Source : www.thehindu.com Date : 2021-04-12

WHY THE PERSONAL DATA PROTECTION BILL MATTERS

Relevant for: Security Related Matters | Topic: Challenges to internal security through Communication Networks

The pandemic has forced more people to participate in the digital economy. More people have taken to digital channels to fulfill a variety of needs like purchasing groceries and accessing health services. Unfortunately, the number of personal data breaches from major digital service providers has increased worryingly in the same period. The recent alleged data breach at MobiKwik could stand to be India's biggest breach with the data of 9.9 crore users at risk. Robust data protection regimes are necessary to prevent such events and protect users' interests. Unfortunately, the existing data protection regime in India does not meet this standard.

However, the Personal Data Protection Bill, 2019, now under scrutiny by a Joint Parliamentary Committee, could play a big role in providing robust protections to users and their personal data. In this context, this article seeks to answer a fundamental question: How can the Bill protect users' interests in the digital economy?

Editorial | For a data firewall: On need for a data protection law

How different entities collect and process users' personal data in India is mainly governed by the Information Technology Act, 2000, and various other sectoral regulations. However, this data protection regime falls short of providing effective protection to users and their personal data.

For instance, entities could override the protections in the regime by taking users' consent to processing personal data under broad terms and conditions. This is problematic given that users might not understand the terms and conditions or the implications of giving consent. Further, the frameworks emphasise data security but do not place enough emphasis on data privacy. In essence, while entities must employ technical measures to protect personal data, they have weaker obligations to respect users' preferences in how personal data can be processed. As a result, entities could use the data for purposes different to those that the user consented to. The data protection provisions under the IT Act also do not apply to government agencies. This creates a large vacuum for data protection when governments are collecting and processing large amounts of personal data. Finally, the regime seems to have become antiquated and inadequate in addressing risks emerging from new developments in data processing technology.

The need for a more robust data protection legislation came to the fore in 2017 post the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy (Retd) v. Union of India* that established the right to privacy as a fundamental right. In the judgment, the Court called for a data protection law that can effectively protect users' privacy over their personal data. Consequently, the Ministry of Electronics and Information Technology formed a Committee of Experts under the Chairmanship of Justice (Retd) B.N. Srikrishna to suggest a draft data protection law. The Bill, in its current form, is a revised version of the draft legislative document proposed by the Committee.

MPs raise concerns over exemptions in Data Protection Bill

The proposed regime under the Bill seeks to be different from the existing regime in some prominent ways. First, the Bill seeks to apply the data protection regime to both government and private entities across all sectors.

Second, the Bill seeks to emphasise data security and data privacy. While entities will have to maintain security safeguards to protect personal data, they will also have to fulfill a set of data protection obligations and transparency and accountability measures that govern how entities can process personal data to uphold users' privacy and interests.

Third, the Bill seeks to give users a set of rights over their personal data and means to exercise those rights. For instance, a user will be able to obtain information about the different kinds of personal data that an entity has about them and how the entity is processing that data.

Fourth, the Bill seeks to create an independent and powerful regulator known as the Data Protection Authority (DPA). The DPA will monitor and regulate data processing activities to ensure their compliance with the regime. More importantly, the DPA will give users a channel to seek redress when entities do not comply with their obligations under the regime.

India's data protection law has potential to propel digital economy, says Facebook

The Bill seeks to bring a massive and meaningful change to personal data protection in India through this regime. However, the reality could be different. Several provisions in the Bill create cause for concern about the regime's effectiveness. These provisions could contradict the objectives of the Bill by giving wide exemptions to government agencies and diluting user protection safeguards.

For instance, under clause 35, the Central government can exempt any government agency from complying with the Bill. Government agencies will then be able to process personal data without following any safeguard under the Bill. This could create severe privacy risks for users.

Similarly, users could find it difficult to enforce various user protection safeguards (such as rights and remedies) in the Bill. For instance, the Bill threatens legal consequences for users who withdraw their consent for a data processing activity. In practice, this could discourage users from withdrawing consent for processing activities they want to opt out of.

Additional concerns also emerge for the DPA as an independent effective regulator that can uphold users' interests.

The issues around data localisation

The time is ripe for India to have a robust data protection regime. The Joint Parliamentary Committee that is scrutinising the Bill has proposed 86 amendments and one new clause to the Bill – although the exact changes are not in the public domain. The Committee is expected to submit its final report in the Monsoon Session of Parliament in 2021. Taking this time to make some changes in the Bill targeted towards addressing various concerns in it could make a stronger and more effective data protection regime.

Indradeep Ghosh is the Executive Director of Dvara Research and Srikara Prasad is a Policy Analyst at the Future of Finance Initiative housed at Dvara Research

Please enter a valid email address.

END