Gaps in data protection*

Subhashis Banerjee†

Computer Science and Engineering, IIT Delhi
New Delhi 110016

July 9, 2023

The Union Cabinet on Wednesday approved the draft data protection bill which is envisaged to be the bedrock for the digitalisation and data endeavours of both the state and the private sector. The bill will now go to the parliament for debate and approval. The bill is crucial because, irrespective of our levels of digital literacy or comfort with digital technologies, digitalisation and data will inevitably and increasingly impact vital aspects of our public and private lives. But, does the draft bill adequately address the still extant public concerns that led to the unanimous privacy judgement by a nine-judge bench of the SC almost six years back? I think not.

The central design objective of the bill appears to be to facilitate data collection and processing by the government and private entities, rather than to address the public concerns for data protection that led the SC to recognise privacy as a fundamental right of citizens. The SC identified informational self-determination to be crucial for protection of privacy and liberty of individuals, and laid down the standards of determination with the three-fold tests of legality, legitimacy and proportionality. The requirement of legality suggests that there need to be enabling laws as preconditions, at least for large public service digital applications of the government. This includes digital surveillance for law enforcement. But, surprisingly, the sense of the draft bill seems to be the opposite. Section 5 actually seems to suggest that the proposed Act will allow any purpose which is not expressly forbidden by law.

Legitimacy demands that the state should be obligated to establish that there is a legitimate interest behind a proposed digitalisation, and proportionality demands that the digital application should be the least intrusive for the purpose and that there should be balancing of the extent to which fundamental rights are likely to be impinged. Surprisingly, the bill does not lay down the standards for either of these tests. Legitimacy, which should require a rigorous and not a mere speculative theory of public good, is not addressed at all, and the required standards for proportionality are also left unclear. The vague directives of "reasonable efforts" and "appropriate technical and organisational measures" are clearly inadequate for determining whether an application is the least intrusive for the purpose, or that it balances the risks correctly. In particular, balancing requires specifying clear standards for both risk assessments and legitimacy which the data protection bill should have addressed. It appears to be entirely unlikely that these standards can be worked out without well thought out guidelines and a pre-determined grammar, or that they can be left to subordinate regulations.

An effective data protection bill also needs to understand the various nuances of privacy risks from digital applications. As legal scholars like Daniel Solove and others have pointed out – and have also been extensively cited and elucidated in the SC judgement – that apart from the risks of

*The articles is based on the version of The Digital Personal Data Protection Bill, 2022 available at https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf.

†Views are personal.

direct harms arising out of illegal surveillance, profiling and possible uncovering of one's private world to the public, the risks from other indirect harms also need to be considered. These typically arise out of invasions that link siloed data items to create digital hallucinations of personae and use them inappropriately, or loss of informational self-determination that lead to unknown, insensitive and opaque entities using unknown aspects of personal data in unknown ways. The indirect harms are often hard to detect, because their effects are more subtle and long-term. Hence, the measures of post-violation complains and penalties – of the type envisaged in the draft bill – are simply not adequate. Protection from indirect harms needs to be ex-ante rather than ex-post, and data fiduciaries and data controllers need to have exacting standards for ex-ante privacy protection and purpose limitation which the draft bill seems to have failed to recognise.

The other problematic aspect of the draft bill appears to be its over-dependence on consent. Apart from unreasonably putting the onus on unsuspecting individuals to recognise the privacy risks entailed in complicated digital applications, consent also often presents a false choice. Denying consent in pervasive applications may unreasonably limit options, cause hardships or put barriers in freedom of expression. Hence, effective data protection requires an accountability-based rather than a consent-based framework, which puts the onus on data controllers and fiduciaries irrespective of the level of consent. This is not to say that consent is not required but that one cannot hide behind consent for privacy protection. Also, the section on "deemed consent" and the exemptions of Section 18 seem to grant dangerous powers to the state or even employers. The clauses of deemed consent under "in public interest" or "for provision of any service or benefit to the Data Principal...by the State or any instrumentality of the State" appears to be unacceptably empowering.

The draft bill is also completely silent about the standards of anonymisation, encryption and access control. These are not mere technical and operational issues, but crucial considerations for digitalisation and data without which any data protection discourse is woefully incomplete. Even if the details are relegated to subordinate regulations, the objectives and standards need to be clearly specified in an effective and modern data protection bill.

Similarly, a data protection bill that fails to address the concerns of fairness, bias and misinformation that arise out of automated processing of data, especially by AI applications, is probably outdated even before it is passed. The concerns are many, and they are reasonably well articulated in various discourse. An effective data protection bill must take these in to account.

In summary, the bill falls short of expectations in many respects. Most significantly, it bears testimony to a mindset of technocrats and the executive to somehow bypass the objections and concerns – including those articulated in the SC judgement – in their zeal to enable digitalisation, rather than try to understand and address them in earnest. This should hopefully change.