SPECIAL REPORT no. 205

The Draft Digital Personal Data Protection Bill 2022: Recommendations to the Ministry of Electronics and Information Technology

Trisha Ray, Shravishtha Ajaykumar, and Sameer Patil

JANUARY 2023

Introduction

On 1 December 2022, the Observer Research Foundation hosted a roundtable discussion on the Digital Personal Data Protection Bill, 2022. The discussions elicited feedback from stakeholders representing platforms, startups, civil society, consultancies, and academia on three themes:

Data collected by third parties for use by government agencies/entities: The Bill provides for multiple parties to collect and retain data with "deemed" consent, including third-party organisations. In the Bill, the organisation collecting information is permitted to retain personal data for business and legal purposes; however, third-party organisations have inadequate outlined accountability. The patchy data security practices of third parties, including unsecured public buckets and endpoints, have been the source of major data breaches over the past five years. It is, therefore, essential to discuss the accountability of these third parties, even as the government itself is exempted from the Bill.

Rights of the Data Principal: The current draft Bill also differs from the previous versions in one important aspect: discarding the category of sensitive personal data. This typically includes biometric, financial, and genetic data, which require an additional layer of protection. However, by doing away with this categorisation, it appears that the current draft offers a diminished safeguard for personal data.

Disclaimer

The recommendations are based on a stakeholder consultation organised by ORF on 1 December 2022. Although the authors have made the best efforts to give voice to the concerns of various stakeholder groups, this is not a consensus document and does not attribute comments to, or claim to represent, the positions of any individual or organisation. All statements, assertions or factual errors are attributable only to ORF.

Localisation and Cross-Border Data Flows: In the last few years, India has placed a strong emphasis on data localisation in international forums, even proposing a framing of digital sovereignty based on data at the United Nations Open-Ended Working Group on Cyber. The removal of broad localisation requirements aligns India with international partners; instead, the Bill states that the central government will notify countries or territories outside for this purpose after an assessment, although the draft does not illustrate parameters for such an assessment.

Based on the feedback received during the roundtable discussion, ORF submitted to the Ministry of Electronics and Information Technology, as part of the call for comments, recommendations in the following three areas:

1. Recommendations for notifying trusted geographies

2. Constitution and functioning of the Data Protection Board of India

3. Rights of the data principal

Recommendations for Notifying Trusted Geographies

Section 17 of the draft Bill states, "The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified." This is a positive development and addresses concerns regarding data localisation and digital sovereignty from India's partners. Additionally, this provision more closely aligns India with its partners around the world.

While the provision in the draft Bill is a welcome step, it does not specify the parameters for the government's assessment of trusted geographies—the countries or territories where data will be transferred. To address this, the government could add an appendix to the Bill outlining the criteria for such an assessment. For example, India could follow the European Union's "data adequacy" template, which certifies countries that have robust data protection standards and are, therefore, eligible to receive and host data from EU member states. In addition, India could use principles such as the rights of data principals, the use and disclosure of data, and the state of security and encryption standards to determine the eligibility of a given country.

A critical aspect of cross-border data flows is the ability to access the data for national security and other purposes. For instance, the need to access the data of Indians in cybercriminal investigations was cited as the primary reason for enforcing data localisation. Therefore, when conducting this assessment, the government must also consider this dimension and ensure it can access the data as needed.

In addition to addressing access to data, the government must also ensure that the provision for trusted geographies does not result in data concentration in only one location, where most tech companies are located. This would ultimately undermine the purpose of the provision for cross-border data flows. To prevent this, the government must specify the parameters for assessing data transfer to other jurisdictions. This will enhance privacy and potentially pave the way for an Indian model of data protection similar to the European General Data Protection Regulation.

Constitution and Functioning of the Data Protection Board of India (Chapter 5)

The Bill is primarily a regulation meant to foster the responsible and inclusive growth of India's digital economy. As such, it is framed in accordance with traditional market regulation paradigms where the State is the intermediary between businesses (in this case, the data fiduciaries) and consumers (the data principals). It devises policies that regulate businesses, in the interest of fostering economic growth while maximising social benefit.[1]

The Data Protection Board of India (DPBI) has the following outlined functions:

- Determine non-compliance and impose penalties.
- Direct individuals, as defined by the Act, to act in accordance with the Act, and withdraw/modify/suspend such directions as it sees fit.
- Direct data fiduciaries to adopt measures to mitigate harm to data principals, and act to address a data breach.

The Bill states that the DPBI shall function as an independent body, functioning as a digital office. In furtherance of this goal of independence, we recommend that the DPBI take a co-regulatory approach.

Co-regulation is a regulatory model where the State and private sector collaborate in implementing regulations. The rationale for co-regulation in data governance is two-fold. First, it addresses issues of government resource shortages. ORF's submission on the Personal Data Protection Bill 2019 highlights the steep operational, technical, and human costs of data audits and analysis.[2] The implementation of the Digital Personal Data Protection Bill, as it stands, will be a massive strain on the limited government funding and manpower. Second, it accommodates diverse stakeholder viewpoints within the governance mechanism itself. Furthermore, the success of co-regulation is conditional on three tenets: transparency, clear definition of objectives and benchmarks of success, and robust dispute resolution mechanisms.[3]

The DPBI should provide overarching directions to data fiduciaries, in keeping with the re-orientation of the Bill toward a leaner, more flexible legal mechanism. It should encourage industry to develop enforceable standards for data privacy, safety, and integrity, with its own role being to ensure that such standards are regularly updated with the data principal's interests in mind, along with other parameters as mentioned in Section 2(18).

We also recommend that the DPBI consider the accessibility implications of functioning as a digital office.

Rights of the Data Principal

Under Chapter 3, which discusses the rights and duties of the data principal, there are specific gaps that must be addressed:

- **Difference Between Sensitive Personal Data and Personal Data**

The draft Bill discards the categories of sensitive personal data and critical personal data. Yet, there is a crucial difference in practice: while personal data can be information that someone can use to identify (with some degree of accuracy) a living person, some categories of data that include sensitive characteristics (like racial and ethnic background, and genetic and health information) necessitate greater protection.[4] This type of personal information needs to be highlighted as a protected sphere, in a way that ensures there is no detrimental impact on the data principal's access to critical services, like banking, schooling, and other social infrastructure.[5]

- **Age of Consent**

The draft Bill states that a 'child' is a person who has not reached 18 years of age. The draft says that the data fiduciary must have verified parental consent from such data principals, based on a predetermined method of collection.

However, this definition must address the reality of who has access to technology at the ground level. In India, 85 percent of non-adult users have access to cell phones. This population spends an average of five hours online daily, with 80 percent acknowledging using social media and 80 percent noted an interest in spending time on OTT platforms.[6]

With a large segment of the youth being online, nuances in age differences, and even social backgrounds permitting such access, need to be considered. The Bill does not consider the difference between the autonomy of a five-year-old and that of a 15-year-old, for instance. Thus, nuances regarding the age groups, the value of parental consent, the consistency and longevity of said parental consent, and the possible removal of this consent need to be discussed in greater detail.[7]

Another issue regarding the age that is missing in the Bill is the protection of the elderly. In many instances, the elderly are disproportionately vulnerable due to their lack of familiarity and fluency with online platforms and digital technologies. Protections for the elderly, similar to the protections for minors, will also assist in increasing digital inclusion.[8] The penalties imposed by the Bill for raising false or "frivolous" complaints (Section 16) are a barrier to the inclusion of digital non-natives.

For a country like India where most of the population is relatively new to digital platforms, and still has a rudimentary understanding of digital rights, such a steep penalty may have a chilling effect and discourage even valid claims.

Further, the onus is on the data principal to present a fair claim, weakening protections for the data principal. In this vein, the Bill could use the OECD's Privacy Framework's individual participation principle, which seeks to maximise the individual's knowledge and participation, as a frame.[9]

Participants

Abhishek Jain, Privacy Manager, Public Policy (India), Meta

Anoushka Roy, Public Policy Associate, PWC

Antara Vats, Junior Fellow, Centre for Security, Strategy and Technology, ORF

Aparajita Bharti, Co-founder, The Quantum Hub

Apoorva Lalwani, Associate Fellow, ORF

Arindrajit Basu, Non-resident Research Fellow, Centre for Internet and Society

Astha Kapoor, Co-founder, Aapti Institute

Berges Y. Malu, Senior Director, Public Policy, ShareChat

Devashree Shah, Associate Principal Counsel, Data Privacy, Disney

Gangesh Verma, Senior Associate, Saraf Associates

Gulshan Rai, Distinguished Fellow, ORF

Hardeep Singh, Legal and Policy Head, Cred

Isha Suri, Senior Researcher, Centre for Internet and Society

Kazim Rizvi, Founding Director, The Dialogue

Kumar Deep, India Lead, Information Technology Industry Council

Nehaa Chaudhari, Partner, Ikigai Law

Neha Singh, Director of Public Policy, CoinDCX

Nikhil Iyer, Senior Analyst, Public Policy, The Quantum Hub

Pranav Bhaskar Tiwari, Empowerment Specialist, Fellowships, Internet Society

Sameer Patil, Senior Fellow, ORF

Shravishtha Ajaykumar, Associate Fellow, Centre for Security, Strategy and Technology, ORF

Sourabh Lele, Correspondent, Business Standard

Tejasi Panjiar, Associate Counsel (Policy), Internet Freedom Foundation

Tejaswita Kharel, Centre for Communication Governance, NLU Delhi

Trisha Ray, Deputy Director, Centre for Security, Strategy and Technology, ORF

Vignesh Shanmugam, Centre for Communication Governance, NLU Delhi.

Endnotes

1 Richard A. Posner, "Theories of Economic Regulation", NBER Working Paper No. 41 (May 1974); Nancy Rose and Paul Joskow, "The effects of economic regulation", Chapter 25 in Handbook of Industrial Organization, 1989, vol. 2, pp 1449-1506

2 ORF Technology and Media Initiative, "The Personal Data Protection Bill 2019: Recommendations to the Joint Parliamentary Committee," ORF Special Report No. 102, March 2020, Observer Research Foundation. https://www.orfonline.org/research/the-personal-data-protection-bill-2019-61915/

3 Glen Hepburn, "Alternatives to Traditional Regulation", OECD Report (OECD: 2013), https://www.oecd.org/gov/regulatory-policy/42245468.pdf.

4 Luke Irwin, "Personal Data vs Sensitive Data: What's the Difference?", IT Governance Blog, February 18, 2021, https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data; "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD, updated 2013, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

5 Vipul Mathur and Arpit Kumar Parija, "Bias in banking", World Bank, October 5, 2021, https://blogs.worldbank.org/allaboutfinance/bias-banking.

6 Anurag Singh Bohra, "Patterns of Internet Usage among Youths in India," Social Media Matters, December 16, 2022, https://www.socialmediamatters.in/patterns-of-internet-usage-among-youths-in-india#.

7 Lokesh Choudhary, "DPDPB Opts 'One Size Fits All', Ignores Vulnerable Age Groups", *Analytics India*, November 29, 2022, https://analyticsindiamag.com/dpdpb-opts-one-size-fits-all-ignores-vulnerable-age-groups/.

8 Sofiat Akinola, "How Can We Ensure Digital Inclusion for Older Adults?" World Economic Forum, October 1, 2021, https://www.weforum.org/agenda/2021/10/how-can-we-ensure-digital-inclusion-for-older-adults/.

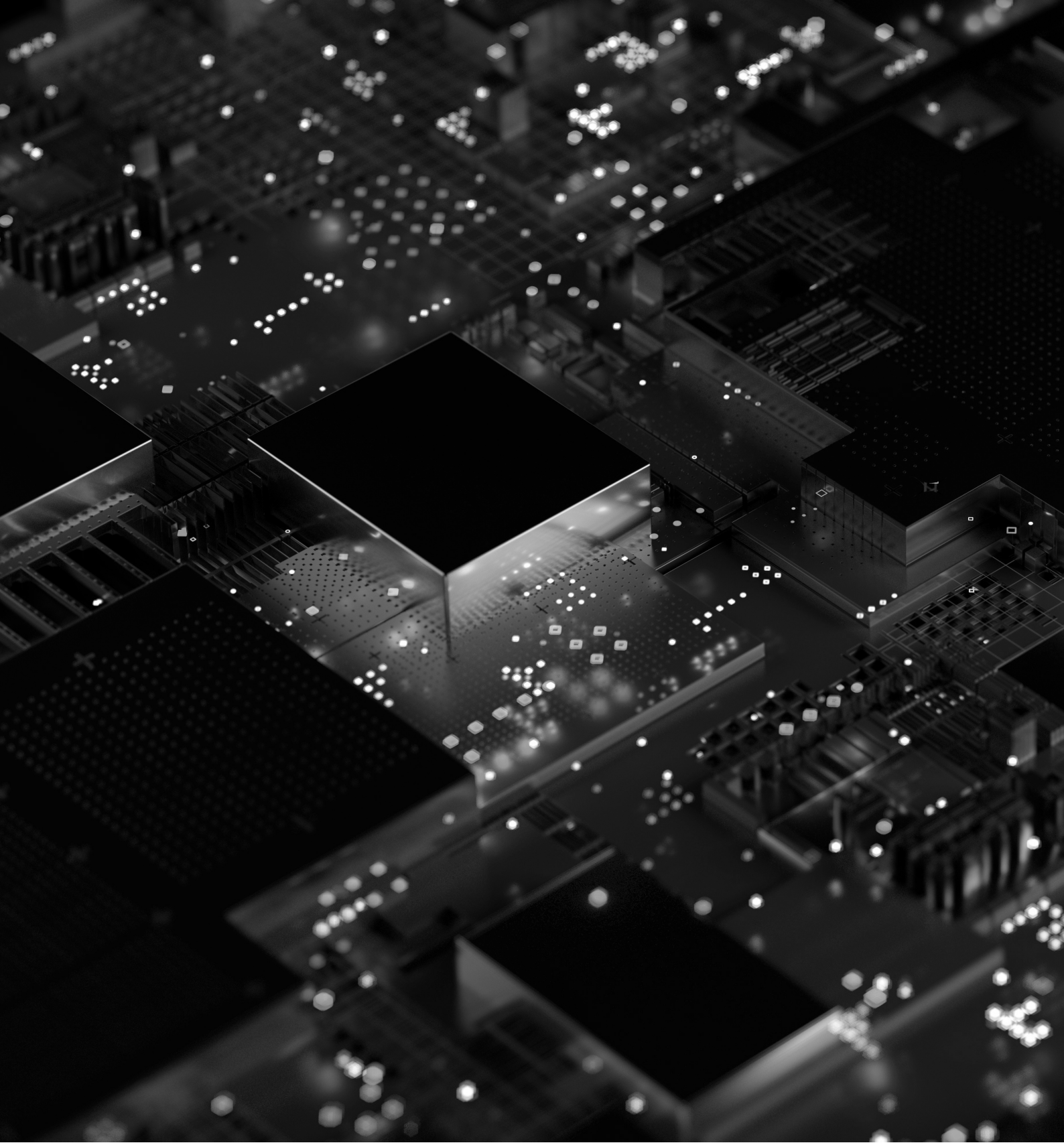
9 "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"; *The OECD Privacy Framework*, OECD, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

About the Authors

Trisha Ray *is a Deputy Director, Centre for Security, Strategy and Technology at ORF.*
Shravishtha Ajaykumar *is Associate Fellow at the Centre for Security, Strategy and Technology at ORF.*
Sameer Patil *is a Senior Fellow at ORF Mumbai.*

Attribution: Trisha Ray, Shravishtha Ajaykumar, and Sameer Patil, "The Draft Digital Personal Data Protection Bill 2022: Recommendations to the Ministry of Electronics and Information Technology," *ORF Special Report No. 205, January 2023*, Observer Research Foundation.

Cover image: Getty Images/ Andriy Onufriyenko
Back cover image: Getty Images/Andriy Onufriyenko



OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org