The Centre for Internet and Society's comments and recommendations on the

The Data Protection Bill, 2021

14 February 2022

By **Pallavi Bedi and Shweta Mohandas**

Review and Editing: Arindrajit Basu

Copyediting: The Clean Copy

The Centre for Internet and Society, India

After nearly two years of deliberations and a few changes in its composition, the Joint Parliamentary Committee (JPC), on 17 December 2021, submitted its report on the Personal Data Protection Bill, 2019 (2019 Bill). The report also contains a new version of the law titled the Data Protection Bill, 2021 (2021 Bill). Although there were no major revisions from the previous version other than the inclusion of all data under the ambit of the bill, some provisions were amended.

This document is a revised version of the comments we provided on the 2019 Bill on 20 February 2020, with updates based on the amendments in the 2021 Bill. Through this document we aim to shed light on the issues that we highlighted in our previous comments that have not yet been addressed, along with additional comments on sections that have become more relevant since the pandemic began. In several instances our previous comments have either not been addressed or only partially been addressed; in such instances, we reiterate them.

These general comments should be read in conjunction with our previous recommendations for the reader to get a comprehensive overview of what has changed from the previous version and what has remained the same. This document can also be read while referencing the new Data Protection Bill 2021 and the JPC's report to understand some of the significant provisions of the bill.

General Comments

1. Inclusion of non-personal data within the bill

One of the JPC's first recommendations is to change the name of the bill from 'Personal Data Protection' to 'Data Protection'. According to the committee, it is impossible to distinguish between what is personal and what is non-personal data and, therefore, it is important to have a single legislation dealing with both data sets. Non-personal data is defined under Clause 3 (28) as "data other than personal data", and non-personal data breach is given under Clause 3 (29) as "any unauthorised, including accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to non-personal data that compromises the confidentiality, integrity or availability of such data".

The JPC report recognises that real possibilities for the identification and subsequent profiling of individuals from non-personal and anonymised data exist. However, it does not seem to acknowledge the possibility of misuse by the state when it comes to the processing of non-personal data and re-identification of anonymised data sets.

On the contrary, both the 2019 Bill and the 2021 Bill provide exemption/unrestricted power and access to the central government to collect anonymised personal and non-personal data from different data fiduciaries for the digital economy. Clause 92 (1) of the bill states, "Nothing in this Act shall prevent the Central Government from framing (***) any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse,(***) and handling of non- personal data including anonymised personal data". At face value, it appears as if a carte blanche has been given to the central government to empower the different departments to frame policies which could contradict the provisions of the data protection law. Considering that the central government is the custodian of a large set of non-personal data across different sectors

such as health, transportation, and finance, it is concerning that such extensive power has been vested in them. Such clauses also go against the assertion in the JPC's report and the preamble of the 2021 Bill that data protection must be privileged over data economy interests.

We recommend that this provision be deleted and the scope of the 2021 Bill be limited to protecting personal data and providing a framework for the protection of individual privacy. Further, the central government should not be given a blanket exemption to access and monetise non-personal/anonymised personal data, nor should the 2021 Bill create a blanket provision allowing the central government to request such data from any data fiduciary that falls within the ambit of the bill. If the government wishes to use data resting with a data fiduciary, it must do so on a case-by-case basis and under formal and legal agreements with each data fiduciary.

2. Clause 35: Executive notification cannot repeal fundamental rights

We reiterate our earlier comments on Clause 35. Indeed, the sweeping powers and almost blanket exemption given to the central government to exempt any government agency from the ambit of the bill continue and are further cemented by the insertion of a non-obstante provision in Clause 35 which reads, "Notwithstanding anything contained in any law for the time being in force". The current version of the bill clarifies "such procedure" to mean "just, fair, reasonable and proportionate procedure". We appreciate the addition of this explanation, but we restate our comments on the 2019 bill: any restriction on the right to privacy would have to comply with the conditions prescribed in Puttaswamy I[1], i.e., (i) the restriction should be backed by law; (ii) have a legitimate state aim; and (iii) be necessary and proportionate. While the amendments to this clause reflect just, fair, reasonable, and proportionate procedure, it only applies to the procedure of processing of data by the government authority and not to the test of whether the reasons for exemptions are backed by the three-pronged test of necessity, legality, and proportionality prescribed in Puttaswamy I.

We also reiterate that the executive order issued by the central government authorising any agency of the government to process personal data does not satisfy the first requirement laid down by the Supreme Court in Puttaswamy I, as the above order will not have be a a law passed in Parliament. The Supreme Court while deciding on the validity of Aadhar in K.S. Puttaswamy v. Union of India[2] noted, "An executive notification does not satisfy the requirement of a valid law contemplated under Puttaswamy. A valid law in this case would mean a law passed by Parliament, which is just, fair and reasonable. Any encroachment upon the fundamental right cannot be sustained by an executive notification".

Several members of the JPC also highlight this issue in their dissenting notes to the JPC report. Jairam Ramesh, Manish Tiwari, and Gaurav Gogoi have criticised the wide range of exemptions given to the union government. Manish Tiwari recommended that the exemption be subject to a judicial determination. Jairam Ramesh also noted that any restriction on the fundamental right should (a) be backed by a law made in Parliament,

[1] Justice K.S. Puttaswamy (Retd) v. Union of India (2017 10 SCC 1.
[2] Justice K.S. Puttaswamy (Retd) v. Union of India (2019) 1 SCC 1 (2018).

(ii) should have a legitimate state aim; and (iii) be necessary and proportionate.

3. Further dilution of the powers of the data protection authority

An independent and robust data protection authority (DPA) is the hallmark of a strong data protection regime; unfortunately, in its various iterations, the bill has continued to dilute the independence and powers of the DPA. As per the 2019 Bill, the selection committee for the appointment of the members of the DPA would comprise entirely of the members of the executive, raising concern about the independence of such a selection body. Though the 2021 Bill appears to have addressed this concern in a limited manner, by including the attorney general and an independent expert on the selection committee, the underlying concern regarding the independence of the DPA still remains. It still does not provide for any representation from any member of civil society.

The 2018 bill had expressly stated that the salaries, allowances, and other terms and conditions of service of the chairperson and members of the DPA would not be varied to their disadvantage during their term. This provision was deleted in the 2019 Bill and remains so in the 2021 Bill. This gives the central government the power to reduce salaries or amend the terms of appointment to the detriment of DPA members.

Further, in the 2019 Bill, the DPA was bound by the orders of the central government on "questions of policy", with the central government having the power to decide whether a question is one of policy or not. Unfortunately, under the 2021 Bill the powers of the DPA have been further diluted. Under Clause 87 (2), the DPA is bound by the directions of the central government **on all matters**, not just questions of policy. Considering the wide exemption given to the central government to bypass privacy and data protection mechanisms, the further dilution of the DPA's authority is worrying.

In order to govern data protection effectively, a responsive market regulator with a strong mandate, ability to act swiftly, and resources are necessary. The political nature of personal and non-personal data also requires that the governance of data – particularly the rule-making and adjudicatory functions of the DPA – is independent of the executive.

4. No clarity on data sandboxes

The bill contemplates a sandbox for "innovation in artificial intelligence, machine-learning or any other emerging technology in public interest". A data sandbox is a non-operational environment where the analyst can model and manipulate data inside the data management system. Data sandboxes are envisioned as a secure area where only a copy of the company's or participant companies' data is located.[3] In essence, it is a scalable and creation platform which can be used to explore an enterprise's information sets. Regulatory sandboxes are controlled environments in which firms can introduce innovations to a limited customer base within a relaxed regulatory framework, after which they may be allowed entry into the larger market on meeting certain conditions. This purportedly encourages innovation by lowering entry barriers and protecting newer

[3] Keith Laker, "DBAs Guide to Sandboxes vs. Data Marts", *The Data Warehouse Insider*, 16 May 2014,https://blogs.oracle.com/datawarehousing/post/dbas-guide-to-sandboxes-vs-data-marts#:~:text=A%20%22sandbox%22%20is%20generally%20meant,on%20the%20core%20operational%20processes.

entrants from unnecessary and burdensome regulation. Regulatory sandboxes can be interpreted as a form of responsive regulation by governments that seek to encourage innovation – they allow selected companies to experiment with solutions within an environment relatively free of most cumbersome regulations that they would ordinarily be subjected to, while still including some appropriate safeguards and regulatory requirements.

In the 2021 Bill, the relaxing of data protection provisions for data fiduciaries could lead to restrictions on the privacy of individuals. The 2021 Bill replaces the mandatory sounding "shall" with "may" to make the creation of a sandbox more of a suggestion. As sectoral sandboxes have already been or are being established while the 2021 Bill is still in the discussion stage, there needs to be some clarity on how the sandboxes will work within different regulatory regimes. For example the Reserve Bank of India (RBI) has established a sandbox for the banking sector. But if a sandbox for the fintech space is created under the 2021 Bill there is the possibility for confusion over which data protection and regulatory practices the companies should follow.[4]

5. The definition of 'harm' in the bill ought to be reconsidered

A harms-based approach is necessary for data protection frameworks. However, such approaches should be restricted to the positive obligations, penal provisions, and responsive regulation of the DPA. While the 2021 Bill expands the categories of harm and includes a provision for more harms to be added later, it still fails to offer any guidance on the interpretation of 'harm',[5] 'or the various activities covered within the definition of the term harm. Phrases such as "loss of reputation or humiliation" "any discriminatory treatment" are a subjective standard and are open to varied interpretations. The expansion of the definition to include "psychological manipulation which impairs the autonomy of the individual" creates further concern about how such an instance will be proved and how it would play out in a case of data protection. The ambiguity in the definition and provisions will make it difficult for the data principal to demonstrate harm. Moreover, for the data fiduciary, too, these provisions can prompt a lack of confidence and a fear of penalties as a result of inadvertently causing harm. Even for the DPA, the current definitions make taking necessary action a challenge, as several provisions are based on harm being caused or likely to be caused. This is troubling as the bill envisions a tiered approach to harms, distinguishing between 'harm' and 'significant harm'.

Some significant provisions where 'harm' is a precondition for the provision to come into effect are

---

[4] RBI, "Reserve Bank Announces the Opening of First Cohort under the Regulatory Sandbox", *Reserve Bank of India*, 4 November 2019, https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=48550.

[5] Clause 3 (23): "'Harm' includes (i) bodily or mental injury; (ii) loss, distortion or theft of identity; (ii) financial loss or loss of property; (iv) loss of reputation or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of service, benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; (x) any observation or surveillance that is not reasonably expected by the data principal; (xi) psychological manipulation which impairs the autonomy of the individual; or (xii) such other harm as may be prescribed."

i. **Clause 32 (2)**: A data principal can file a complaint with the data fiduciary for a contravention of any of the provisions of the act, **which has caused or is likely to cause 'harm'** to the data principal.
ii. **Clause 64 (1)**: A data principal who **has suffered harm** as a result of any violation of the provision of the act by a data fiduciary has the right to seek compensation from the data fiduciary.
iii. **Clause 16 (3)**: The manner to be adopted by the data fiduciary to verify the age of the child has to take into consideration among other factors the possibility of harm to child arising out of processing of personal data.

6. Steps towards greater decentralisation of power

The JPC report and the 2021 Bill recommend one legislation for both personal and non-personal data, and that one DPA handle both personal and non-personal data. Therefore, we reiterate our previous comments about greater decentralisation of power and devolved jurisdiction:

i. **Creation of state DPAs**: A single centralised body may not be the most appropriate form of such a regulator. We propose that along the lines of central and state commissions under the Right to Information Act, 2005, state DPAs are set up. These state DPAs will be in the position to respond to local complaints and to exercise jurisdiction over entities within their territorial jurisdictions. The data fiduciary should, along with the grievance redressal mechanism and the right of the data principal to file a complaint, also specify the jurisdiction of the DPA before which a complaint can be filed by the data principal.
ii. **More involvement of industry bodies and civil society actors**: In order to lessen the burden on DPAs, active engagement of the DPAs with industry bodies, sectoral regulators, and civil society bodies conducting privacy research is necessary. Currently, the bill provides for the involvement of industry or trade associations, associations representing the interests of data principals, sectoral regulators or statutory authorities, and any departments or ministries of the central or state government in the formulation of codes of practice. However, it would also be useful to have more participation of industry associations and civil society bodies in activities such as promoting awareness among data fiduciaries about their obligations under this act, encouraging measures for proactive data protection, and undertaking research for innovation in the field of protection of personal data.

7. The DPA must be empowered to exercise responsive regulation

In India, the challenge is to rapidly move from having few or no data protection laws, and consequently abysmal data privacy practices, to having strong data protection regulations and a powerful regulator capable of enabling robust data privacy practices. This requires supportive mechanisms for stakeholders in the data ecosystem and systemic measures that enable the proactive detection of breaches. Further, keeping in mind the limited regulatory capacity in India, there is a need for the DPA to make use of

different kinds of inexpensive and innovative strategies. This could follow the sliding scale proposed by Ian Ayres and John Braithwaite[6]. As per the enforcement pyramid they propose, the regulatory mechanism should have a dynamic and gradual sanctioning regime. The scale they envisage starters predominantly with cooperation and persuasion, followed by progressively tougher sanctions depending upon the seriousness of the non-compliance and the responsiveness of the offender.

We reiterate some recommendations, emphasising that the following additional powers for the DPA be clearly spelt out:

i. **Informal guidance**: It would be useful for the DPA to set up a mechanism along the lines of the Security and Exchange Board of India (SEBI) Informal Guidance Scheme, which enables regulated entities to approach the authority for non-binding advice on the law. Given that this is the first omnibus data protection law in India, and there is very little existing jurisprudence on the subject from India, it would be extremely useful for regulated entities to guidance from the regulator.

iii. **Power to name and shame**: When a DPA publicises the names of organisations that have seriously contravened the data protection legislation, it is known as 'naming and shaming'. The UK Information Commissioner Office (ICO) and other DPAs recognise the power of publicity, as evidenced by such organisation's willingness to cooperate with the media. The ICO does not simply post monetary penalty notices on its websites for journalists to find, but frequently issues press releases, briefs journalists, and uses social media. **Undertakings**: The UK ICO has leverages the threat of fines into an alternative enforcement mechanism, seeking contractual undertakings from data controllers to take certain remedial steps. Undertakings have significant advantages for the regulator. Since an undertaking is a 'cooperative' solution, it is less likely that a data controller will challenge it. An undertaking is simpler and easier to put in place than legal proceedings, which usually take longer.\

8. Children's data and privacy

The age at which a person has the ability to legally consent in the online world is intertwined with the age of consent under the Indian Contract Act, i.e., 18 years. The bill makes no distinction between a 5-year-old and a 17-year-old. Thus, it assumes the same level of maturity for all persons under the age of 18. It is pertinent to note that the law in the offline world does recognise a distinction and acknowledges changes in maturity level. For example, under the Juvenile Justice Act and the Indian Penal Code, any act by a child under the age of 12 will not be considered as an offence as the law recognise that children under the age of 12 do not have the maturity to determine the consequences of their actions. While the consequences of the actions of children between the age of 12–18 will be determined by the court (individuals aged 16–18 years can also be tried as adults for heinous crimes). Similarly, child labour laws in the country allow children above the age of 14 years to work in non-hazardous industry jobs.

[6] Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford Socio-Legal Studies 1992), 2.

Additionally, the categorisation of all individuals under the age of 18 as children fails to acknowledge how teenagers and young adults use the internet. This is especially important when looking at the 2019 data, which suggests that those in the 12–19 age group account for about 21.5% of the total internet usage in metro cities. Given that the pandemic has compelled students and schools to adapt to virtual schools, a reliance on the internet has become ubiquitous with education. As per the Annual Status on Education Report (ASER) 2020, more than 33% of all schoolchildren are pursuing digital education, either through online classes or recorded videos.[7]

Instead of setting a blanket age for determining valid consent, we should look at alternative means to determine the appropriate age for children at different levels of maturity, similar to what the UK Information Commissioner's Office developed. The Age Appropriate Code 2021 prescribes 15 standards that online services need to follow. It broadly applies to online services "provided for remuneration"[8] – including those supported by online advertising – that process the personal data of and are "likely to be accessed" by children under 18 years of age, even if those services do not explicitly target children. This includes apps, search engines, social media platforms, online games and marketplaces, news or educational websites, content streaming services, and online messaging services.

The reservations to keeping 18 as the age of majority under the 2021 Bill has also been expressed by some members of the JPC through their dissenting opinion. Ritesh Pandey noted that keeping in mind the best interests of children, the bill should consider a child as a person who is younger than 14 years of age.[9] Similarly, in his dissenting note, Manish Tiwari observes that the regulation on processing children's data should be based on the type of "content or data".[10]

The JPC report observes that the bill does not require the data fiduciary to obtain fresh consent of a child once the child has turned 18. It also does not give the child the option to withdraw their consent upon reaching the majority age. It therefore makes the following recommendations:

i. Registration of data fiduciaries, exclusively dealing with children's data.
ii. Application of the Majority Act, 1875 to a contract with a child.
iii. Obligation of a data fiduciary to inform a child to provide their consent three months before the child attains majority age.
iv. Continuation of the services until the child opts out or gives fresh consent upon achieving majority.

[7] "Annual Status of Education Report (Rural) Wave 1",ASER Centre, 01 February 2021 https://img.asercentre.org/docs/ASER%202021/ASER%202020%20wave%201%20-%20v2/aser2020wave1report_feb1.pdf.

[8] The code applies to "information society services likely to be accessed by children". The definition of an ISS is "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."; available at https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/#code2

[9] "Dissent is democratic: Looking at the dissent notes in the report of the JPC, *Internet Freedom Foundation*, accessed 11 February 2022, https://internetfreedom.in/pdpb-jpc-report-dissent-notes/

[10] "Dissent is democratic", Internet Freedom Foundation

These recommendations have not been incorporated into the provisions of the bill.

9. No clear roadmap for the implementation of the bill

Unlike the 2018 bill, the 2019 Bill did not specify or provide any timelines for its implementation. The 2019 bill therefore recommended that all the provisions of the bill should be implemented within 24 months of its enactment. It provided for phased implementation in the following manner:

Time period	**Phase to be implemented**
Within 3 months	Chairperson and DPA members appointed
Within 6 months	DPA commences its activities
Within 9 months	Registration of data fiduciaries begins
Within 12 months	Adjudicators and appellate tribunal start work
Within 24 months	All provisions of the bill deemed effective

Though the JPC provides a timeline for the implementation of the bill, this plan has not been incorporated into the provisions of the 2021 bill. Indeed, the revised bill does not have a clause that specifies hese timelines.

We recommend that the bill clearly specify a timeline for the implementation of the different provisions of the bill, and especially a time frame for the establishment of the DPA. This is vital to ensure that individuals have an effective mechanism through which to enforce the right and to seek recourse in case the data fiduciaries breach any obligations.

All the three versions of the bill and the JPC report are silent on time periods for the enforcement of punishments. Here, we reiterate our earlier comments. For offences, we suggest a system where provisions and punishments are enforced in a staggered manner, for a period till the fiduciaries align with the provisions of the act. The DPA must ensure that data principals and fiduciaries are sufficiently aware of the provisions of the bill before applying the provisions for punishment. This will allow the data fiduciaries to align their practices with the provisions of the new legislation and give the DPA time to define and determine certain provisions that the bill leaves for the DPA to define. Additionally, enforcing penalties for offences must initially be staggered and combined with warnings in order to prevent first-time and mistaken offenders from paying high prices. This may relieve the concerns of smaller companies and startups that avoid processing data for fear of paying penalties for related offences.

10. Legal uncertainty

In its current structure, there are a number of provisions in the bill that, when implemented, run the risk of creating an environment of legal uncertainty. These include; (i) the lack of definition of critical data'; (ii) lack of clarity in the definition of 'harm' ; (iii)

ability of the government to define further categories of sensitive personal data; (iv), framing of the requirements for data transfers; and (v) bar on processing certain forms of biometric data as defined by the central government. To ensure the greatest amount of protection of individual privacy rights and the protection of personal data while also enabling innovation, it is important that any data protection framework is structured and drafted in a way to provide legal certainty

11. Expand the list of offences

Clause 83 (1) restricts offences to the re-identification and processing of personal data. Considering the personal data health breaches during the pandemic (In January 2021, a website published a story[11] on how the Covid-19 test results of patients in Delhi were disclosed on the internet), the list of offences should be expanded to include intentionally or recklessly obtaining, transferring, or selling either personal or sensitive personal data by both the state or private entities"; this was prescribed by the Srikrishna Committee. The 2019 Bill as well as the 2021 Bill do not include unauthorised disclosure of personal data as an offence. Further, there is no penalty for the breach of health data specifically and unlike the Digital Information in Security Healthcare Bill Act (DISHA)[12], the 2021 Bill does not specify that the owner of the breached health data has to mandatorily be informed about the breach.

[11]"Data, Privacy, Pandemic: India just had the Biggest Medical Records Breach Ever", *ORF Foundation*, accessed 11 February 2022,https://www.orfonline.org/expert-speak/data-privacy-pandemic-india-just-had-the-biggest-medical-records-breach-ever/

[12] Digital Information Security in Healthcare Act, 2017.