NUS National University of Singapore | ISAS Institute of South Asian Studies

ISAS Brief

No. 977 – 23 November 2022

Decoding India's 2022 Data Protection Bill

Karthik Nachiappan

Summary

The Indian government's latest Digital Personal Data Protection Bill, 2022, clarifies some qualms relating to data localisation while raising other concerns over consent and regulation.

The Indian government released a newly updated draft version of the data protection law – the Digital Personal Data Protection Bill, 2022, – on 18 November 2022. The latest iteration of the proposed law will be available for public consultation before ostensibly being finalised. What does this version stipulate? Has the push toward data localisation softened?

This draft bill is simple and concise and directly targets a few issues, compared to previous versions that were far more comprehensive and lengthier. This bill is a pithy pared down draft that applies to all firms and organisations that process all data collected online and offline in India. Specifically, this version has 30 clauses, compared to nearly 90 in the previous iteration. This culling of the bill suggests that Indian officials are keen to provide clarity on key issues. These include the role and responsibilities of data fiduciaries, penalties imposed for failure to adhere to the law, data flows (particularly localisation) and the regulator that would govern data. The bill has left other issues and details to be addressed as the law gets implemented and gaps and opportunities for further regulation arise.

This version lowers the information that data fiduciaries – collectors of data – are required to provide to those who give their personal data. The burdens on fiduciaries have been reduced to give them sufficient time and ability to comply. However, the draft bill mandates that companies do not perpetually store data collected; data storage should be limited to specific purposes. The fines imposed for failure to adhere to rules are stiff; penalties up to US$30 million (S$27.4 million) can be levied should a fiduciary fail to "provide reasonable security safeguards to prevent personal data breach" or should they "fail to disclose a personal data breach".

Data collection by fiduciaries is centred almost entirely on consent acquired through a notice but questions remain over whether users who give their consent have an adequate understanding of the kinds of data they provide and the purposes for which their data are used since these requirements have been removed from this draft. For instance, will the location data provided be used for the purposes identified or will they be deployed for related purposes as per the fiduciary? This bill makes all data collection, storage and processing contingent on consent without expanding on how data fiduciaries will undertake these latter functions.

This draft bill narrows the scope of data protection by eliminating aspects related to non-personal data, which was part of the earlier bill. Additionally, this version removes the

categorisation of sensitive and critical personal data present in earlier drafts and left them undefined. One potential concern of removing these two components is that all data is now effectively 'personal' data, which could be problematic since only certain kinds of data like biometric data, health, genetic and financial data require more protection. The data protection legislations of other countries have different categories of data given the dangers associated with certain kinds. The removal of these definitions and distinctions could affect and complicate how the government and others deem who was harmed by data breaches.

Importantly, this draft does away with data localisation or provisions that mandate data storage in India. This iteration allows for cross-border data flows with 'certain notified countries and territories' or trusted jurisdictions where the data of Indian citizens should be protected and secure. Data fiduciaries, big tech companies like Meta, Google and Amazon, can transfer the personal data they collect abroad for processing. This concession represents a triumph for big technology firms that were openly lobbying against data localisation since the first version of the Personal Data Protection Bill, 2019. It appears as though New Delhi heeded the wishes of Indian start-ups whose business models and applications and services could be enhanced by external partnership and collaboration, for which cross-border data flows would be essential. That said, the government now must identify the countries to where Indian data would flow seamlessly and the conditions or frameworks under which those flows would occur.

Finally, the latest draft bill calls for establishing a 'Data Protection Board' to enact the bill and govern data thereafter. Like its erstwhile predecessor, the Data Protection Authority, the composition and responsibilities of the eventual Board will be left to the discretion of the central government. Previous versions of the bill called for the data regulator to be staffed and managed by government officials which do create concerns over whether the state will remain exempt from the requirements that others will follow. Unfortunately, there is little clarity on this critical question in this draft.

This latest draft bill emphasises trust and protection, relative to its previous iterations while whittling away provisions that do not target or contribute to these objectives. Ultimately, the draft bill allows space for new problems to emerge and rule-making thereafter, instead of looking to regulators to foresee and address all issues now. Minister of State for Electronics and Information Technology, Rajeev Chandrasekhar, confirmed as much by adding that this draft bill will facilitate the "move towards more data-led governance where we can create analytical models to figure out the gaps and plug them". Time will either vindicate or refute Chandrasekhar's desire.

. . . . .

Dr Karthik Nachiappan is a Research Fellow at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore (NUS). He can be contacted at isaskn@nus.edu.sg.
The author bears full responsibility for the facts cited and opinions expressed in this paper.