Centre for The Digital Future

Op Ed

The Data Protection Bill is dead, long live the Data Protection Bill

BY

NISHANT CHADHA
CENTRE FOR THE DIGITAL FUTURE

AUGUST, 2022

On August 3, the Union IT minister, Ashwini Vaishnaw, announced in parliament that the government was withdrawing the Data Protection (DP) bill from the Lok Sabha. The Bill was introduced in 2019 and had been referred to a joint committee of the parliament (JCP). The JCP proposed 81 amendments and 12 recommendations were made toward a comprehensive legal framework for the digital ecosystem. Reconsidering the Bill is a good step. In its current avatar, the bill will do little to provide users any real protection online but may well stymie the growth of an indigenous digital economy. The new version of the Bill needs to get this balance right. And a good first step towards this will be to divorce the Bill from the General Data Protection Rules (GDPR) in the European Union (EU) and think afresh.

The core of the withdrawn bill is the consent framework, incidentally, almost a replica of the GDPR. This framework, if implemented well, ensures that the data fiduciary (loosely understood as the collector of the data) provides enough information to the data principal (the person to whom the personal data refer, the user) to allow the data principal to control the use of their data. Thus, this framework tasks the user with preserving their own privacy and safety online. In the complex digital economy, where the data fiduciary has much more information and understanding of how collected data will be used than the data principal and also more bargaining strength, this is unlikely to work. It will simply require too much effort, time, and technical understanding on the part of the user.

Imagine living in a country where automobile safety is regulated and provided through a framework rather like the consent framework. The car companies are not actually required to make their cars safe - they are simply required to inform the customer how safe or unsafe the car is. In this imaginary setting when you go to buy a car you find a row of them with different makes and models, and, affixed to each of the windshields are the safety parameters of that model. A list of at least 58 items! At present, the Central Motor Vehicles Rules, 1989 (CMVR 1989) list 58 requirements that cars in India have to fulfil. You have to study all 58 all of them and decide whether you find the car safe enough.

This list will range from details of the brake hose and brake fluids to interior fittings and even overall dimensions. I don’t think even automobile engineers will be able to make such informed choices, forget laypeople. And what such a framework for safety will do is throttle competition in the car market. Buyers will flock towards knows models and makers since they will find it impossible to judge a newer model for safety. Do we want to create a situation like this in the innovation intensive digital economy?

While the consent framework may not provide much to users in the way of protection it can hurt the growth of the digital economy. I will take the example of two provisions here - collection limitation and purpose limitation. Collection limitation restricts companies from collecting more data than they need and

purpose limitation restricts them from using collected data for any purpose other than what the user initially consented to. Aside from the obvious problem of who decides what are the exact categories of data needed to provide a service, these restrictions hit at the heart of how the digital economy functions and grows. Companies do not know what data they will need when they start out developing a service. They experiment and innovate until they arrive at the most parsimonious models. So how will they know what is the exact data needed to provide a service? Similarly, economies of scope are the backbone of the digital economy. Data is recombinant and different datasets can be combined to provide services that could not have been possible with standalone data. How is such innovation to happen if companies have to go back to the users to seek fresh consent every time they want to engage in such experimentation? Even the GDPR and the California Consumer Privacy Act (CCPA) allow companies to use collected data for materially similar purposes.

Early evidence from the EU suggests that the GDPR has had significant negative effects on startup activity, hurting their growth and formation, and entrenching the advantage of the incumbents in most markets. The Centre for The Digital Future (CDF) carried out an online survey of startups to understand the possible impact of the DP Bill - especially the consent framework - on their business activity. An overwhelming number, about 70%, reported that purpose limitation and the issue of seeking fresh consent would adversely impact them. This is certainly not a desirable situation for a country with significant ambitions in the digital economy.

The minister has indicated that a new version of the bill will be introduced soon. To take India’s digital economy to the next step trust is important. Users have to believe that their data and information are safe online. Companies need to have certainty in their operations and the freedom to innovate. Providing users protection for their data online will necessarily involve some restrictions on what companies can do with the data they collect. This is only fair. However, we need to avoid having regulations that hurt the economy without achieving the primary purpose of protecting users online and ensuring that their data and information are really safe online - especially for the most vulnerable. Those who will not be able to make themselves safe.

(A version of this article first appeared in *The Economic Times* on August 5, 2022.)