

POLICY BRIEF TO THE JPC: DATA STEWARDSHIP IN THE CONTEXT OF THE PDPB

AAPTI INSTITUTE, JANUARY 2020

Data Sharing and Governance under the Personal Data Protection Bill, 2019

While the PDPB chiefly deals with regulation of personal data, it nonetheless makes a limited mention of Non Personal Data in the context of mandatory data sharing and anonymised data.¹ Data stewardship takes a more important role in the context of Non Personal Data, as there no longer exists the same kind of privacy concerns in connection with this kind of data, and as well because of the higher financial value attached to larger datasets that take the nature of Non Personal Data.

The PDPB defines non-personal data as “all data that is not personal data”.² This catch-all negative definition of non-personal data is extremely wide in ambit and covers a lot of information that may be proprietary information of companies and other stakeholders. While a broad definition may not be a problem in and of itself, the Bill also allows state agencies to direct any data fiduciary to provide such state agencies with anonymised personal data, or “other non-personal data”.³ This provision gives the state agencies unrestricted power to requisition any piece of non-personal data without guidelines, checks, or limitations.

We recommend that the language of the Bill be altered to reflect standards and guidelines that allow for a specific set of conditions that must be satisfied to allow state agencies to direct data fiduciaries to provide anonymised under Section 91. Our specific language on this recommendation is provided below on page 2.

These restrictions allow for a controlled manner of sharing non-personal data and prevent abuse of powers under the provision. Further, ensuring that request for mandatory data sharing is only made under the specified circumstances is an important function – one that may further be helped by the presence of an intermediating body such as the data

¹ Section 91(2), The Personal Data Protection Bill, 2019.

² Explanation to Section 91, The Personal Data Protection Bill, 2019.

³ Section 91(2), The Personal Data Protection Bill, 2019.

steward.

Managing data sharing is one of the principal functions of data stewards, and already plays an important role in this regard across the globe. For instance, the X-Road system of data sharing by citizens across services is used in Estonia and replicated in a number of developed nations, such as Japan, Iceland, and Finland.

A form of such principles is also currently being attempted to be put in practice through the Reserve Bank of India's guidelines on Account Aggregators. While the system does not go into data management itself, it nonetheless prescribes a consent management engine⁴ that empowers users to give and revoke consent to third parties to access their data that is stored amongst various data fiduciaries whose services they employ.

In light of these drawbacks in the proposed legislation, we recommend that the Committee strongly consider the adoption of a framework to effectively regulate data, which can balance the multiple interests of security, commerce, and user rights. It is in this regard that our proposal seeks to provide an alternative: we believe that the idea of data stewardship provides a basic framework to create a conducive regulatory regime for companies and users in India to work with Non Personal Data.

Proposed Language on Section 91:

- We propose an amendment to Clause (2) of Section 91 and the addition of two further Clauses as follows:

Section 91. Act to promote framing of policies for digital economy, etc.

(2) The Central Government may, in consultation with the Authority, direct any data fiduciary to provide non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed.

(3) The Authority shall not direct the fiduciary as under (2) in case of the possibility of significant harm being caused to either the fiduciary or the data principals to whom the data relates.

(4) The directions issued under (2) may be responded to by the fiduciary making representations on the likelihood of significant harm being caused to the fiduciary

⁴ Section 6, Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016.

or the data principals to whom the data relates.

- We recommend that the sharing of Non Personal Data be addressed outside the PDPB, namely, by the committee of non-personal data constituted by the Ministry of Electronics and Information Technology (MEITY) specifically to evolve comprehensive policies and guidelines laying out the principles and frameworks for the regulation of non-personal data.

Data Stewardship and its relevance to the Personal Data Protection Bill, 2019

Simply put, data stewardship is a system of managing data storage and sharing where an intermediary facilitates policies for and carries out consent-related decisions and functions for the benefit of users. This function has not been specifically called out in the Personal Data Protection Bill (the “PDPB”), however is still relevant in the larger context of data governance.

Policies on specific issues in data sharing and management – such as the security requirements around certain sensitive kinds of data, the sharing restrictions on such data, the terms on which consent operates in terms of granularity and duration – will define the patterns of value sharing and accruing of benefits to various stakeholders in the data ecosystem. This is evinced by the contents of the 2018 SriKrishna Report on Data Protection (the “Report”).

Significantly, both the PDPB and the Report adopt the framework of data fiduciaries and a consent-centric regulatory approach.⁵ As another point of interest, the report attempts to discuss community data as being a “natural resource”, and defines it as “a body of data sourced from multiple individuals, over which a juristic entity may exercise rights”.⁶

The new draft of the PDPB goes a step further and establishes a class of data fiduciaries known as ‘consent managers’.⁷ These are fiduciaries that enable users (“Data Principals” under the PDPB⁸) to manage consent that they have granted to various data fiduciaries. Consent managers here perform the role of handling responsibilities in relation to permissions granted and the associated access to data. In our work, we have discussed such a role in a much broader form – that of the data steward.

Under our analysis, the current framing of consent managers forms one subset of the possible approaches to data stewardship, but eschews aspects of stewarding data other than collection of consent and permissions. Enabling data sharing amongst a wider set of stakeholders is crucial to utilizing the dormant value of data that is soiled and restricted to

⁵ Section 3(11), and Sections 4-11, The Personal Data Protection Bill, 2019.

⁶ “A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians”, Committee of Experts under the Chairmanship of Justice B.N. SriKrishna, p. 45.

⁷ Section 23(3), The Personal Data Protection Bill, 2019.

⁸ Section 3(14), The Personal Data Protection Bill, 2019.

sharing solely on the terms of the initial point of collection – points which have resulted in existing oligopolies of aggregated datasets.

Consider for example, the case of ecommerce platforms, which has been explained at length by Lina Khan, a thinker on technology regulation and the power of companies over mediums of communication. She illustrates how the competitive advantage that a company gains through online market puts it at a different starting point in different markets, and when combined with the size of an industry incumbent, it leads to high barriers to entry for any new player, and leads to an abuse of dominant position by existing oligopolies.⁹

The reason for the relevance of data stewardship is that the current framework of data sharing and usage does not lend itself to efficient usage of data and the value flowing from it. Users need a path towards maximizing agency in order to be able to realize the rights granted to them under the PDPB.

The presence of a data steward, an entity that can represent their interests, is a regulatory structure that creates space for the empowerment of users. This forms our central premise underpinning the proposal. Such entities can serve as a balancing force between the competing interests of the user and the data fiduciary. The lack of control that users face in relation to their data can be addressed by these entities that are bound to prioritise the interests of the users when framing policies for sharing and use of data. The value created by aggregated data can therefore be routed back towards utilities that serve the interests of the users who served as the initial creators of the data.¹⁰

The Data Steward also presents a structure where the rights of users are protected in situations where the fiduciary is unable to comply with the requirements of the PDPB. Section 19 of the PDPB for instance, while requiring fiduciaries to ensure the right to Data Portability, does not specify any framework for making such a feature operational. Further, the Bill provides an exception to the right where such data portability is not “technically feasible”, in effect emptying the right of any real impact and leaving the user with no recourse to enforce the right. Data stewardship, in this context, provides a

⁹ “Sources of Tech Platform Power”, Lina Khan, Georgetown Law Technology Review, 2018.

¹⁰ “Bottom-up data Trusts: disturbing the ‘one size fits all’ approach to Data Governance”, Sylvie Delacroix & Neil Lawrence, International Data Privacy Law, 2019.

framework where it can work with fiduciaries to provide services that enable users to control the access to their data in situations where users are unable to directly access their information from the fiduciary.

There exist a number of functions that a data steward may perform:

Collaborate to benefit fiduciaries: The PDPB contains functions such as notice requirements which may require parties to take actions to notify users based on interactions with third parties.¹¹ Such interactions can benefit from the existence of entities that carry out obligations and act as a check on the compliance of notice requirements in order to assist data fiduciaries in regulatory issues. These entities also actively bring stakeholders to share data in a safe, secure manner, to foster innovation while ensuring that individual consent and preference is taken into account.

Management of data policies and execution: The PDPB requires data fiduciaries to restrict data collection and usage based on certain principles, including storage limitation,¹² purpose limitation,¹³ and privacy by design¹⁴. These in turn involves practices such as data minimization, which involves minimal collection of data, only those data points that are required for the overall purpose of data collection. Data fiduciaries are in need of guidance in this regard, right from policies on data storage and streamlining sharing permissions to questions on how to maximize privacy in the data flow inherent in their design of their products and services. Data stewards can help develop policies for secure management of data, and enforce them on behalf of users.

Accountability of fiduciaries: The primary function of the data steward is to protect and negotiate on behalf of users from whom the data is primarily extracted, and in order to act in their interest the steward will carry out functions of accountability such as auditing functions and ensure disclosures on data usage and sharing. When working with data fiduciaries that hold large stores of data, these functions can benefit a large proportion of users when carried out efficiently and on a regular basis. Requirements from the PDPB

¹¹ Section 7, The Personal Data Protection Bill, 2019.

¹² Section 9, The Personal Data Protection Bill, 2019.

¹³ Section 5, The Personal Data Protection Bill, 2019.

¹⁴ Section 22, The Personal Data Protection Bill, 2019.

such as restrictions on cross-border data transfer¹⁵ may also require expertise to enforce the policy.

Intermediate between stakeholders: Data stewards can act as a go-between for users and data fiduciaries, and work with fiduciaries of various sizes and relevance to address user concerns on data security and data sharing. The PDPB also allows for users to revoke permission from data fiduciaries to store or process their data,¹⁶ and compliance in this regard can be facilitated and ensured by an intermediating body such as the data steward. Data stewards can also act as a platform for users to effect judicial orders in cases where there is a successful civil claim against a data fiduciary in their favour.

An exclusion from the function of the data steward is enforcement of criminal penalties. This is to ensure that the data steward does not encroach on the state functions of regulating entities and enforcing the letter of the law.

Data stewards are likely to be attractive to data fiduciaries, who can rely on the intermediary to negotiate data use, ensure quality and standards, and more importantly unlock data that is currently underused and underutilized.

¹⁵ Sections 33, 34(2), The Personal Data Protection Bill, 2019.

¹⁶ Section 11(2)(e), The Personal Data Protection Bill, 2019.

Key Takeaways

- Management of more tailored and specific policies on data will define the patterns of value sharing and accruing of benefits to various stakeholders across the data ecosystem. As discussed in the SriKrishna Report, it is important to **equitably distribute the generation of value from large-scale data accumulation**.
- The primary function of the data steward is to benefit users. The establishment of a regulatory structure to support a Data Steward, **an entity that can represent the interests of users and other stakeholders**, will help utilise the dormant value of big data. Data stewards can **work with fiduciaries to address user concerns on security and sharing data**.
- The PDPB contains requirements from data fiduciaries on store and processing data, notice requirements, and **compliance in this regard can be facilitated by a non-aligned entity such as the data steward**. The steward may carry out such obligations in order to assist data fiduciaries with regulatory requirements and act as a check for compliance.
- Managing data sharing is one of the principal functions of data stewards. We **recommend that the principles of data stewardship be strongly considered with regard to sharing of Non-Personal Data** to provide a basic framework for a comprehensive regulatory regime beneficial to companies and users. We recommend that **Consent Managers be broadened to include a wider framework**, and that Non-Personal Data be handled by its own dedicated policy document.
- We recommend that a specific set of conditions be specified where state agencies are permitted to direct data fiduciaries to provide anonymised or non-personal data.