

Why the Personal Data Protection Bill Won't Stop Data Proliferation in Digital India

*India is rapidly digitising. There are good things and bad, speed-bumps on the way and caveats to be mindful of. The weekly column **Terminal** focuses on all that is connected and is not – on digital issues, policy, ideas and themes dominating the conversation in India and the world.*

The Digital Personal Data Protection Bill 2022 is finally expected to be pushed through the parliament this Monsoon Session.

Nearly five years after the Supreme Court judgement on the right to privacy in *Puttaswamy Vs Union of India*, this Bill is too late and entirely ignores our fundamental right to privacy in the data economy. The final draft of the Bill also ignores the years of public consultations, disregarding Indians' roles in giving ourselves a dignified way to be safe in Digital India.

Let's be real about the upcoming Bill. It is, first and foremost, inadequate to address the threats posed in this era of surveillance capitalism. The Bill is more of a rubber stamp that is coming at the end of a digitisation process which has been allowed to run uninterrupted with no safeguards at any stage. We needed a privacy law a decade ago, but it was never a priority and now that we have a law, it will be one that threatens to undermine our constitutional rights.

The very idea of Digital India has been to promote a data economy where data is the foundation for all forms of economic transactions – a prime feature of surveillance capitalism.

This economic setup, by design, wants proliferation of our personal data through institutions that are controlled by the government.

Every digital infrastructure project from Aadhaar, UPI and Digital Locker to CoWIN and Aarogya Setu has promoted this proliferation by providing Application Programming Interfaces to the private sector for building a data economy. It is this proliferation that is causing all the problems as it has no controls in place as to who uses our personal data. No law can change this when the systems remain the same.

One of the key wins around the public movement around digital rights in India has been to make the Supreme Court of India understand unrestricted proliferation of personal data. This is reflected in the judgement on Aadhaar, where the court categorically restricted and cut down the provisions of the Aadhaar Act allowing private sectors' access to Aadhaar. These wins, however, have been quickly over-ruled by the parliament with amendments to the Aadhaar Act to allow Aadhaar to be shared again with the private sector with the excuse of the Prevention of Money Laundering Act and good governance.

To be blunt, the Supreme Court judgements around Aadhaar did not result in active changes in the architecture or code of the Aadhaar system.

I can categorically say there has not been a single line of change in the code or architecture of Digital India either because of the court judgements.

But before the judgement there was a lot of public scrutiny of the system. New privacy-respecting provisions like Virtual ID, Masked Aadhaar and locking of biometrics were all brought in because of the public demand for privacy and security measures. While some features remained and some were ignored like the Virtual ID, the changes only happened because of pressure from citizenry.

In cyberspace, software code becomes rules and architecture translates into legislation.

The way digital infrastructures are designed, implemented and function is entirely dependent on software code. In Digital India, software code enforces rules of government, private corporations and technocrats. These have been codified and turned invisible to society at large. No matter what a judgement of a court, a legislation by the legislature or a rule by the government is, as long as the code remains unchanged, these laws of humans are not being enforced by machines.

Whatever form the Data Protection Bill may take, good, bad or ugly, it will not help if the engineers who build these systems do not change their software to adapt to the provisions of the law. Even with a very good Data Protection Bill with an independent regulator which really wants to implement the law, it will be really hard to change decades of digitisation that led to so many social problems. Enforceability of laws has never been a strong domain of the Indian state, and especially with cyberspace, it becomes a challenge in many different ways.

Given this background, members of legislature and the judiciary can't be oblivious around this issue while designing social protections for the public. If the laws of the land are being made so distant from social realities, then the process in itself is devoid of legitimacy. This is especially true in the case of the Data Protection Bill, where at every stage economic interests were used as an excuse to limit discourse and need for social protections.

A digital economy has emerged as a social need where certain practices that may promote digitisation, are also harming society at large. It is these social harms that need to be arrested, while allowing safe practices to flourish. The current version of the Data Protection Bill will not do that. As much as one wants a Data Protection Bill to be quickly enacted, these poorly drafted laws, which do not protect the citizenry, are of no use other than to make media announcements that claim that we are the best digital society in the world.

In the end, the Digital Personal Data Protection Bill, 2022, will do more harm to the fundamental right to privacy than help protect it – with all the exceptions it provides. With this version of the bill, the state is making its intent clear that it has no interest in safeguarding our fundamental rights. In such a situation, it is up to people to educate themselves and stay safe as the guard has now turned into a thief himself.