Submission to the Public Consultation on the Digital Personal Data Protection Bill, 2022

IT for Change

December 2022

Submission to the Public Consultation on the Digital Personal Data Protection Bill, 2022

IT for Change

December 2022

1. Preliminary - Chapter as a Whole

The Digital Personal Data Protection Bill, 2022 (hereinafter the Bill) has diluted the constitutional basis of personal data protection. The normative moorings of the 2019 version in the fundamental right to privacy and accountability of data fiduciaries for unauthorized and harmful processing are missing in the current Bill.

By limiting personal data protection to a contractual obligation of the data fiduciary, the Bill implicitly embraces a propertarian framework that eschews the right to privacy.

The tremendous imbalance of power between data principals (typically individual users) and data fiduciaries (typically powerful digital platforms with their de facto 'opt-in' tactics) is not acknowledged.

The absence of safeguards against the retention and reuse of anonymized personal data beyond the purpose for which it was originally collected opens up the potential for new risks of individual and collective harms. This is borne out in emerging jurisprudence in the EU General Data Protection Regulation (hereinafter GDPR).

The introduction of a 'deemed consent' framework has resulted in a perverse conceptualization of 'public interest' that may be manipulated by both public and private sector agencies to unjustifiably override consent as a necessary ground for personal data processing.

Recommendation:

The Indian Supreme Court has exhorted that privacy is to be understood in its widest sense – including not just informational privacy, but also personal autonomy. The Preamble and the entire Bill should be revised to reflect the vision of the Puttaswamy judgement and trailblazer legislation such as the GDPR –

recognizing personal data protection as an extension of the foundational human right to privacy. In the context of the Bill, such a rights-based approach would mean ensuring the processing of personal data by data fiduciaries (whether state or private agencies) is strictly delimited through robust safeguards against individual and group profiling and placing the costs of consent withdrawal and the obligation of demonstrating the lawful basis of processing personal data on grounds other than consent squarely on data fiduciaries.

2. Preliminary: Definitions

I. Personal data

The Bill defines 'personal data' as any data about an individual who is identifiable by or in relation to such data. This ignores the risk of indirect identification.

Recommendation:

Replace with the GDPR definition; "'Personal data' means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

II. Data Principal

In the case of children, the Bill erroneously ascribes the identity of data principal to their parent/guardian.

Recommendation:

Consider parent/lawful guardian only as a trustee responsible for protecting the interests of a child whose personal data is being processed. The child is the principal for her data.

III. Sensitive personal data:

Excluding 'sensitive personal data' from definitions precludes possibilities for additional checks and balances on the processing of such data.

Recommendation:

This definition needs to be reintroduced from the 2019 version.

IV. Harm:

Categories such as 'prevention of lawful gain' or 'causation of significant loss' do not adequately cover harm. The Bill also does not account for 'significant harms'.

Recommendation:

Use the definition of harm in the Joint Parliamentary Committee (JPC) Report, 2021 that included categories such as "any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled", and "psychological manipulation which impairs the autonomy of the individual". Introduce the category of 'significant harm' to account for harm that has an aggravated effect.

3. Preliminary: Application of the Act

Section 4(3) exempts non-automated processing of data, offline personal data and personal data about an individual that is contained in a record for at least 100 years from the scope of this legislation. The rationale for why these data categories is undeserving of personal data protection is not clear as privacy risks are latent even in their processing.

Data businesses may claim unjustifiable exemption even in cases of largely automated processes on the ground that there is some manual (non-automated) intervention. In any case, manual processing also poses privacy risks.

There is also no basis for distinguishing offline personal data from online personal data.

Rights in personal data should not be treated as intellectual property rights that expire at the end of a stipulated time period (100 years time limitation clause). Revenue records and land titles that are over a century old and put out in the public domain have been known to aid predatory acquisitions of forest and grazing commons by land sharks, opening up risks of profiling and violation of personal autonomy for vulnerable sections of society.

Recommendation:

Non-automated processing of data, offline personal data and personal data in public records that are over 100 years old should not be exempted from the scope of this legislation. A leaf should be taken out of the GDPR that covers both fully or partly automated processing of personal data, and even manual processing of personal data if the latter is part of or is intended to be part of a manual register that is searchable using special criteria.

4. Obligations of Data Fiduciaries: Chapter as a Whole

This chapter lacks rigor in laying out the obligations of data fiduciaries to ensure lawfulness, fairness, and transparency of personal data processing – principles that are foundational to robust personal data protection legislation. By reducing storage limitation to the obligation of data fiduciaries to remove identifiers from personal data sets (after the initial business or legal purpose of data processing is met), the Bill fails to preserve the rights of data principals from the reuse of anonymized personal data.

'Deemed consent' as a basis for processing personal data gives state agencies sweeping powers to process personal data without any necessity and proportionality safeguards.

By classifying business activities as search engine optimization, credit scoring, fraud recovery and so on as 'public interest' grounds for data processing, Section 8(8) incorrectly equates grounds that may be available to private actors for non-consensual processing of personal data with legitimate powers of state authorities. Additionally, it curiously exempts such business activities from the assessment for determining 'fair and reasonable purpose' of processing laid down in Section 8(9).

The provisions also do not account for any obligation of data fiduciaries to institute privacy-by-design measures.

Additional obligations of 'significant data fiduciaries' who may be processing extensive volumes of Sensitive Personal Data (not defined in the Bill) have been left to the Central Government instead of the regulator.

Recommendation:

This chapter should be re-drafted to establish the normative principles that should guide personal data processing. The 'deemed consent' basis for processing personal data on grounds other than consent should be scrapped. Instead, akin to Article 6 of the GDPR, a new clause on the lawful basis of processing on grounds other than consent should be introduced. For processing on the grounds of public interest, an assessment should be taken to ensure that such processing is proportionate to the legitimate aim pursued. 'Purpose,' 'necessity' and 'balancing' tests are necessary for processing on grounds of legitimate interests.

5. Obligations of Data Fiduciaries: Consent

The understanding of consent in Section7(4) goes against the principle that consent is 'good' only if the ease of withdrawing it is as easy as giving it. Data fiduciaries are obligated to ensure that data principals are able to make an informed choice about the data they are sharing and have clarity about how to withdraw consent. Ironically, by stating that "the consequences of such withdrawal shall be borne by [the] Data Principal", the Bill places an unfair burden on the data principal.

Section 7(5) merely obligates data fiduciaries to stop processing personal data within a reasonable time, after consent is withdrawn. An express restriction on processing within a set number of days is necessary to avoid vagueness.

As per Section 7(5), after the withdrawal of consent, a data fiduciary is obligated to cease the processing of the personal data of the concerned data principal "unless such processing without the Data Principal's consent is required or authorized under the provisions of this Act or any other law". This ends up creating a loophole where data fiduciaries are able to invoke the overbroad 'deemed consent' provision of the Bill as a workaround and continue processing personal data even after the data principal has withdrawn her consent.

Recommendation:

A provision placing express obligations on data fiduciaries for processing of data must be specific in its scope. Elements of purpose limitation, data minimization, and storage limitation must be introduced to avoid 'deemed consent' from becoming an escape clause in case of consent withdrawal.

Providing information about consent withdrawal and procedural clarity about this must be a mandatory obligation on data fiduciaries. The responsibility of informing data principals, including consequences of consent withdrawal, and enabling them to provide free and informed consent, must be placed on the data fiduciary.

6. Obligations of Data Fiduciaries: Deemed Consent

'Deemed consent' framework has been utilized by Singapore, but this law contains guardrails that are missing in the Indian Bill. The Singapore Law considers an individual's consent as deemed to be given, if they have been adequately notified by an organization and given a reasonable opt-out period but have not taken any action to opt out. It also underscores that such deemed consent by notification cannot be used for sending direct marketing messages.

In contrast, the current version of the Indian Bill interprets deemed consent as consent given where there is reasonable expectation that such data will be provided to the concerned data fiduciary. This opens up the risk that data fiduciaries can pursue any kind of data processing, without purpose limitation, data minimization, and storage limitation.

Given that there is no separate definition for Sensitive Personal Data, the scope of data processing 'for purposes related to employment', as per Section 8(7), is expansive. Unlike the 2019 version, the Bill does not prohibit the use of Sensitive Personal Data from the ambit of personal data processing in the employment context, intensifying the threat of privacy intrusions. In the context of data processing related to employment, inclusion of grounds such as "preventing corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information" is not justifiable given that these aspects are sufficiently covered by private law.

Section 8(8) that invokes 'deemed consent' uses an overbroad conceptualization of public interest.

Recommendation:

The 'deemed consent' section should be done away with and replaced with a new clause clearly outlining the legal basis of personal data processing on grounds other than consent, with sufficient checks and balances to ensure lawfulness, fairness, and transparency of data processing. GDPR's provisions for processing personal data on grounds other than consent -- for performance of a contract, a legitimate interest, a vital interest, a legal requirement, and a public interest -- are a useful pointer on this.

7. Obligations of Data Fiduciaries: General Obligations of Data Fiduciaries

I. Section 9(4) does not specify the obligations of data fiduciaries to ensure security of data processing, beyond 'reasonable security safeguards'.

Recommendation:

Pseudonymization and anonymization safeguards as appropriate, and audit of security measures on a routine basis, like those specified in Article 32 of the GDPR should be instituted.

II. Section 9(5) does not stipulate a time period within which data fiduciaries have to notify the Data Protection Board about personal data breaches.

Recommendation:

The Bill needs to stipulate a specific window within which notification about breaches has to be made to the appropriate authority when there are risks to the rights of data principals, like the 72-hour period in the GDPR.

III. Section 9(6) permits the retention of personal data beyond the completion of its original purpose of collection if the data fiduciary removes "the means by which personal data can be associated with particular data principals". There is no obligation to express notice to data principals about their data being retained after de-identification. Further, data principals do not have a 'right to object', unlike in the GDPR.

Recommendation:

Purpose limitation is a core principle of personal data protection and data fiduciaries cannot be permitted to retain anonymized personal data beyond the original purpose, without express notice-and-consent and a 'right to object' for data principals.

IV. Section 9(9) allows data processors who have been contracted by the data fiduciary to enter into further contracts with other data processors, as long as such data re-sharing has been permitted in the original contract with the data fiduciary. This opens the door for privacy violations in third party data sharing given that Section 9(6)(a) does not include any safeguards for processing of personal data from which identifiers have been removed, after the original legal purpose is met.

Recommendation:

Data fiduciaries must be made liable for individual and collective harms stemming from the entire chain of personal data processing. Third party data sharing has to be based on clear consent-based frameworks and adequate purpose limitation.

8. Obligations of Data Fiduciaries: Additional Obligations in Relation to Processing of Personal Data of Children

Though Section 10(3) of the current version of the Bill prevents data fiduciaries from undertaking tracking, behavioral monitoring or targeted advertising directed at children, Section 10(4) allows for exceptions to this rule to be determined for 'specific purposes'. This is an ineffectual safeguard against algorithmic profiling and violation of privacy rights of children, in a context where predatory ed-tech behaviors are becoming commonplace.

Recommendation:

Profiling of children is an issue of grave concern, and a specific provision to that effect is necessary. Article 8 of the GDPR clarifies that Internet services can be provided directly only to minors aged 16-18 years. For children below 16 years, parental consent is essential for the provisioning of such services. Such a differentiation of children in access to digital services will also preserve the personal autonomy of teenage individuals exploring the online space. Additionally, digital service providers could be required to

comply with the standards described in the Age-Appropriate Design Code (like in the case of the UK), to build an internet that is safe and usable for children, while protecting their data.

Parental/guardian consent may not be appropriate in all cases and may even contravene the 'best interest of the child' principle, enshrined in the Convention on the Rights of the Child. The 2019 version contained a provision that "data fiduciaries providing exclusive counselling or child protection services to a child shall not require to obtain the consent of parent or guardian of the child". This exemption has to be reintroduced.

9. Rights & Duties of Data Principal: Chapter as a Whole

Instead of specifying the obligations of data fiduciaries to provide transparent information, communication, and modalities for the exercise of the rights of the data principal, this Chapter perplexingly imposes duties on data principals, causing confusion about the intended target of the legislation. The exhortation that data principals should not bring 'false or frivolous complaints' to the Data Protection Board in Section 16(2) can have a chilling effect given the extensive imbalance of power between data principals and data fiduciaries.

Section 16(3) requires the data principal to furnish information that authenticates their identity when exercising their rights. A potential fallout of Section 16(3), when read with the requirements for authentication that are proposed for users in the Telecommunications Bill, 2022, is the foreclosure of online anonymity and pseudonymous identities. This can impact vulnerable communities that often use online spaces to collectivize and create safe spaces.

The Bill also has an extremely limited conceptualization of the rights of the data principal. The right of data access as outlined in Section 12 does not mandate an obligation on the data fiduciary to provide the information sought in a clear and concise manner that is comprehensible to a reasonable person. Section 13(2)(d) provides a qualified right to erasure that does not guarantee the right to be forgotten. The critical right of data portability has been omitted as has been the right to raise objections to non-consensual processing on the basis of public interest/legitimate interest grounds. These gaps result in a failure to safeguard the full spectrum of rights for data principals.

Additionally, there is no grievance redressal mechanism for the data principal to claim compensation for loss caused as a result of actions of the data fiduciary or processor.

Recommendation:

The rights of the data principal need to be clearly outlined as enshrined in the fundamental right to privacy, and should incorporate the right to data portability, the full spectrum of the right to data access, the right to raise objections, the right to be forgotten as well as a right not to be subject to a decision solely based on automated processing. Section 16 should be removed because the rights sought to be guaranteed to the data principal cannot be contingent on her duties. As such, due process guidelines for redressal cannot be confused with data principal's duties.

10. Special Provisions: Transfer of Personal Data Outside India

Taking a diametrically opposite stance from the 2019 version, the Bill enables the Central Government to notify countries where personal data can be transferred by data fiduciaries, leaving the question of the terms and conditions of such transfer and the criteria that must guide the selection of countries unspecified.

First, the restrictions on cross-border data transfers of Sensitive Personal Data in the 2019 version has been done away with, opening up a Pandora's Box of risks to privacy. Second, there are no clear criteria for determining the selection of countries to which personal data may be transferred. Even in the EU, where an 'adequacy' clause has been put in place to ensure that cross-border data transfers of citizen's personal data are made only to territories which have adequate levels of privacy protection legislation, there have been concerns about violations (such as the dispute over the US Privacy Shield). Not having any baseline safeguards seems unadvisable in this context. Third, the idea of a Central Government list of notified countries leaves decisions about the cross-border flows of personal data to the international realpolitik of trade and economic cooperation, undermining a principled evaluation of what such transfers would imply for the right to privacy and individual and collective data sovereignty.

Recommendation:

The framework on cross-border flows of personal data must be determined in a manner that protects the right to individual and group privacy; the economic right of communities to the social commons of non-

personal data (specifically, anonymized personal data in the context of this Bill); and the right to autonomous data-supported development of India through a flourishing local digital economic sector.

11. Special Provisions: Exemptions

The exemptions to the data protection framework are expansive, with state and all state instrumentalities, as well as certain data fiduciaries, as notified by the Central Government, allowed to seek exemption from the purview of the law. Such exemptions hollow out the purport of the law and create a stratified regulatory system. The Bill exempts state instrumentalities from the storage limitation clause of removing personal data retained after the purpose of retaining it has concluded. As such, these decisions should be taken based on a stringent retention policy, not dependent on which institution holds the data, but for what purpose the data is being retained.

Recommendation:

The power to exempt data fiduciaries from the purview of the law should vest with the regulator, instead of the Central Government. Whether such exemption is needed for data fiduciaries at all also needs to be considered, since creating broad exemptions dilutes the purpose for which the law is passed.

12. Compliance Framework (Chapter as a Whole)

The strength of any regulatory framework lies in the independence of its regulatory authority. Independent regulatory authorities are generally created under the power of legislation and are expected to have some distance from the executive. However, the Data Protection Board of India in the Bill (Board) has only been created in name under Section 19. All its powers, composition, and management have been left to rule-making by the Central Government, which defeats the purpose of the Bill. This is also a departure from earlier versions that provided details on the Data Protection Authority's (DPA) powers and responsibilities. Simplification of the language of the law cannot come at the expense of removing whole sections that define the powers of the regulator that will seek to address the concerns of the data economy. The Organisation for Economic Co-operation and Development (OECD), in its 2016 report on making regulators independent, notes that lack of clarity on roles and functions can lead to undue

government interventions. It cannot be the goal of the government to create a weak data governance regime.

The role of the Board in the Bill has been relegated to a post-facto quasi-adjudicatory body, with the mandate to determine non-compliance of this law and impose penalty and perform any other activity that the Central Government may assign. Previous versions of the bill clarified that powers of the DPA included a duty to protect the interests of data principals, prevent misuse of personal data, ensure compliance of the law, and promote awareness about data protection, which enabled the DPA to be a full-fledged regulator. As per this Bill, the Board is only to direct data fiduciaries to adopt urgent measures to address personal data breaches and mitigate harm to data principals.

Recommendation:

The Board's role in protecting privacy and principles of data protection in the data economy has to be more proactive and preemptive. It is hence necessary to incorporate additional provisions for the duty of the regulator to uphold rights of data principals and prevent misuse of personal data. Details on who appoints the members and chairperson to the Board, their tenure, how many members to the Board, etc. should be incorporated in the law, and not left to delegated legislation.

13. Miscellaneous: Amendments

The Bill provides wholesale powers to the Central Government to frame rules within the ambit of the law. While it is common practice to keep some space for delegated legislation, the Bill is over-reliant on such executive-led rule-making that can compromise effective enforcement and independence of the regulatory mechanism.

I. Section 43A of the IT Act, 2000 defines the standards of reasonable security practices and procedures that body corporates have to adopt in handling Sensitive Personal Data, and institutes compensation to affected parties in case of breaches. By repealing this Section, the Bill has created a lacuna. While Section 9(4) of the Bill obligates data fiduciaries and data processors to adopt reasonable security safeguards to prevent personal data breach or face penalties, it neither defines 'reasonable security safeguards' nor provides for compensation to the affected parties.

Recommendation:

The Bill should obligate data fiduciaries and processors to compensate parties affected by data breaches and introduce a definition of reasonable security safeguards in all forms of personal data processing.

II. The Bill also amends the Right to Information Act to create a blanket exemption on the provision of personal information under Section 8(j). While ostensibly intended to protect personal data, the prohibition of publication of personal information that is in public interest runs counter to the ethos of transparency and accountability in the RTI. Also, the R Rajagopal judgement of the Supreme Court has declared that on matters of public records, no claim for privacy would sustain unless it was violative of 'decency or morality'.

Section 8(j) of the RTI also notes that information that cannot be denied to the legislature cannot be denied to a person. This is also proposed to be deleted.

Recommendation:

The Bill needs revisions to ensure that large parts of the regulatory framework for personal data protection are not left undefined, and the discretionary power of Central Government is delimited. The RTI Act amendment should be deleted.