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

ISAS Brief

No. 889 – 10 January 2022

Protecting India's Data

Karthik Nachiappan

Summary

After the recent tabling of a new report on its personal data protection legislation, India inches closer to a comprehensive framework to govern data, albeit one that strengthens state power over privacy.

After two years, India's Joint Parliamentary Committee (JPC) on data protection recently tabled its report on the Personal Data Protection (PDP) Bill in Parliament on December 16, 2021. The original PDP Bill (2019), drafted by the Srikrishna Committee, consisted of a range of provisions for managing, processing, and storing data. Qualms about the initial legislation led to the bill's referral to a JPC where policymakers and other stakeholders, including bureaucrats, businesses, activists, and data security experts, discussed how to improve the bill.

After scrutinising India's data protection legislation, the JPC offered 80 recommendations alongside 150 corrections to improve the legislation that will govern India's digital economy and safeguard privacy. The committee's mandate and deliberations are crucial to create a viable governance framework that will preserve and propel India's digital future. Once enacted, the updated draft legislation will create a framework and law that emboldens government control of data relative to privacy and security considerations.

The most contentious part of previous iterations of the bill was data localisation or provisions that obliged companies and organisations handling data of Indian citizens to store a copy within India. This provision was ostensibly relaxed due to pressure from American government officials and tech companies. Localisation requirements have not been totally excised but do remain, however fitfully, in the latest draft. As per the JPC report, firms seeking to transfer sensitive data out of India will require the approval of the data protection regulator and the central government. Free flow of data remains fettered by security concerns. The committee's report affirms the Indian government's preference to reinforce data sovereignty given the vital and strategic importance of data to India's economic trajectory. Data represents an area where India will unabashedly assert its sovereignty despite the misgivings of the United States and Big Tech.

Critically, the report further bolsters the government's hand and powers vis-à-vis data. Governmental agencies remain exempted from the bill's provisions, giving officials carte blanche access with some procedural constraints. Exemptions exist for the Indian government agencies as they collect and use data on grounds ranging from public order, national security and protecting India's sovereignty and integrity. The blanket exemption has, in effect, engendered a dual policy regime to govern data — one for the government and one for the private sector.

The most significant shift from the report has been expanding the remit to cover both personal and non-personal data, instead of just the former in the previous two versions. Indeed, the change is also reflected in the title; the bill will now be referred to as the 2021 Data Protection Bill, not the PDP Bill. The scope of the law, once passed, covers non-personal data, anonymous data generated in different ways. All references to personal data have been replaced by just 'data'. This change does indicate that the government prioritises controlling data over privacy since non-personal data has little bearing on privacy.

Conversely, personal data relates directly or indirectly to a specific individual. This proposed shift could also affect how companies and services handle personal information of their customers since they will have little incentive to de-identify personal data and make it anonymous which reduces personal harm to individuals. In effect, the government regards non-personal and personal data as community resources that can be monetised and leveraged for public benefit. By clubbing personal and non-personal data, however, the government favours collecting and leveraging data more than protecting privacy. Regulators will also seek to protect data not privacy when no distinctions exist between personal and non-personal data.

Other changes recommended by the committee appear positive. The personal data of children, however collected, will have to be done in the 'best interests of the child' with deference to parents and guardians. Data principals or individuals whose data is being collected and processed can file a complaint directly with the new data protection authority should they be unsatisfied with how their data has been handled. Data fiduciaries, entities that collect and manage data, must appoint data protection officers from upper management not lower levels. The reworked bill also includes a sunset clause, giving companies two years to adjust to new rules instead of being immediately applicable. The JPC text also limits the scope for employers to access employee data.

That India is on the cusp of finalizing and passing a data protection law is a net plus given its growing digital economy and market and the need for clarity to operate in it. India's digital economy and its position as a potential data hub hinge on this policy framework. The new framework will mark a definitive change in India's data governance. Initially, the first bill was conceived as a way of protecting privacy and enforcing the rights of users over their data. The 2021 Data Protection Bill has different ambitions — it lays down a data governance regime that exempts the government from the very provisions it imposes on others while paying lip service to privacy and individual welfare online.

. . . . .

Dr Karthik Nachiappan is 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.