Technology Law Analysis

December 17, 2021

PROPOSED INDIAN PRIVACY LAW REVAMPED: LIGHT AT THE END OF THE TUNNEL?

I. BACKGROUND

A comprehensive data privacy law for India has been in the works for over five years since the Supreme Court's recommendation in 2017.[1] Two draft versions of proposed law (2018 and 2019) were previously released for public consultation, after which the Personal Data Protection Bill, 2019 (**PDP Bill**) was referred to a Joint Parliamentary Committee (**Parliamentary Committee**).[2] Initially expected to be presented in early 2020, the Parliamentary Committee presented its report on the PDP Bill in the Parliament on December 16, 2021 (**Report**). While the Report has been adopted by the members of the Parliamentary Committee, eight members have submitted dissent notes on certain aspects of law.

The Report recommends several amendments to the PDP Bill, including a change in title i.e., renaming the draft law to *Data Protection Bill, 2021* (**DPB**), since the law now proposes to regulate the collection and processing of both personal data and non-personal data **(NPD)**. At this stage, the DPB is merely a draft law, and is yet to be tabled as a Bill for the consideration of the Parliament. Notably, the recommendations of the Parliamentary Committee are not binding upon the Government. The DPB may be tabled in Parliament in its current form, or undergo change. Nonetheless, the legislative process is likely to entail the following steps prior to law enactment:

- The DPB could be accepted as it is, or amended further by the Ministry of Electronics and Information Technology (**MeitY**)
- The MeitY is then expected to seek Cabinet approval prior to the introduction of the revised DPB on the floor of the Parliament
- The draft DPB, as will be introduced in the Parliament, will be debated and passed by both Houses of the Parliament
- The version of the DPB passed by both Houses of the Parliament (including further amendments suggested by the Parliament, if any) would then require Presidential assent.
- Subsequent to obtaining Presidential assent, enactment of the law entails its publication in the Official Gazette.

II. KEY TAKEAWAYS FROM THE REPORT AND RECOMMENDATIONS OF THE PARLIAMENTARY COMMITTEE

Over the course of 2020-21, the Parliamentary Committee consulted various stakeholders and obtained oral evidence from 26 stakeholders in addition to written submissions from over 200 stakeholders. The stakeholders consulted, range from Government agencies, regulatory bodies and professional bodies to companies, law firms, academics and data security experts.

While these inputs have been summarized at various places throughout the Report, the Parliamentary Committee has by and large side-stepped a majority of the recommendations from stakeholders, without providing specific reasons for doing so. Certain key recommendations that were not taken into consideration by the Parliamentary Committee include suggestions to: remove/dilute data localization requirements, bring in further clarity over the scheme of data classification and the definitions of personal data, sensitive personal data (**SPD**) and critical personal data (**CPD**), reduce the age beyond which children are allowed to validly consent to the processing of their personal data from 18 to 13/14/16 years, and dilute of the exemptions extended to processing of personal data by Government agencies, to name a few.[3]

A summary of the key recommendations made by the Parliamentary Committee are as follows

1. The Parliamentary Committee found that limiting the scope of the law only to personal data would be "*detrimental to privacy*", and therefore recommended the inclusion of NPD within the scope of the law, and retained enabling provisions for the Central Government to prescribe policy frameworks on the usage and sharing of NPD.

   The Committee of Experts on Non-Personal Data Governance (**NPD Committee**) convened by the MeitY for recommending appropriate policy and regulatory frameworks for the usage and sharing of NPD, has reportedly submitted its recommendations to the MeitY.[4] While the final recommendations of the NPD Committee are not publicly available, the recommendations in the NPD Committee's interim reports could foreshadow future policies of the Central Government with regard to processing and sharing NPD.

2. The Parliamentary Committee recommends extending the regulatory mandate of the Data Protection Authority

Research Papers

Littler International Guide (India) 2024
November 08, 2024

Unmasking Deepfakes
October 25, 2024

Are we ready for Designer Babies
October 24, 2024

Research Articles

The Bitcoin Effect
November 14, 2024

Acquirers Beware: Indian Merger Control Regime Revamped!
September 15, 2024

Navigating the Boom: Rise of M&A in Healthcare
August 23, 2024

Audio

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I
August 26, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part II
August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FII8 event in Riyadh
October 31, 2024

Analysing SEBI's Consultation Paper on Simplification of registration for FPIs
September 26, 2024

(**DPA**) to include both personal data and NPD. It is not clear how the same regulator can act as protector of personal data and as framer of policy for use of NPD for public benefit. Clearly, the outlook required for these roles is completely different.

3. Interestingly, while the DPB does not impose any obligations upon data fiduciaries to report NPD breaches, it requires the DPA to address NPD breaches along the lines prescribed by the Central Government through the issuance of rules. The DPB adopts a more rigid approach to obligations triggered on account of data breaches and expands the DPA's mandate to include tracking of personal and NPD breaches and recommending measures to mitigate the impact of data breaches. Data fiduciaries are required to mandatorily report data breaches within 72 hours of gaining knowledge of the occurrence of a personal data breach. The function of evaluating the impact of such breach on data principals, has been vested in the DPA. Interestingly, there is no express obligation to report NPD breach under the Report.

4. The Report recommends the regulation of hardware manufacturers and urges the Central Government to establish a certification process for all digital and IoT devices, including emerging technologies that have the potential to train AI systems. The Report also recommends the establishment of a dedicated lab/testing facility for this purpose. The corresponding edit to the DPB, imposes the responsibility of testing and certification of hardware and software through appropriate agencies, upon the DPA.

5. The Parliamentary Committee's recommendations continue to place emphasis upon the localization of certain categories of personal data. Importantly, the Parliamentary Committee Report recommends localization requirements to be adhered to on a retrospective basis, by adding that *"concrete steps must be taken by the Central Government to ensure that a mirror copy of the sensitive and critical personal data which is already in possession of the foreign entities be mandatorily brought to India in a time bound manner".* As a justification for its recommendations, the Report primarily relies on the notion of "data sovereignty" and states that the Government is "*duty bound to safeguard the privacy of its citizens",* and that India "*may no more leave its data to be governed by any other country."* The Report specifically urges the Central Government to prepare and pronounce an extensive policy on data localization, in consultation with sectoral regulators.

Certain observations and recommendations contained in the Report seem to be recommendations implemented through other laws or amendments to existing laws. For instance, at one point the Report recommends mandatory local incorporation requirements as a pre-condition to permitting a social media platform to operate in India, and calls for the establishment of a statutory media regulatory authority along the lines of the Press Council of India for the regulation of content on social media. Similarly, the Report recommends amendments to the Patents Act, 1970 with a view to promoting data-driven innovation. These recommendations are beyond the purview of the Parliamentary Committee constituted for the limited purpose of formulating a data privacy law.

III. OVERVIEW OF KEY ISSUES WITH DPB

1. The DPB continues to maintain a widely worded exemption provision, enabling the Central Government to exempt any agency of the Government from any or all provisions of the law. The retention of this provision has been objected to in separate dissent notes provided by 8 members of the Parliamentary Committee. The grounds for triggering the exemption are relatable to the reasonable restrictions on the freedom of speech and expression, as listed under Article 19(2) of the Indian Constitution. However, the possibility of an absolute exemption from all obligations of the DPB, may not fulfill the constitutional requirement for narrowly tailoring restrictions. While the revised provision clarifies that the exemption so granted would be subject to just, fair, reasonable and proportionate procedures, it is unclear whether this alone would remedy the widely worded scope of the exemption.

2. The DPB retains the broad mechanics of cross-border data transfers as contained under the PDP Bill. However, the DPA is now required to consult with the Central Government prior to approving intra-group schemes or contracts for cross-border transfers of SPD. Likewise, the transfer of SPD to a foreign government is prohibited without the approval of the Central Government.

3. As was the case with the PDP Bill, the transitional provisions included in the 2018 draft of the PDP Bill as recommended by the Justice B. N. Srikrishna Committee continue to be omitted in the DPB. While the Parliamentary Committee has recommended (Recommendation No. 3 in the Report) that the "phased implementation" referred to in the Preliminary chapter of the DPB should be carried out over a period of 24 months, no specific provision has been included under the DPB to reflect this recommendation apart from an enabling provision.

4. The provisions of the DPB relating to data classification, remain unchanged in comparison to the PDP Bill. Given the differential obligations applicable to the processing and transfer of personal data and "sensitive personal data" respectively, it would have been desirable to exclude or partially carve out certain types of data from the scope of what constitutes "sensitive personal data".

5. Lastly, the DPB explicit consent remains the only permissible ground for the processing and sharing of "sensitive personal data". Obtaining explicit consent can prove to be impracticable or inappropriate in certain situations, such as in the case of processing SPD of employees, capture of biometric data such as video feed from security cameras – or in situations where such data is processed for fraud-detection, or for the purposes of complying with regulatory reporting requirements or court orders.

The remainder of this update is a summary of the key provisions of the proposed DPB on businesses. A detailed analysis of the proposed law (as envisioned by the Parliamentary Committee in its Report) is also included as a link towards the end of the draft.

IV. DECODING THE IMPACT OF THE PROPOSED DPB FOR THE INDUSTRY

1. *Major overhaul of current data protection law*

The erstwhile data protection regime under the *Information Technology Act, 2000*, was limited in scope to electronic information, largely concentrating on SPD and information. It was a notice-and-consent-based regime, with minimal compliances. The DPB is far more complex and far-reaching than the current law.

Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996
September 22, 2024

in India:	
2. *Extra-territorial application*:	It applies to entities outside India if they have a business connection to India or carry on profiling of individuals in India. While the intent behind the incorporation of the terms ``business connection", "systematic activity" and "profiling" have not been discussed in the Report, further guidance on the interpretation of these terms could be derived from supplementary sources such as taxation laws, and prior reports on the subject, including the Report of the Justice B. N. Srikrishna Committee on data protection.
3. *New data regulator (the Data Protection Authority, the "**DPA**"), adjudicating officers, and appellate tribunal*:	The DPA will be the first cross-sector data protection regulator in India (governing both personal and NPD) vested with significant regulation-making powers. The DPA is however required to consult with other sectoral regulators, and the Central Government, for the discharge of certain functions. The DPA will contain an independent adjudicatory wing, consisting of adjudicating officers tasked with adjudicating contraventions of the law, determining penalties, and other matters such as determining the enforceability of a "right to be forgotten" request. Appeals against orders of the DPA will lie before the Appellate Tribunal established under the DPB.
4. *Subordinate legislation*:	The DPB delegates a host of important matters, including the specification of types of data, classes of regulated entities, and codes of practice to the Central Government and the DPA. A true compliance picture will form only when these rules and regulations are framed.
5. *Wider categories of data protected*:	The proposed DPB will apply to all 'personal data',[5] SPD,'[6] CPD,[7] as well as NPD,[8] including anonymised personal data[9]. Higher benchmarks of compliance are prescribed for SPD and CPD (which are subsets of 'personal data').
6. *Data localization for sensitive data*	A copy of all SPD must be stored in India but may be transferred outside India subject to obtaining explicit consent of the data principal, and compliance with the terms of DPA-approved contracts or intra-group schemes. CPD (which will be defined by the Central Government through Rules) must be processed only in India, with the exception of transfers required for prompt action in terms of delivering health or emergency services, and transfers permitted by the Central Government in accordance with the DPB. Organizations processing SPD should prepare their infrastructure for data localization.
7. *Cross-border transfer restrictions*:	Personal data (that does not qualify as SPD or CPD) has been exempted from cross-border transfer restrictions. SPD may be transferred outside India if there is: (a) Explicit consent of the individual, and (b) Either: i. A regulator-approved contract or intra-group scheme for the transfer; or ii. A regulator-approved transferee entity or country. Data notified as CPD may be transferred outside India with the permission of the Central Government, on certain narrow grounds. These include transfers required for prompt action in relation to the provision of health and emergency services, and transfers to countries or international organisations, specifically greenlit by the Central Government, in line with strategic interests of the State.
8. *Privacy principles*:	The principles underlying the DPB are largely in line with global regulation, and include consent (with exceptions), purpose limitation, storage limitation and data minimization.
9. *Rights-based law*:	The rights conferred on individuals include: ▪ the right to data portability; ▪ the right to be forgotten; and ▪ the rights to access, correction, and erasure. Data fiduciaries (those that determine the purpose and means for processing) will need to implement processes to honor these rights when exercised by individuals.
10. *Consent managers*:	A new concept of registered 'consent managers' who liaise between individuals and data fiduciaries, including for the exercise of the above rights, has been introduced. The idea of 'consent managers' is innovative but relatively untested in practice. Similar frameworks have been explored by the RBI in the financial sector through the "Account Aggregator" model, which enables consumers to manage consent across a variety of financial accounts and products. The underlying intention appears to be mitigation of 'consent fatigue' and providing greater awareness to the uninitiated. These entities will be a new class of players in the data ecosystem. It will be interesting to keep an eye on the implementation of the consent manager framework.
11. *Three types of regulated*	In increasing order of compliance obligations, these are:

entities:	(a) Data processor (akin to the eponymous GDPR concept); (b) Data fiduciary (akin to the GDPR 'data controller'); and (c) Significant data fiduciary (a subset of data fiduciary). Significant data fiduciaries (**SDFs**) are treated as full-fledged regulated entities and are required to implement independent data audits, appoint a data protection officer, and carry out data protection impact assessments prior to carrying out any processing with a risk of significant harm, among other obligations. SDFs include 'social media platforms' with over a certain number of users and whose actions are likely to have a significant impact on the sovereignty and integrity of India, electoral democracy, and security of the State. Data fiduciaries processing children's personal data, or involved in the provision of services to children, have also been included within the scope of SDF.
12. *Personal data breach notifications*	Personal data breaches (including breaches of SPD and CPD) must be reported to the DPA, who may upon evaluation of the impact of the breach, require that the breach be reported to affected individuals and that remedial action be taken.
13. *Special provisions concerning children's data*:	The DPB mandates age verification, and parental consent. No exemptions have been provided for the requirement of obtaining parental consent. The DPB prohibits the profiling, tracking, or behavioral monitoring or targeted advertising directed at children and undertaking any other processing of personal data that can cause significant harm to the child.
14. *Innovation sandbox for artificial intelligence and emerging technology*:	The innovation sandbox instituted by data fiduciaries and start-ups is supervised by the regulator, and eligible data fiduciaries can avail of relaxations from certain obligations of the DPB up to a maximum period of 3 years.
15. *Government requests for anonymized and NPD*:	The Central Government has been given the power to direct that anonymized / NPD be shared by any entity with the Central Government, in certain circumstances. The Central Government has also been given the policy space to frame a policy on the regulation of NPD including anonymized data.
16. *GDPR-like penalties*:	The DPB provides for civil compensation; financial penalties such as fines (up to 4% of global turnover); and criminal penalties in the limited case of unauthorized de-identification of data.
17. Phased Implementation	The DPB provides that it will come into force on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may be appointed for different provisions of the law.

*Our detailed analysis of the DPB is available **here**.*

– NDA Privacy and Data Protection Practice

You can direct your queries or comments to the authors

[1] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

[2] See our analysis of the draft at, https://www.nishithdesai.com/SectionCategory/33/Research-and-Articles/12/60/ResearchatNDA/4455/14.html.

[3] See our take on the earlier draft at, http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Privacy-and-Data-India_s-Turn-to-Bat-on-the-World-Stage.pdf.

[4] See, https://www.medianama.com/2021/11/223-npd-authority-separate-recommends-expert-panel/

[5] Personal data is defined in the DPB as "*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, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling*".

[6] Sensitive personal data is defined in the DPB as "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; (iv) 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.
Explanation.- For the purposes of this clause, the expressions,- (a) "intersex status" means the condition of a data principal who is- (i) a combination of female or male; (ii) neither wholly female nor wholly male; or (iii) neither female nor male; (b) "transgender status" means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure".

[7] Critical personal data is explained in the DPB as any personal data that is notified by the Government as critical personal data.

[8] Non-personal data is defined in the DPB as "*data other than personal data*".

[9] Anonymised data is defined in the DPB as "data which has undergone the process of anonymisation" and anonymisation, in relation to personal data, is defined as "such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the [Data Protection] Authority".

based on the specific facts and circumstances. This Hotline does not substitute the need to refer to the original pronouncements.

list.