102

ORF SPECIAL REPORT

MARCH 2020

The Personal Data Protection Bill 2019: Recommendations to the Joint Parliamentary Committee

ORF Technology and Media Initiative

Getty Images/Andriy Onufriyenko

Attribution: 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.

Observer Research Foundation (ORF) is a public policy think tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research, and stimulating discussions.

To know more about ORF scan this code

ISBN: 978-93-89622-72-0

Disclaimer

The contents of this response are based on a stakeholder consultation organised by ORF on 7 February 2020. Although we have made our best efforts to give voice to the concerns of various stakeholder groups, this response 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.

INTRODUCTION

On 7 February 2020, the Observer Research Foundation convened a non-partisan multi-stakeholder roundtable to solicit views on the Personal Data Protection Bill 2019 (PDP Bill).[1] The roundtable focused on Sections 35 and 91 of the Bill, tackling two key questions that concern industry and civil society organisations: (a) the Central Government's power to exempt agencies from the Bill's provisions; and (b) the government's access to anonymised and/or non-personal data gathered by data fiduciaries and processors.

The roundtable focused on these provisions because they re-animate India's digital 'trilemma' of simultaneously generating economic growth, protecting individual privacy, and safeguarding national security. These tensions have manifested themselves repeatedly across the policy life cycle of the Data Protection Bill, including in the Justice B. N. Srikrishna Committee report[2] and in the Supreme Court's verdict in *K.S. Puttaswamy v. Union of India*.[3]

Based on the discussions at the roundtable, this special report advances two preliminary propositions on data as it relates to national security and economic growth for the Joint Parliamentary Committee (JPC) to consider.

1. National security is better served by streamlining state oversight to prevent information overload and duplication of effort.

In an interdependent and data-abundant world, government access to data is a necessary but insufficient condition to ensure optimal national security outcomes. The digital economy is influenced by a multi-layered ecosystem of domestic laws, commercial choices, bilateral arrangements, and international norms and institutions. In this ecosystem, access to data is *one tool* to secure our increasingly digital societies. This tool must be complemented by others, such as transparency and accountability frameworks for technology platforms, new bilateral data-sharing agreements, and cooperation with international security organisations.

Where access to data is necessary, it would be in the government's interest to tailor access norms as narrowly as possible, including by providing clear stipulations on the conditions under which data can be accessed, the precise nature of data that can be sought, and the purpose for which it can be accessed.

Sifting through large volumes of data incurs operational, technical and human costs, increasing the time and effort required to glean actionable intelligence. Government[4] and academic[5] research on the US National Security Agency's surveillance of phone meta data, for instance, reveals that the project had little discernible impact on preventing terrorism, while consuming a disproportionate amount of the intelligence agency's resources. A tailored provision under the Data Protection Bill would exempt a limited number of agencies from protection standards, but would employ judicial, executive and technological safeguards that prevent information overload.

Beyond reasons of state capacity, avoiding information overload is also a cyber security imperative. A longer list of organisations which store sensitive information also multiplies the vectors for malicious non-state and state behaviour. Exempting agencies operating without a clearly defined national security purpose or without established industrial security standards may well make them susceptible to similar risks. Streamlined state powers will also be more conducive to ensuring they do not infringe the clearly defined parameters on the protection of individual rights, and enable compliance with established judicial and legislative standards for executive national security action.

2. Generating social and economic value from data will require reforming laws and rules in the fields of market power and competition, contract law, intellectual property rights, taxation, and international trade.

Personal and non-personal data will likely be used in a variety of business and state operations, and will be shared, transferred and processed across multiple actors. Facilitating this flow will require complementary and enabling regimes. Formalising ownership structures will be crucial to this effort. Individuals, businesses and the government must share a common lexicon on the different types of data and the protection standards afforded to them. The Organisation for Economic Cooperation and Development (OECD), for instance, identifies[6] three broad categories of data (private, proprietary and public), and at least another four sub-categories based on the origin of data.

The government will also have to create new regimes for sharing data between multiple stakeholders that take into account considerations of competition, intellectual property rights, privacy and cyber security. The EU, for instance, has identified[7] four potential alternative models for private sector to government data sharing: standardising data sharing contracts; data donorship models, similar to Corporate Social Responsibility (CSR) obligations; new intermediary institutions, such as data trusts; and regulatory models for public interest reasons in the fields of healthcare, finance, among others.

We reiterate that the Data Protection Bill should only be seen as one tool in an overarching architecture that leverages data to serve development outcomes. Regulators should be wary of attempting to achieve through the Bill outcomes that could be better achieved using other policy levers.

RECOMMENDATIONS

Section 35: Power of the Central Government to exempt any agency of government from the application of the Act

Section 35 of the Bill empowers the Central Government to issue reasoned orders exempting any government agency from the application of any/all provisions of the Bill for reasons listed in the provisions.

Discussants agreed that blanket exemptions and lack of executive or judicial safeguards will fail to meet the standards laid out by the Supreme Court in the *K.S. Puttaswamy v. Union of India*[8] case, where it ruled that measures restricting the right to privacy must (1) be backed by law, (2) serve a legitimate aim, (3) be proportionate to the objective of the law, and (4) have procedural safeguards against abuse. Vague grounds that trigger exemptions, absence of procedure in granting exemptions, and the lack of independent oversight were highlighted as major concerns.

Participants pointed out that Section 42 of the PDP Bill 2018[9] had adopted the test laid out in *Puttaswamy* in creating exceptions. Additionally, exemptions were limited to Chapters II – VIII of the Bill, corresponding to data protection obligations, grounds for processing, children's data, rights of data principals, transparency/accountability measures, and cross-border transfers. Obligations related to fair and reasonable processing and implementation of security safeguards continued to apply, along with provisions relating to powers of the Data Protection Authority and Appellate Tribunal, among others.

The 2019 Bill is a step backward in comparison as it significantly expands the scope of exemptions while simultaneously diluting important safeguards. While national interests may in some cases override individual interest in privacy, it is critical, as the Justice Srikrishna Committee noted,[10] "to ensure that the pillars of the data protection framework are not shaken by a vague and nebulous national security exception".

Participants highlighted the following concerns for the JPC to consider:

1. Grounds for exemptions

Participants felt that terms like 'sovereignty', 'integrity', 'state security', 'international relations' and 'public order' are liable to be interpreted subjectively and sought clear parameters that would trigger exemptions. Earlier Private Members' Bills and other government reports on personal data protection may provide guidance. The Private Member's Bill introduced by Shri Baijayant Panda in 2017[11], for instance, lists five specific grounds under which the state may restrict the right to privacy. Similarly, the Intelligence Services (Powers and Regulation) Bill,[12] introduced by Shri Manish Tiwari in 2011, provided eight definitions to ascertain situations in which national security was under threat.

2. Scope of exemptions

Participants stressed that obligations like fair and reasonable processing and implementation of security safeguards should continue applying even to exempted government agencies. Additionally, participants felt that it would be inappropriate to strip the Data Protection Authority of its powers to prevent the misuse of personal data or to specify codes of good data protection practices. Exemptions in the national interest should, therefore, not extend to the entirety of the PDP Bill and must be limited to specified portions, as was the case in the PDP Bill, 2018.

3. Principles of legality, necessity, and proportionality

Participants argued that the "necessary and expedient" standard in the current Bill conflicts with well-established legal principles for administrative action and the Supreme Court's verdict in the *Puttaswamy* judgement. They agreed that exemptions must be granted under the authority of law as opposed to executive orders, and that the PDP Bill must specify that exempted processing must be necessary and proportionate vis-a-vis the objectives of the legislation. Section

42 of the PDP Bill, 2018, is a good point of reference as it already contains language that gives effect to these principles.

4. Procedural safeguards

Laying down a detailed procedural framework may be beyond the scope of Section 35, but it should specify what procedure will apply. The actual procedure could be framed under a separate legislation that oversees state exemptions. Alternatively, the procedure could be notified by the Data Protection Authority in exercise of its rule-making powers under Section 94 of the Bill. We would again like to draw the committee's attention to earlier Private Members' Bills and government reports that have laid out detailed procedural frameworks to oversee government access to information.

5. Independent oversight mechanism

Participants agreed that an independent oversight mechanism will lead to better accountability and national security outcomes. Such a mechanism should ideally be established within the amended Section 35 itself rather than be determined later by executive orders. The Srikrishna Committee report, for instance, recommended *ex ante* judicial review for government exceptions. Others also recommended that an investigations and oversight committee be set up within the Data Protection Authority. Beyond institutional mechanisms, participants also recommended regular public audits and the mandatory submission of annual reports to Parliament.

Section 91: Government Access to Anonymised and Non-personal Data

Section 91 of the PDP Bill enables the Central Government to direct data fiduciaries and data processors to grant access to all anonymised or non-personal data. This provision is predicated on the assumption that unfettered access to certain categories of data is essential for the targeted delivery of government services as well as other state functions such as "growth, security, integrity and prevention of misuse".[13]

Participants agreed that non-personal data is likely to serve a wide range of public functions. However, they felt that introducing such a provision in the present Bill was premature, given that the Ministry of Electronics and Information Technology has constituted an expert committee to establish a framework for the governance of non-personal data.

Participants argued that in the absence of complementary provisions and legislations in other fields, Section 91 in its current form is unlikely to serve the stated objective of supporting public service functions.

Participants highlighted the following concerns for the JPC to consider:

1. Grounds for government access to non-personal and/or anonymised data

Participants pointed to the need for clearer definitions or legislative standards for state functions that warrant access to non-personal and anonymised data. Most businesses store mixed data sets, which contain both personal and non-personal data, and afford these data sets differential protection depending on whether these were collected based on human input, statistical inferences, or other means. Participants stressed that a lack of shared taxonomy between state, business and civil society could undermine the ease of doing business, complicate data sharing efforts and undermine privacy rights.

2. Definitions and standards for anonymised data

Anonymised data defined under Section 3(2) is data that has undergone an "irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified". Participants overwhelmingly agreed that irreversible anonymisation is impossible— an assertion that is supported by the Justice Srikrishna Committee Report along with other government[14] and academic[15] research. They stressed that the Data Protection Authority must first prescribe standards for anonymisation and penalties for breach—ideally differential standards based on the type of data and level of risk—before enabling the state to access non-personal data.

3. Intellectual property and related business regimes

The definition of non-personal data as "all data that is not personal data" is likely to include trade secrets and the intellectual property of companies. Compelling businesses to share this data is likely to create legal risk and dampen incentives for innovation. Further, it could discourage foreign data fiduciaries from entering or continuing to operate in the Indian market, given the looming threat of state takeover of private knowledge assets. Participants also agreed that a broader framework for non-personal data would only be viable once its implications on Intellectual Property Rights regimes are settled.

4. Limitations on secondary use

Participants expressed concern over the lack of additional safeguards, rules or regulations related to secondary use, i.e., use for purposes other than what was envisaged at the time of collecting the data. Such secondary applications may well conflict with established data privacy standards, other constitutional rights, and business and economic rights. Absence of safeguards in this context may also affect adequacy findings by external regulators on the Indian data protection framework, which in turn may limit cross-border data transfers into India.

5. Ethical considerations

Participants noted that non-personal or anonymised data may contain biased inputs or inferences. Deploying these data sets for public functions risks exacerbating existing social, political and economic inequities. Participants suggested that data that has been acquired or licensed for public functions must undergo a social impact or ethics audit before being deployed towards fulfilling public policy objectives.

ANNEX: LIST OF PARTICIPANTS

1. Akshat Agarwal (Koan Advisory)
2. AlpanRaval (Wadhwani AI)
3. Amrita Choudhury (Cyber Cafe Association of India)
4. Arnab Kumar (NITI Aayog)
5. Ashutosh Chadha (Mastercard)
6. B.K. Syngal (Dua Consulting)
7. Baijayant Panda (Member of Parliament)
8. Basil Ajith (Software Freedom Law Centre, India)
9. Bhairav Acharya (Facebook)
10. Bhawna Sangwan (Amazon)
11. Debmalya Banerjee (Indian Chamber of Commerce)
12. Gajendra Upadhyay (Afilias)
13. Garima Rathore (Amazon)
14. Gokul Vijay (Cohen Group)
15. Gulshan Rai (Distinguished Fellow, ORF)
16. Jagdish Mitra (Tech Mahindra)
17. Jagjit Singh (Tata Consultancy Services)
18. Kumar Deep (Information Technology Industry Council)
19. Naman Aggarwal (Access Now)
20. Nikhil Pahwa (Medianama)
21. Rahul Sharma (The Perspective)
22. Shikha Thaman (American Express)
23. Smitha Prasad (Centre for Communication Governance)
24. Tripti Jain (Internet Democracy Project)
25. Venkatesh Krishnamoorthy (Business Software Alliance)

ENDNOTES

1. Draft of the Personal Data Protection Bill, 2019, as introduced in Lok Sabha, Parliament of India by Ministry of Electronics and Information Technology, Bill No. 373 of 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

2. Committee of Experts under Chairmanship of Justice B.N Srikrishna, “A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians”, Submitted to Ministry of Electronics and Information Technology, 2018, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

3. 2017 (10) SCC 1, https://indiankanoon.org/doc/91938676/

4. The President’s Review Group on Intelligence and Communications Technologies, “Liberty and Security in a Changing World: Report and Recommendations”, The White House Archives of President Barack Obama, December 12, 2013, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

5. Cahall, Bailey., Bergen, Peter., Sterman, David, and Schneider, Emily, “Do NSA’s Bulk Surveillance Programs Stop Terrorists?”, Policy Paper, New America, January 13, 2014, https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/

6. OECD (2019), “Enhancing Access to and Sharing of Data : Reconciling Risks and Benefits for Data Re-use across Societies”, https://www.oecd-ilibrary.org/sites/b4d546a9-en/index.html?itemId=/content/component/b4d546a9-en&mimeType=text/html

7. Staff Working Document, “Guidance on sharing Private Sector Data in the European Data Economy”, European Commission, April 25, 2018 https://ec.europa.eu/digital-single-market/en/news/staff-working-document-guidance-sharing-private-sector-data-european-data-economy

8. 2017 (10) SCC 1, https://indiankanoon.org/doc/91938676/

9. Draft of the Personal Data Protection Bill, 2018, Ministry of Electronics and Information Technology, https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

10. Committee of Experts under Chairmanship of Justice B.N Srikrishna, “A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians”, Submitted to Ministry of Electronics and Information Technology, 2018, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

11. Draft of the Data (Privacy and Protection Bill), 2017, Bill no 100 of 2017 as introduced in Lok Sabha, Parliament of India by Shri Baijayant Panda, Member of Parliament http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/889LS%20AS.pdf

12. Draft of the Intelligence Services (Powers and Regulations) Bill, 2011, Bill No, 23 of 2011 as introduced in Lok Sabha, Parliament of India by Shri Manish Tewari, Member of Parliament, http://164.100.24.219/BillsTexts/LSBill Texts/asintroduced/7185LS.pdf

13. Draft of the Personal Data Protection Bill, 2019, as introduced in Lok Sabha, Parliament of India by Ministry of Electronics and Information Technology, Bill No. 373 of 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

14. See for instance, "Opinion of Anonymisation Techniques" adopted by Data Protection Working Committee, European Commission,10 April, 2014 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

15. For instance see Rocher, L., Hendrickx, J.M. & de Montjoye, Y. "Estimating the Success of Re-identifications in Incomplete Datasets using Generative Models." Nat Commun 10, 3069, 23 July, 2019. https://doi.org/10.1038/s41467-019-10933-3, https://www.nature.com/articles/s41467-019-10933-3/

ORF 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