India's data protection bill:

Further work needed in order to ensure true privacy for the next billion users

February 24, 2019

India, the largest democracy in the world and second-largest internet user base, has been trying to enact a national data protection law for quite some time now. The latest development is the Personal Data Protection Bill, 2019 (PDP Bill) which has been approved by the Union Cabinet and was placed in the Lok Sabha (lower house of the Indian Parliament). During the deliberations in the Lok Sabha, it was decided that the Bill would be sent for review to a Joint Parliamentary Committee - consisting of members from the Lok Sabha (Lower House) and Rajya Sabha (Upper House). The Joint Parliamentary Committee is currently holding consultations and deliberations on the merits of the bill.

The process of drafting a data protection law started through an assurance provided by the Government of India in the case of Justice Puttaswamy vs the Union of India, to set up an expert committee, chaired by Justice Srikrishna in July 2017. This committee over the next year, published a draft report, along with a final report and bill in July 2018. Access Now published an analysis of this bill - *Assessing India's Proposed Data Protection Framework*. This analysis was a result of an exercise of evaluating the final bill presented by the Srikrishna committee, against the principles noted in the *Do's and Don'ts Guide for Lawmakers* - which draws on the experiences from the European Union's General Data Protection Regulations' (GDPR) negotiation process.

Below we provide our analysis of the PDP Bill, drawing from the changes made to the bill submitted by the Justice Srikrishna Committee, along with the principles outlined under our Data Protection Do's and Dont's Guide for Lawmakers.

1. **Strengthen Data Protection Principles and Rights under Chapter II of the PDP Bill**

   [RECOMMENDATION: Amend Clauses 5, 17, 19(2)]

Under Clause 5 of the PDP Bill, it has been provided that personal data shall only be processed "*for the purpose consented to by the data principal*". This provides a purpose limitation to the processing of data. However, this principle is diluted by the presence of

language - "*which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected*". These allowances dilute the principle of purpose limitation and are ambiguous in nature.

The PDP Bill does provide some user rights, including the rights to confirmation and access, the right to correction and erasure, and the right to data portability. The right to erasure has been added from the previous iteration of the PDP Bill, and is a welcome step.

The right to information is diluted under the last version of the PDP Bill; it is limited to a "brief summary" of the personal data being processed and the processing activities. Further, it does not entitle users with the right to an explanation as provided to the users under the EU's GDPR and also the UK Data Protection Act, 2018. The right to explanation is crucial for accountability and transparency in the use of algorithms to make decisions in our lives.

The right to data portability is an important right provided to the data principal under the PDP Bill. However, under Clause 19(2)(a), an exemption for the exercise of this right has been provided in relation to processing "*necessary for functions of the State*". This exception provides very broad language and may effectively ensure that the State, as a data fiduciary, is not required to provide the right to data portability to data principals.

2. **Limit exemptions for processing of personal data without the consent of the data principal provided under Chapter III of the PDP Bill**

   [RECOMMENDATION: Amend Clauses 12, 13, 14]

The PDP Bill provides concerning and broad limitations to the exercise of prior consent by the data principal for the processing of data. Under Clause 12, the state is authorised to process personal data for "the exercise of any function of the state" without the consent of the individual. The provision is vague and overbroad, and it gives the government an absolute power over citizens' data and rights. It is imperative that data protection principles apply to the state as well as to private actors. Further, the processing of personal data to comply with any law, order, or judgment of courts or tribunals, is allowed without the need for the consent of the data principal. These provisions are particularly harmful, given that the broad language allows legislatures and executive offices across the breadth of India's federal polity to undermine the comprehensive aim of a national data protection law by allowing state authorities citing general laws (including those that might have established them as a statutory body) to override data protection provisions. Further, in addition to the exemptions above, Clause 12(f) provides an exception wherein processing of personal data may be done without any consent of the users, in case of "breakdown of public order". Such broad, undefined language, especially in the background of deployment of mass facial recognition and other technologies, creates concern, and may lead to the mass surveillance of users. The aim of this legislation is to establish users' protection and it

should not be turned as a tool to justify the deployment of techniques and technologies that enable surveillance.

Clause 14 allows an exception where personal data may be processed without consent for "reasonable purposes". This phrase is vague and gives latitude for violating the data rights of citizens. The presence of an illustrative list of "reasonable purposes" is concerning as it seeks to include "credit scoring", "recovery of debt", etc., already indicating that "reasonable" commercial interests could trump rights-protecting data protection measures.

The PDP Bill also entitles employers with overbroad rights in relation to their employees, reinforcing an already imbalanced power relationship in favor of the employers. Clause 13 of the PDP Bill allows employers to process the personal data of their employees for purposes related to employment, including recruitment, termination, and assessment of the employee, without the need for consent. These rights are overbroad and unnecessary, and subjugate an employee's rights to those of the employer. An employment relationship does not lead to the cessation of fundamental rights of an employee. Such a provision is not present in the GDPR, UK Data Protection Act 2018, and other comparative legislation.

3. **Strengthen the provisions regarding reporting of data breaches by data fiduciaries**

   [RECOMMENDATION: Amend Clause 25]

Clause 25 of the PDP Bill provides for a legal requirement for data fiduciaries to inform the Data Protection Authority (Authority) of breaches of personal data. In case of data breaches, the data fiduciary has to notify the Authority regarding the breach, where such breach is likely to cause harm to any data principal. The notification sent to the Authority is supposed to include details on the nature of personal data, number of data principals affected, possible consequences, and measures being taken by the data fiduciary. Further, informing the data principal about the breach depends on the discretion of the Authority. Upon receipt of the notification, the Authority is authorised to determine whether such breach should be reported by the data fiduciary to the data principal or not. In addition, the Authority may direct the data fiduciary to take appropriate remedial action. The Authority may, under its discretion, post the details of the personal data breach on its own website. However, the entitlement of discretionary powers provided to the Authority could weaken the data breach prevention and notification mechanism — the users must have the right to always be notified so that they know when their information has been breached in order to take steps to remedy any possible harms.

Data fiduciaries may in fact often wish to quickly inform users of data breach incidents impacting them; the current text prevents them from doing so until the Authority has allowed them to do that, adding an unnecessary step - user reporting should instead by the default. Effective data breach reporting also serves a key national cybersecurity need, allowing those involved in cybersecurity roles to be made aware of intrusions triggering data breach and the

scale of such incidents. Additionally, in case such information is only disclosed to the Authority, the Authority must make public the criteria for its assessment of severity of the harm to the user of a data breach and such criteria must include a human rights impact assessment.

4. **Reduce risk of mass surveillance and other privacy harms by establishing limitations to power of central government to issue exemptions under Chapter VIII of the Bill**

   [RECOMMENDATION: Delete Clause 35; Amend Clause 36, 37]

In addition to the exemptions provided for the processing of data without the consent of the data principal, Clause 35 of the PDP Bill provides broad provisions under which the government can exempt its own departments from the very application of the law itself. These exemptions are too vague and dangerously broad. As noted by many experts, there is a need for the tightening and evolution of Indian statutory law overseeing the processing, including collection and use of data by government agencies - including those engaged in law enforcement matters and other areas of internal security and intelligence. The absence of comprehensive surveillance law reform provides the State with wide access powers over the information of citizens of India, and thus puts their informational privacy under threat.This contradicts the spirit and aim of the PDP Bill.

Government agencies - including those responsible for carrying out security, foreign relations, law enforcement, and other state functions - must be clearly identified, notified, and bound by the provisions of the Bill. An extraordinary carve-out power that can be used by the Central Government with no parliamentary oversight and accountability would undermine core pillars of the PDP Bill and the effective and rights-respecting functioning of the privacy legal framework in India as a whole.

Additionally, other clauses in this chapter confer other wide powers to the Central Government, undermining the role of the Authority as the independent regulator. We recommend amending Clauses 36 and 37 to better protect privacy of data principals, including requiring the Data Protection Authority to be in charge of deciding the exemption of certain data processors abroad, instead of the Central Government.

5. **Establish a strong and independent data protection authority, and appellate tribunal**

   [RECOMMENDATION: Amend Clauses 42, 43, 62, 63, 64, 66, 79, 86]

No comprehensive data protection framework can be effective without a dynamic and powerful enforcement mechanism. A powerful enforcement mechanism includes the creation of an independent data protection authority. Clause 41 of the PDP Bill seeks to establish and

incorporate a data protection authority for the purposes of the PDP Bill, which will be known as the Data Protection Authority of India.

As per the current text of the PDP Bill, the chairperson and the members of the Authority shall be decided by a committee of six members, consisting solely of members within the executive branch of the State. The criteria for membership provided under the PDP Bill is vague, and given that the appointments are made by the government, there is a possibility of a pro-government bias creeping into the Authority - at the same time as it is expected that cases involving government departments and agencies will form a large part of the Authority's docket of complaints and decisions. In India, the government may soon be the biggest processor of data. This proposed nomination process raises concerns regarding the independence of the Authority and requires considerable improvement; the government's modifications of the original text proposed by the Srikrishna Committee has actually weakened the independence of the Authority. The current text of Clause 42 proposes a selection committee that is completely controlled by the Central Government, with no independent members or other forms of checks and balances. Clause 43 allows the Central Government considerable control over the salaries and other terms of service of the Authority's chairperson and members, without even a guarantee that these will not be modified to their detriment during their tenure - which allows to use of this as a threat to intimidate the Authority and weaken its independence.

Additionally, it seems that of members of the Authority could be easily re-employed by the private sector or the government. It has been noted many times in India that limitations on revolving doors t help in creating an unbiased regulator, as observed in the original text of the Telecom Regulatory Authority of India Act, 1997.

There also continues to be significant issues with the defining the role of "adjudicatory officers", which the PDP Bill proposes would hear, inquire, and decide on all complaints and penalties under the law. While the current text makes the role of "inquiry officers" clearer (namely, that all questions about data and reporting by data fiduciaries will be handled by specific inquiry officers appointed by the Authority), the relationship between the "inquiry officers" and "adjudicatory officers" remains unclear.

More troubling is the current language about the appointment and control of those who act as adjudicating officers; this is left to the Central Government and not the Authority, essentially creating a situation where the Authority's effectiveness and independence is greatly curtailed. Additionally, the current language on penalties and the budgetary powers of the Authority requirements amendments. It currently does not allow the Authority to retain money from the penalties it levies, and instead makes it rely solely on Central Government budgetary allocations; this could impact the Authority's independence. That is further exacerbated by the wide powers given to the Central Government to issue directions to the Authority under Clause 86, leaving aside the additional general power includes there that the Authority will be bound by directions on questions of policy by the Central Government.

Further work is also needed on ensuring the independence of the proposed appellate tribunal, to which one would go in appeal on any of the directions, findings, or penalties of the Authority. We recommend amendments to Clauses 67, 68, and 70 in order to ensure the independent functioning of the appellate tribunal. Currently, the Central Government is left in charge of its establishment, control over the terms of service of its members, and near complete discretion over the staff that would work for the tribunal.

6. **Reduce exemptions in relation to "non-personal data"**

   [**RECOMMENDATION: Delete Clause 91]**

It is both peculiar and concerning to observe that while the PDP Bill envisages only personal data within its ambit, there are specific exemptions and provisions provided in relation to non-personal data. While "non-personal data" has not been defined comprehensively within the PDP Bill, the Central Government has been given the right to direct any data fiduciary to provide anonymised data or non-personal data for the purpose of policy making and targeting of delivery of services in Clause 91. These are broad exemptions provided in relation to this subset of data which has not been defined. It may lead to wide interpretation of powers by the government, resulting in the possibility of exposure and breach of personal data of users, limitation of rights and other privacy harms. The reference to government policies on the digital economy that do not impact personal data is out of place and confusing in a law that is meant to explicitly govern the collection and use of personal data.

7. **Revise provisions on the transfer of sensitive personal data and critical personal data outside India**

   [RECOMMENDATION: Amend Clauses 33, 34]

The PDP Bill troublingly seeks to establish a data localisation regime. Clause 33 of the PDP Bill allows for sensitive personal data to be transferred outside India by a data fiduciary provided the requirements of clause 34 are met, but makes it mandatory that such sensitive personal data be continued to be stored in India. The current wording of the clause makes it unclear as to how the data is to be stored while also being allowed to be transferred outside India.

While it is important to safeguard the rights of users and protect their sensitive personal data, the absence of developments in reforming the procedural checks and substantive oversight of data access and interception powers of government authorities in India put data, including sensitive data stored in India at risk as they could be access and misused by public authorities. The Justice Srikrishna Committee report noted that current powers likely fail to meet the standards of constitutionality in Indian law following the further elaboration and strengthening of privacy standards by the Supreme Court of India in its landmark 2017 judgment in

Puttaswamy v. *Union of India*. Given this context of the lack of sufficient curbs on access to such data by the government in India, this proposed data localisation provision betrays a governmental interest in desiring more control over the data of Indian citizens - not protecting privacy.

Similarly, Clauses 33(2) and 34(2) authorise the central government to mark categories of personal data as "critical personal data". The current text of the PDP Bill (which has changed from the Srikrishna Committee PDP Bill) proposes that such data cannot ordinarily be transferred out of India except in certain emergency cases or only if the Central Government has deemed such transfers to be not prejudice state security or strategic interests - without making any considerations for the data principle interests. No guidance has been provided regarding the criterion for classifying critical personal data, and such decisions have been left at the behest of the Central Government. Once again, such proposals go against the spirit and objective of comprehensive data protection and privacy legislation.

8. Delete troubling Right to be Forgotten provision

[RECOMMENDATION: Delete Clause 20]

A key lesson learnt from the experience of the GDPR and other data protection laws is to not develop a "right to be forgotten". The "right to be forgotten" or the "right to de-list" gives users the right to request that search engines de-list web addresses from results when a search is done using their name. This right is frequently confused with the "right to erasure", which allows the users to delete all personal data in case they have left the service or application. In the EU GDPR, the right to be forgotten was added to the right to erasure, codifying the jurisprudence of the EU Court of Justice in the "Google Spain" case. The right to erasure is one of the most important binding rights to ensure data protection and privacy of the user, and the 2019 version of the PDP Bill improves on the Srikrishna PDP Bill by including clear language on the right to erasure, as we have noted above. However, the current PDP Bill text does include a "right to be forgotten" provision in its current clause 20. The text of this proposed clause does contain the necessary safeguards which would limit the exercise of thisright on a motion to the Authority (and not served directly on the data fiduciary) as well as other requirements of protecting free expression and news reporting. This provision opens avenues for abuse and confusion, in particular since it is not made clear how it relates to the more established right to erasure included as part of clause 18. Additionally, there is the possibility of conflict with the established, landmark Right to Information Act. Clause 20's safeguards propose that a "right to be forgotten" request under the PDP Bill shall only be effectuated pursuant to an order by an adjudication officer, who must consider the rights and interests of the data principal in preventing or restricting the continued disclosure of personal data and ensure that they don't override the right to freedom of speech and expression and the right to information of any citizen. However, under the Indian legal framework, the right to information is a separate right established under a distinct institution. Interactions between the "right to be forgotten" and the

"right to information" must necessarily be decided upon by the authorities under the right to information framework - that is the Central Information Commission and state information commissions established under the RTI Act.

Given the risk created by this provision, we recommend that clause 20 proposing a "right to be forgotten" should be omitted from the PDP Bill.

9. **Maintainencouraging provisions for protecting Data Security and Data Integrity under Chapter VI of the PDP Bill**

   [RECOMMENDATION: Keep Clause 22, 24 and 27]

The PDP Bill takes steps to protect personal data by introducing the principle of "privacy by design" under Clause 22. Clause 22 of the PDP Bill entitles the data fiduciary with the responsibility to implement policies and measures for privacy by design. Privacy by design not only protects data; it also leads to data integrity. This is in line with the EU GDPR principle of data protection by design and default.

Further, Clause 24 of the PDP Bill holds the data fiduciary and the data processor responsible for implementation of appropriate security safeguards for the protection of the data of the user. Specifically, provisions encouraging the data fiduciary to use encryption along with the requirement for periodic reviews of such steps would help in creating an ecosystem of data security and integrity for the user.

Under Clause 27 of the PDP Bill, data fiduciaries have the responsibility of making data protection impact assessments from time to time, especially when new technologies are introduced, or they use sensitive data, or carry out large-scale profiling. This is a positive measure. Furthermore, steps related to establishing transparency in data processing (under 23 of the PDP Bill) holds the data fiduciary responsible to notify the data principal of important operations in personal data processing. The PDP Bill also makes it mandatory for data fiduciaries to appoint a Data Protection Officer in order to ensure transparency and accountability measures. This person is also responsible for providing assistance to, and cooperating with, the Authority, and to act as the point of contact for the data principal for the purpose of raising grievances to the data fiduciary.

These three provisions are interconnected and would positively impact the development of a sustainable data economy in India. We appreciate the drafting of the PDP and recommend maintaining this language.

10. Remove references to consent managers as an agent of the data principal

[RECOMMENDATION: Amend Clause 19, 21 and 23]

Under Clause 23 of the PDP Bill, a new stakeholder is introduced called the "consent manager". It appears that the role of a consent manager is to act as an agent of a data principal in being able to exercise their rights with respect to other data fiduciaries. There is a lack of clarity on the role, and regulation of consent managers. It is essential that some data fiduciaries are not privileged over other data fiduciaries, and opportunity is given to public interest organisations too also serve the interests of data principals. Such rules on the use of consent managers would be premature and could affect the development of future technologies.

We recommend that relevant clauses 19, 21, and 23 are amended to either drop consent managers from the current framework, or provide adequate regulatory oversight over such actors, while allowing public interest representatives acting on behalf of data principles space in the ecosystem.

11. Remove proposals for sand boxes for AI and other purposes under Clause 40

[RECOMMENDATION: Remove Clause 40]

India is currently at a nascent stage of development of data protection and privacy principles. Introduction of regulatory sandboxes open up a variety of concerns and avenues for abuse. We recommend that Clause 40 be currently removed, and inclusive consultations must start on this process. After such a process, a comprehensive regulatory proposal for sandboxes could be explored at a later date.

Internationally, it has been reiterated that there is an obligation upon states to protect human rights in the context of AI. The Toronto Declaration on human rights obligations in the context of machine learning includes the principle of "Holding private sector actors to account". It states that:

> "*States should put in place regulation compliant with human rights law for oversight of the use of machine learning by the private sector in contexts that present risk of discriminatory or other rights-harming outcomes, recognising technical standards may be complementary to regulation. In addition, non-discrimination, data protection, privacy and other areas of law at national and regional levels may expand upon and reinforce international human rights obligations applicable to machine learning.*"

12. Redefine special provisions for Biometric Data under Clause 92

[RECOMMENDATION: Amend Clause 92]

Under Clause 92, a special provision has been provided wherein biometric data shall not be processed, as notified by the Central Government of India. While it is encouraging to see that biometric data, given its special nature of irreversibility and intimacy to an individual is given additional oversight, we recommend that instead of the Central Government, the Authority (subject to doing so after due public consultation), be provided the power to notify any such exceptions. This is especially important given that the Central Government is one of the largest processors of biometric data in India.

Conclusion

This bill may prove to be a highly consequential legislation, not only for India but for the world. India is home to the next billion users of the internet, and is also home to many data fiduciaries which process data from across the world.

Amidst discussions of the pros and cons of the PDP Bill, users and experts in India are pushing for amendments before it is presented in the Parliament. Initiatives such as the #SaveOurPrivacy, an Indian advocacy movement, has provided constructive feedback through a model draft law called the Indian Privacy Code, 2018. The model law — drafted by a committee of volunteer lawyers from the digital rights community in India — covers the specific and nuanced issues of privacy, data protection, interception and security, and builds on seven privacy principles the drafting committee identified as the pillars of the legislative effort. Such efforts are notable towards enabling citizen centric and rights respecting legislation.

While the PDP Bill draws from various sources, most notably the recently enacted General Data Protection Regulation (GDPR) in the EU, our analysis shows there are multiple areas of concern for its efficacy in protecting the rights of the users in India. A rights respecting regime would empower the citizens to assert their rights, along with creating contours of agreeable actions by data fiduciaries. The recommendation we make in this analysis aim to assist in the creation of this regime.

For any queries, please reach out to Naman M. Aggarwal (naman@accessnow.org), and Raman Jit Singh Chima (raman@accessnow.org). This document has been prepared with the assistance of Estelle Massé (estelle@accessnow.org).