

Notice and Consent Framework of the PDPB

The Way Forward

Background

The Personal Data Protection Bill (PDPB) 2019¹ under S. 7(1) mandates service providers (data fiduciaries) to give notice to users (data principals) regarding the collection of their personal data with respect to the purpose and terms of data processing, rights available to users, among other details. Furthermore, S. 7(2) prescribes that notice to be clear, concise and easily comprehensible to a reasonable person.

With respect to consent, S. 11(1) necessitates service providers seek the consent of users before processing their personal data. The next sub-section, i.e. 11(2), lays down the principles of valid consent that it should be free, informed, specific, clear and capable of being withdrawn. The concept of consent managers has been introduced under S. 23 of the PDPB, which are required to be registered with the Data Protection Authority (DPA), and seek to provide a centralised consent management mechanism to users.

Shortcomings of these Provisions

Though the above provisions intend to provide useful protection to users against the processing of their data without their consent, doubts remain on the efficacy of the provisions, due to the nuances of notice and consent frameworks.

Lack of awareness of privacy policies: The provisions make a biased assumption of users being cognizant and capacitated of reading and understanding notices of data collection, as well as providing informed consent for the processing of their data. CUTS' user perception survey² on privacy and data protection pointed out that most people don't read privacy policies (notices), mostly due to their exhaustive length. Few users who attempt to read them, do not understand them, due to excessive legalese.

Service providers should not be allowed to use notices as a means to shrug away from their liability of data collection disclosure. On the contrary, the essence behind them should be to inform users about service providers' data processing practices and enable them to compare policies while making their decision.

In this regard, PDPB has omitted the requirement for providing the 'Data Protection Awareness Fund' for capacity building and awareness generation activities which were stipulated in the Draft Bill of 2018.

Notice and consent fatigue: Users today avail of numerous data-driven services. Notices from each of the many service providers might burden users, and they may not be able/willing to spend time reading them (notice fatigue), thereby accepting them without thought.³ A similar observation was also made in a recent study,⁴ which concluded that after the implementation of European Union's (EU) General Data Protection Regulation (GDPR), there has been an increase in consent notices to be accepted by users, which has led to them being fatigued with such notifications. Hence, the bill should include provisions for encouraging innovation in privacy-enhancing technologies pertaining to notice and consent mechanisms that are accessible and consumer-friendly.

Consent Managers: In order to address the issue of consent fatigue, the bill introduces the use of consent managers. This is somewhat similar to the Account Aggregator (AA) mechanism which provides a centralised framework for providing consensual sharing of information with financial service providers through Data Protection and Empowerment Architecture (DEPA). Such mechanisms are new for users and there are concerns

regarding the acceptability of such infrastructure and familiarity of its functioning by users and their adherence to privacy by design policies as proposed in PDPB.⁵

Also, various questions remain to be answered such as: how will interoperability of consent managers be functional as there exists a large number of service providers; are consent managers going to be sector-specific, or generic; and how and will the DPA regulate all consent managers etc. Furthermore, there is a need to weigh the security risks posed by having a centralised consent dashboard.

Recommendations

Data Protection Awareness Fund: PDPB should provide for the creation of a 'Data Protection Awareness Fund,'⁶ which could specifically be used for increasing users' knowledge regarding the mechanisms through which they can better exercise their rights under PDPB. This would also assist in making users more acceptable and familiar to consent managers. For this, there should be a provision for funding experienced and credible civil society organisations to undertake user awareness generation and capacity building activities.

Innovation for User-Friendly Consent and Notice Mechanisms: The sandbox⁷ should be used to promote innovation for consumer-friendly consent mechanisms, like consent manager/dashboards. This will

improve research and experimentation to come up with consumer-friendly designs specifically suiting Indian demographics.

Transitional Provision and Codes of

Practice: The codes of practice⁸ may specifically require the DPA, to hold adequate and inclusive stakeholder consultation for coming up with guidelines for innovation of technology for easily accessible and

understandable notices for users, like privacy labels. Regulatory Impact Assessment (RIA) may also be conducted in this regard, in order to ensure that the costs of regulations, do not outweigh its intended benefits. Also, transitional provision must be introduced for introducing guidelines for consent managers to remove the uncertainty and provide for more predictability for businesses.

¹ PDPB 2019, accessible at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

² Kulkarni, Amol and Swati Punia, "Users' Perspectives on Privacy and Data Protection" (C-CIER, CUTS International, n.d.). Available at: <https://cuts-ccier.org/cdpp/>

³ Rishab Bailey et al., "Disclosures in Privacy Policies: Does 'Notice and Consent' Work?" (New Delhi: NIPFP, 2018).

⁴ Christine Utz et al., "(Un)Informed Consent: Studying GDPR Consent Notices in the Field," *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, November 6, 2019, 973–90, <https://doi.org/10.1145/3319535.3354212>.

⁵ Raghavan and Singh, "Building Safe Consumer Data Infrastructure in India: Account Aggregators in the Financial Sector (Part-2)," *Dvara Research Blog* (blog), accessed on February 04, 2020, <https://www.dvara.com/blog/2020/01/07/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector-part-2/>.

⁶ The same provided under S. 77(2) of the draft Personal Data Protection Bill, as prepared by the BN Srikrishna Committee. Available at: https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

⁷ As provided under S. 40 of the bill.

⁸ As provided under S. 94(2)(h)