

## Children's Data Protection

*The Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill, 2019 (PDP Bill)<sup>1</sup> submitted its report to the Parliament, containing the revised Draft Data Protection Bill, 2021.<sup>2</sup> The report suggests a few changes in provisions relating to protecting children's data and ensuring their online safety. This Briefing Paper discusses those changes. However, it misses out on addressing many lacunas, as highlighted by different stakeholders. These issues have been discussed subsequently, and corresponding recommendations are given.*

### JPC Recommendations

#### **Data Fiduciaries to Register with the DPA**

Such a provision,<sup>3</sup> may have an unintended adverse impact on start-ups & digital Medium Small and Micro Enterprises (MSMEs), particularly those engaged in providing children facing services such as edu-tech, digital libraries, entertainment etc., due to the increased compliance burden of registering themselves with the proposed Data Protection Authority (DPA). This may hamper innovation and disincentivise smaller players to invest in and provide such services.

Accordingly, it is suggested that an appropriate threshold should be set after inclusive stakeholder consultation, for classifying data fiduciaries (service providers) that possess the necessary wherewithal to register themselves with the DPA, i.e., a blanket requirement for all service providers to register themselves should not be set.

#### **Removal of Concept of Guardian Data Fiduciary**

All data fiduciaries that operate commercial websites or online services directed at children were classified as '*guardian data fiduciary*' under clause 16(4) of the PDP Bill. These data fiduciaries were to be barred 'from profiling, tracking or behavioural monitoring of, or targeted advertising directed at, children.' Stating that the concept is likely to affect the law's implementation, the JPC report has suggested scrapping the concept in its totality.

In effect, this recommendation,<sup>4</sup> bars all data fiduciaries from profiling, tracking or behaviourally monitoring of, or targeted advertising directed at, children. This may become problematic for smaller data fiduciaries, especially those not providing services to children, as they may need to spend resources on segregating the personal data collected by them and process children's data separately, which may not be a significant part of their collected data. The adverse impact on children has been discussed in subsequent sections. Furthermore, the concept of guardian data fiduciary has mostly been included in the classification of significant data fiduciary.<sup>5</sup>

Significant data fiduciaries may need to comply with additional regulations, such as: undertaking data protection impact assessments in certain circumstances, maintenance of records, an annual audit by an independent data auditor, appointing a data protection officer, among others. Including data fiduciaries dealing with children's data under this category may have an unintended adverse impact on start-ups & MSMEs providing services to children due to increased compliance burden. Accordingly, there is merit in revisiting such removal of the concept of guardian data fiduciaries and delineating it from the concept of significant data fiduciary. Further, the data fiduciaries can be encouraged to adopt privacy by design principles with practices like purpose limitation and data minimisation.

**Three months before a child attains the age of majority, the data fiduciary has to inform the child for providing consent again on the date of reaching the age of majority.**

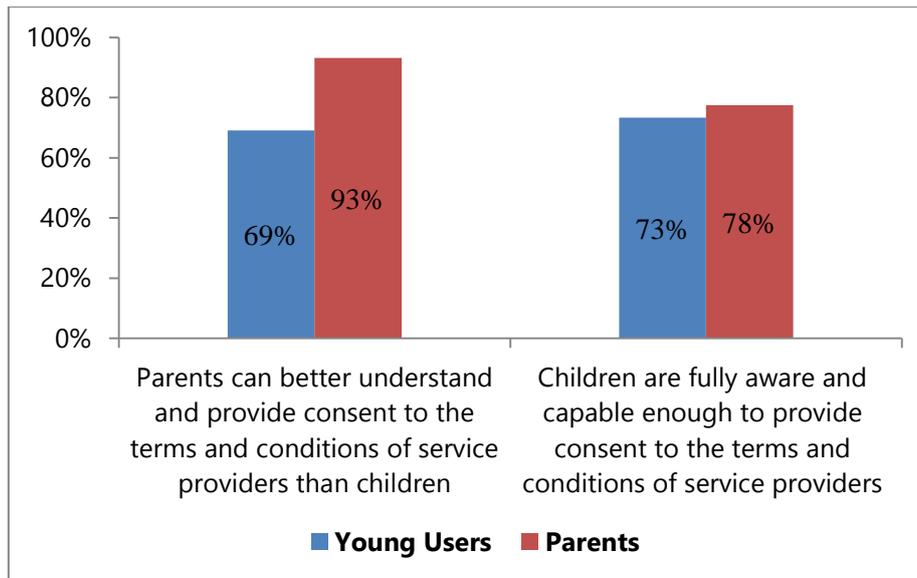
A recent pan-India survey conducted by CUTS on the subject<sup>6</sup>, showed that most children are unaware of the data protection measures undertaken by service providers and do not tend to read the terms of conditions of service providers before providing consent to the same. Accordingly, such a provision,<sup>7</sup> Although well-intentioned can only have the desired impact if the government and service providers undertake awareness generation and capacity building initiatives, in partnership with child rights and consumer groups, to ensure that the child is able to provide informed consent, at the time of attaining majority.

## Pending Issues of Concern

### Age Threshold for Parental Consent at 18 Years

The PDP Bill had defined anyone below 18 years as a child under clause 3(8). Processing of personal data of a child required parental consent under the clause 16(2) of the PDP Bill. While many children may be capable of providing consent to data fiduciaries for processing of their personal data, the PDP Bill had taken a one-size fits all approach and equated the maturity level of children (below 13 years of age), adolescents (13 to 15 years of age) and young users (16 and 17 years of age). Notably, as has been acknowledged by the JPC report, other jurisdictions like the US and the UK have adopted lower age thresholds. Moreover, it does not take into account the vast cultural differences which prevail across the country.

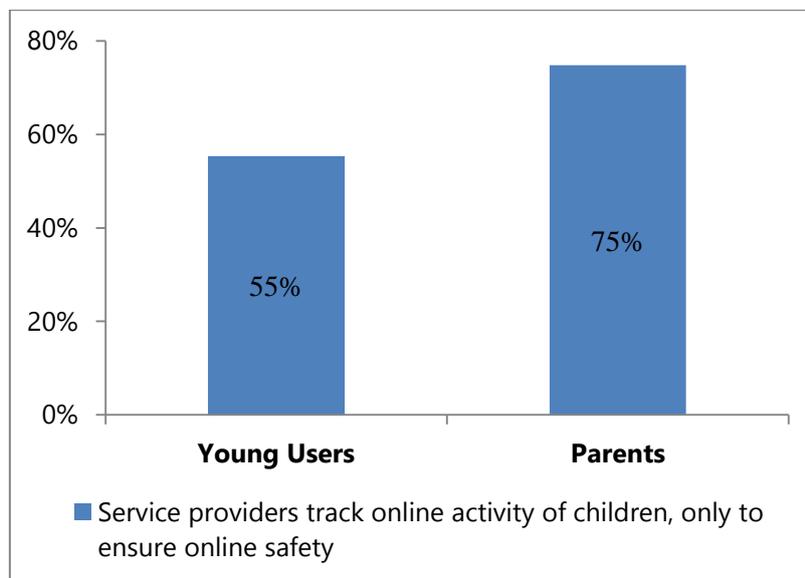
The CUTS study finds that children have already been operating internet-enabled devices for 14 years without parental guidance. The study also finds that over 75 percent of parents believe that their child knows more than them about practices to adopt for a safe online experience. It can provide consent to the terms & conditions of service providers, a claim seconded by around 73 percent of young users.



Furthermore, few JPC members have filed their dissent notes on the issue. Mr Ritesh Pandey<sup>8</sup> suggested classifying users under the age of 14 years as children. Mr Manish Tewari<sup>9</sup> opined that a child's definition could be different for different services where some child-friendly services may be exempt from requiring parental consent. Accordingly, there is merit in revisiting the age fixed for classifying children, and inclusive stakeholder consultation may be required.

### **Barring Behavioural Tracking of Children**

As discussed previously, the JPC recommends that all data fiduciaries be barred from profiling, tracking, or behaviourally monitoring of, or targeted advertising directed at, children. Such a blanket ban will impact the ability of data fiduciaries to protect children from online harm.



CUTS study finds that over 75 percent of parents and 55 percent of young users are comfortable with data fiduciaries tracking and monitoring the online behaviour of young users, but only for the valid objective of ensuring their online safety.

Accordingly, it may be counter-productive to completely prohibit online tracking, since it may hinder child safety measures being implemented by data fiduciaries. Adequate safeguards with respect to purpose limitation and data minimisation may be mandated instead, for ensuring that children's online activity is only monitored for valid objectives.

### Requirement of Age Verification

CUTS study has found that many young users encounter different types of problematic experiences online, such as cyber-bullying/ stalking, exposure to other kinds of problematic content etc. Further, most young users claim to be aware of various tools & strategies to overcome problematic experiences, and however, many do not implement them. Accordingly, the government and data fiduciaries must work with child rights and consumer groups to raise awareness and build the capacity of children on online safety.

Also, to protect children and young users from online harm, data fiduciaries need to verify the age of users. In this regard, the JPC report recommends that the DPA frame codes of practice for age verification. As found out in the CUTS study, both parents and young users prefer the least privacy intrusive mechanisms for age verification, through technology, instead of linking government-issued ID cards. Global technological developments in this regard have been compared on various consumer-facing parameters, such as availability, ease of use, scalability, etc., in a CUTS Briefing Paper.<sup>10</sup> Accordingly, it is recommended that the DPA may frame codes of practice for age verification keeping these in mind.

## Endnotes

- <sup>1</sup> The Personal Data Protection Bill 2019, available at [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf)
- <sup>2</sup> Report of the Joint Committee on the Personal Data Protection Bill, 2019 [http://164.100.47.193/lssccommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17\\_Joint\\_Committee\\_on\\_the\\_Personal\\_Data\\_Protection\\_Bill\\_2019\\_1.pdf](http://164.100.47.193/lssccommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf)
- <sup>3</sup> Recommendation 5, JPC Report, on Page No. 30. has been covered in 26(2).
- <sup>4</sup> Recommendation 38, JPC Report, Page No. 73. Changes to be made in clauses 16(4) & 16(7) of the Bill.
- <sup>5</sup> Recommendation 47, JPC Report, Page No. 97. Changes to be made in clause 26(1) of the Bill.
- <sup>6</sup> Highlighting Inclusive and Practical Mechanisms to Protect Children's Data, details available at: <https://cuts-ccier.org/highlighting-inclusive-and-practical-mechanisms-to-protect-childrens-data/>
- <sup>7</sup> Recommendation 5, JPC Report, Page No. 31. To be covered through rules/ regulations under the Bill.
- <sup>8</sup> Ritesh Pandey's Dissent Note in the JPC Report on the PDP Bill, 2019.
- <sup>9</sup> Manish Tewari's Dissent Note in the JPC Report on the PDP Bill, 2019.
- <sup>10</sup> CUTS Briefing Paper 'Global Technological Developments in Age Verification and Age Estimation', available at: <https://cuts-ccier.org/pdf/bp-global-technological-developments-in-age-verification-and-age-estimation.pdf>

This Briefing Paper is authored by Prince Gupta, CUTS International and prepared as a part of the project 'Highlighting Inclusive and Practical Mechanisms to Protect Children's Data.'

© CUTS International 2021. This Briefing Paper is published by CUTS Centre for Competition, Investment & Economic Regulation (CUTS CCIER), D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India. Ph: +91.141.228 2821, Fx: +91.141.228 2485, E-mail: c-cier@cuts.org, Web: [www.cuts-ccier.org](http://www.cuts-ccier.org).  
Also at Delhi, Calcutta and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland); and Washington DC (USA).