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

ISAS Brief
No. 952 – 10 August 2022

India's Quest for a Data Protection Framework

Karthik Nachiappan

Summary

The long-running saga of drafting and passing a data protection bill continues with the Indian government unexpectedly withdrawing the proposed bill in parliament.

The Indian government withdrew the long-delayed legislation on data protection in early August 2022, citing the need to create a broader "comprehensive legal framework" to address prevailing concerns on data and related issues like privacy, social media regulation, cybersecurity, telecommunication regulations and non-personal data. This move comes nearly four years after the bill's introduction once the Justice Srikrishna committee completed its deliberations. The withdrawal will come as a surprise to firms and other entities operating in India's digital economy looking for clarity vis-à-vis data collection and sharing. Citizens are generally unsure of what happens to the data they submit while transacting online will be flummoxed by this withdrawal. Also jolted will be India's partners abroad, especially the United States and the European Union, and big technology firms keen to identify and soften, or deflect seemingly onerous regulatory burdens.

The delay, in effect, benefits the government, giving it more time to reconcile aspects related to data generation, collection and transfer. Indeed, the justification provided by the government attests to the complications tied to the legislation and the need to understand better how personal data connects with issues like cybersecurity, artificial intelligence (AI) and social media regulation. The time lost with this withdrawal, however, must be considered. India now has a vacuum in its data governance, just as its digital economy experiences meteoric growth. India is currently going through an inexorable pace of digitalisation that is centred on personal data – collecting, storing, using and transferring it. Across all sectors – from agriculture to welfare and retail – the Indian citizen engages through digital devices, applications, systems, mechanisms, portals and infrastructures that require policy clarity. The withdrawal of this bill means that all digital economic activity will occur in a legal and policy vacuum that will have to be addressed quickly.

The withdrawal also raises questions about India's need to accelerate and sustain its digital transformation. Domestic and foreign firms creating and running digital applications and services require a clear and transparent policy regime that will guide their investments and operations. The lack of a data protection framework could stymie innovation as firms withhold investments or expansion decisions, given the uncertainty around a law that governs how they use the data they collect. In addition, Indian citizens increasingly require sufficient recourse should tech firms misuse or breach their personal data. The scrapped data protection bill listed the measures firms would have to undertake during such scenarios. An urgent need exists to protect India's internet users from social media platforms and other firms that collect their data.

The abandoned bill – the Personal Data Protection Bill (2019) – would have also mandated internet and social media firms like Google, Amazon and Meta to obtain consent to use and leverage user data and added other obligations to protect and safeguard data from being abused or exploited. The bill would have also created a provision expecting technology firms to store sensitive data about Indian users within the country, a stiff test for technology firms looking to expand digital presence in India. The bill would have also created a regulator – the Data Protection Authority – with an ostensibly broad mandate over implementing and enforcing the legislation. Critics were lamenting the potential powers that this body would accrue over India's growing digital economy and the bill's provisions that would have exempted the state from the rules others, especially private firms, would have to follow. Unfortunately, scrapping the bill does little to quell these concerns. We must wait and see whether the new legislation or what the government calls "a comprehensive legal policy framework" will address those issues.

Little is known now of the future bill that will eventually surface. There is speculation that the government will allow unconstrained data transfers between 'trusted geographies' instead of pushing blanket data localisation. 'Trusted geographies' suggest that the government is open to unfettered data sharing and transfer between India and certain jurisdictions with high levels of digital and cybersecurity and where seamless data transfer would be possible. The larger focus is to create a comprehensive legislation to upgrade and replace the 2000 IT Act, currently the regulatory statute governing digital issues. As a result, the remit of the new legislation could be vast, covering issues like cybersecurity, AI, social media, and personal and non-personal data. The timeline for this new legislation is also unknown though the government has promised to table the legislation by early 2023 during the parliament's winter session. Undoubtedly, pressures to draft, complete and table the new data protection bill will only intensify as India's digital economy flourishes, and the policy vacuum festers.

. . . . .

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.