the ambit.

Flawed notice and consent mechanism

CUTS survey highlighted that at present, very few consumers 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 related to length, language and terminology, amongst others. The Bill has rightly laid down important requirements for valid consent – free, specific, informed, clear and capable of being withdrawn. However, it needs to be understood that this might be difficult to implement given the varied socio-economic, education, and demographic factors in a diverse country like India.

Going forward, businesses should not be allowed to use consent notices and privacy policies as a means to shrug away from their liability. Rather the essence behind privacy policies and data collection disclosure must be to educate the consumer about the business' data processing practices. Therefore, they must be easy to read for the consumers, so as to be able to understand the intricacy of the privacy policies and be able to make an informed decision. Thus, in case, such practices that exists today continue, the objective of specifying principles of consent, as mentioned above, might not be achieved.

In addition to addressing the issue of privacy policies and consumer's capacity, concerns with respect to consent and notice fatigue also needs to be addressed. The use of sandbox provisions introduced in the bill should be encouraged, to promote innovation in bridging such information asymmetry, and

educate consumers about their privacy by design policy.

The adoption of privacy labels is a useful tool in this regard. These labels may be designed with a human centred design, on the lines of CUTS broadband labels[8] , and also the Bureau of Energy Efficicency – star labelling, which graphically represent key information in a concise manner, thereby overcoming barriers of language and under-capacity for consumers. Service providers (data fiduciaries) may be urged to undertake further research on designing such labels in partnership with leading consumer organisations such as CUTS.

Grievance Redress

Although only a marginal number of CUTS' survey respondents perceived to have experienced a violation of privacy and data breach, only half of the effected parties went on to report the violation to seek redress.

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 service provider level, no time frame has been stipulated for disposing of the complaint from the level of the DPA and onwards.

It is recommended that the processes adopted by the DPA are simple and comprehensible to enable a consumer to take up its own matter. The redress mechanism should be made accessible, simple to use and should not prove to be burdensome for the consumer, offering them multiple channels to register complaints, such as toll-free calling lines, central online portal, email, letter, fax and even in person. The regulator should also provide regular updates to complainants on the progress of their complaint through a communication channel of their preference.

Alternate dispute redress mechanisms may also be explored for effective grievance redress for consumers, such as mediation. Consumer care centres may also be established in this regard, such as CUTS *Grahak Sahayta Kendra,*[9] which act as a consumer-friendly interface between consumers and service providers, in case of any grievances.

Data Portability

The Bill restricts the right to data portability to data processed through automated means. As revealed in the CUTS survey, in many instances, data is collected through non-automated 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 and offline data processing.

The focus must also be kept on the implementation challenges of data portability. These pertain to determining the scope of data being allowed to be ported, accountability of data fiduciaries, privacy risks with portability, and interoperability between service providers, among other unaddressed issues.[10]

Research may need to be undertaken to prescribe an optimal way forward in this regard. Cost-Benefit Analysis (CBA), or impact assessment studies[11] from the lens of consumer welfare, and/or competition amongst service providers may be useful in this regard.

Lack of awareness and need for capacity building

CUTS survey findings showed that although most consumers were aware of the fundamental right to privacy, not many took measures to enhance their privacy or use data protection tools (such as incognito mode, cookie blockers, antivirus, etc.). Common reasons for non-usage of such tools were noted to be lack of awareness and the perception about their ineffectiveness in protecting data. Many also flagged difficulty in usage in this regard.

Therefore, tthere is a need for raising awareness about the available data protection tools, along with making them more effective and usable. Data fiduciaries[12] should be made responsible to educate consumers about their effectiveness, utility and importance, by clearing any misconceptions about them. Awareness generation and capacity building workshops may be undertaken in collaboration with relevant consumer organisations such as CUTS.[13]

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 service providers, rights available and encouraging their effective enforcement, etc, may also be covered in such workshops.

The Bill may mandate such responsibilities on significant data fiduciaries, by incorporating relevant provisions in the said section, and also providing for a Data Protection Awareness Fund (DPAF) with the DPA. Such fund may be utilised on the lines of the Depositor Education and

Awareness Fund (DEAF) and the Investor Education and Protection Fund (IEAF).

Data Localisation

The bill in its new form does not have restrictions on cross-border data flow of personal data, but places data mirroring requirements for sensitive personal data. The same may be transferred with the consent of the consumer, and satisfaction of certain conditions, whereas, the cross-border data flow of critical personal data has largely been restricted.

CUTS study[14] 'Consumer Impact Assessment of Data Localisation'[15] has highlighted the adverse impact of data localization (DL) on consumers in terms of possible reduced uptake of select data-driven services, such as e-commerce, social media and communication services. The findings of the study showed that consumers perceiving higher risks showed lower levels of usage. Also, consumers showing lower satisfaction with innovation and other service attributes depicted lower usage and perceived lower benefits derived from availing these services. The study also suggests that DL is expected to enhance risks of privacy violation, cyber-attacks and data breaches, while adversely impacting the availability of services and curbing innovation.

It is suggested that harsh measures such as data localisation should be removed. The focus should be retained on enhancing consumers' privacy and setting of clear standards for defining the scope of sensitive and critical personal data, while also preventing abuse of discretion in allowing processing such data outside India.

CUTS study 'Digital Trade & Data Localisation'[16] showcased the adverse impact of DL on India's IT-BPM industry, with respect to digital services export. The scope and extent of data restrictiveness may plunge the digital services exports between 10 to 19 percent. This may translate to a shortfall of US$19-US$36bn in achieving the US$1tn economic value potential of the digital sector in 2025. The decline in digital services export will negatively affect the gross domestic product (GDP) by 0.18 to 0.35 percent, causing a shortfall of US$9bn to US$17bn in US$5tn economy objective in 2025. The impact will also extend to investment and welfare with losses of US$18bn and US$2.4bn respectively.

Therefore, a separate policy may be formulated to incentivise processing of data in India, instead of forced DL. With respect to enabling law enforcement agencies access to data, the same could be addressed through the draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018. Nonetheless, India may pursue international cooperation by becoming a member of 'Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime', or enter into bilateral treaties on the lines of United States Clarifying Lawful Overseas Use of Data (CLOUD) Act. A noteworthy recent development that may inspire India is the Digital Economy Partnership Agreement (DEPA) signed between Singapore, Chile and New Zealand, which seeks to enable trusted cross-border data flows between them[17].

Social Media Intermediaries

The bill empowers the GoI to notify certain social media intermediaries as significant data fiduciaries, who would need to provide its users with voluntary account verification options. From a consumer perspective, such provisions may open the door to user profiling based on the online content posted by them, thereby curbing freedom of speech and expression, and violating privacy.

From the perspective of such intermediaries, the provision may impose compliance costs on them, as they may need to provide for a mechanism for user verification. It may be prudent to undertake Regulatory Impact Assessment (RIA) of such provisions, in order to ensure that the costs imposed by them do not outweigh the benefits intended by it and to design better regulatory alternatives to achieve valid government objectives.

Furthermore, the provision indicatively seeks to solve the problem of inappropriate posts through this legislation, which may be considered an overreach, since the issue is already being deliberated upon in the amendments to the intermediary guidelines 2018.

Exemptions given to the government

The bill allows the GoI to exempt its agencies from some and/or all provisions in certain circumstances,[18] enabling the government to gain unaccountable access to personal data. Furthermore, the list of exempted agencies can also be increased from time to time.

Notably, the bill has done away with the government's obligation of processing personal data only in a manner pursuant to law, after satisfying the test for proportionality and necessity, as had been provided in the draft bill. Such sweeping

exemptions, merely based on a written order (that too an executive order and not a judicial one), raise concerns of possible misuse to squelch privacy and free speech, and harm innovation etc.

Apart from such broad exemptions pertaining to personal data, the government has also been empowered to get access to non-personal data processed by data fiduciaries. Such a provision is seemingly beyond the scope of the bill, which specifically limits its scope to personal data. The same also gets expounded in light of a separate committee chaired by Kris Gopalakrishnan, which is deliberating on framing governance norms for non-personal data.[19]

Also, such forced access to non-personal data may infringe intellectual property rights of data fiduciaries pertaining to such data. Evidence-based policy making through tools, such as RIA may be useful to ensure devising optimal regulations, wherein the interests of all stakeholders are balanced.

Proposed Data Protection Authority

The bill does not prescribe any time limit to set up the DPA. This coupled with the absence of transitional provisions as given in the draft bill, may lead to uncertainty for service providers. It may become difficult to interpret if all the provisions of the bill will come into force with immediate effect upon enactment, or in a phased manner. Furthermore, consumers also run the risk of their rights towards their personal data being guaranteed by law, but without any effective machinery to enforce them, or seek remedy against any grievances.[20]

Also, due to excessive control of the GoI on the DPA, the independence of the proposed authority becomes questionable. The composition of the selection committee for the members of the DPA comprises only of officials from the GoI, as opposed to the Chief Justice of India (or a nominated supreme court judge), along with an independent expert, which was mentioned in the draft bill.

Various exclusive powers of the DPA under the draft bill (such as notifying categories of personal data as sensitive personal data, notifying significant data fiduciaries, publishing results of inspections in public interest) are now removed or need to be exercised in consultation with the GoI. This dilutes the powers of the DPA,[21] and also raise doubts of conflict of interest, considering that the GoI is a data fiduciary under the bill.

CUTS work on the draft regulatory reform bill should be referred for establishing an independent and well-balanced DPA, comprising of members with adequate expertise, whose selection process is transparent, while avoiding the possibility of sinecures.[22]

Sandbox

The bill must be lauded for its intent on creating a sandbox for encouraging innovation, the same has not been defined/explained appropriately by the bill. However, further guidelines should be put in place for laying the process for shortlisting/finalising data fiduciaries applying for inclusion in the sandbox. Furthermore, the obligations and accountability of such data fiduciaries may also be laid down in a non-ambiguous manner.[23]

From a consumer perspective, it is imperative for the bill to clearly set out provisions to strengthen consumer protection against any possible privacy risks arising out of experimental operations performed through the sandbox.[24]

Consent Managers

Introducing the concept of consent managers can be seen as a positive step towards empowering consumers with an efficient consent management tool. However, the bill should provide more clarity regarding the standards and mechanism of interoperability to be followed by consent managers. Studies have shown that the use of consent managers as a tool for obtaining consent has been low due to the cost involved for the same and is a huge budgetary hassle for small companies.[25]

Also, various questions remain to be answered such as: are they going to be sector-specific, or generic; how, and will the DPA regulate all consent managers; will they be successful in seeking informed consent from consumers (studies suggest otherwise) etc. The sandbox may be used here for ascertaining the efficacy of consent managers, while also weighing the risks posed by having a centralised consent dashboard.

Conclusion

Given the drastic changes in the current version of the Personal Data Protection Bill, from the 2018 draft, it may be prudent to hold another round of extensive and inclusive stakeholder consultation on it, before the Joint Select Committee of Parliament submits its report to the government.

Also, CUTS' looks forward to presenting its detailed views on the bill, to the Joint Select Committee of Parliament.

Endnotes

1 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

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

3 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

4 http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

5 http://www.businessworld.in/article/Personal-Data-Protection-Bill-Introduced-In-Lok-Sabha-Prasad-Proposes-Sending-It-To-Joint-Select-Committee-/11-12-2019-180194/

6 **"sensitive personal data"** means such personal data, which may, reveal, be related to, or constitute — (*i*) financial data; (*ii*) health data; (*iii*) official identifier; (*iv*) sex life; (*v*) sexual orientation; (*vi*) biometric data; (*vii*) genetic data; (*viii*) transgender status; (*ix*) intersex status; (*x*) caste or tribe; (*xi*) religious or political belief or affiliation; or (*xii*) any other data categorised as sensitive personal data under section 15. Personal Data Protection Bill 2019.

7 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 2400 respondents (10 percent 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. Findings available at: https://cuts-ccier.org/pdf/survey_analysis-dataprivacy.pdf

8 https://cuts-ccier.org/pdf/Brochure-Consumer_Broadband_Labels.pdf

9 https://cuts-cart.org/consumer-care-centre-grahak-sahayta-kendra/

10 https://about.fb.com/wp-content/uploads/2019/09/data-portability-privacy-white-paper.pdf

11 These may be undertaken on the line of CUTS Consumer Impact Assessment of Data Localisation. https://cuts-ccier.org/consumer-impact-assessment-on-cross-border-data-flow/

12 "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. Personal Data Protection Bill 2019.

13 Consumer Awareness Workshop on Data Protection and Privacy https://cuts-ccier.org/consumer-awareness-workshop-on-data-protection-and-privacy-impact-of-personal-data-protection-bill-2018-2/

14 Though the studies were undertaken for more stringent data localisation requirements as in the draft bill 2018, the possible adverse impacts continue to hold water to a large extent with respect to the revised bill 2019.

15 https://cuts-ccier.org/consumer-impact-assessment-on-cross-border-data-flow/ the study involved in depth interaction with 40 subject experts, and a survey of over 1200 consumers.

16 https://cuts-ccier.org/understanding-impact-of-data-localization-on-digital-trade/

17 http://asiantradecentre.org/talkingtrade/unpacking-the-digital-economy-partnership-agreement-depa

18 (*i*) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or (*ii*) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order

19 https://www.medianama.com/2019/09/223-meity-non-personal-data-committee/

20 https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf

21 https://www.dvara.com/blog/2020/01/17/our-initial-comments-on-the-personal-data-protection-bill-2019/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+dvara+%28Dvara+Blog%29

22 https://cuts-ccier.org/regulatory-reform-bill/

23 https://www.livelaw.in/columns/government-powers-under-the-data-protection-bill-2019-a-critical-analysis-151244 & https://economictimes.indiatimes.com/blogs/et-commentary/lets-be-very-clear-about-data/

24 https://www.dvara.com/blog/2020/01/17/our-initial-comments-on-the-personal-data-protection-bill-2019/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+dvara+%28Dvara+Blog%29

25 "How Privacy Tech Is Bought and Deployed" (IAPP & Trustarc, 2019).

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

This paper has been researched and written by Shubhangi Heda and 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)