REPORT OF THE ONLINE DISCUSSION "DATA PROTECTION BILL 2021: DECIPHERING THE PRIVACY & RIGHTS OF MINORS"

Introduction

After nearly two years, the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill, 2019 (PDPB'19), presented its report to the Parliament, in December 2021. The report also entails a revised draft of the PDPB'19, now called "The Data Protection Bill, 2021" (DPB 2021). The report is available here.

Minors account for nearly 39% of India's population and constitute the most active internet user base of the country. Due to the pandemic, there has been a massive acceleration of children online and the trend is expected to continue. However, there are growing concerns related to the security and privacy of minors online as they are vulnerable.

The DPB 2021 has several provisions to protect the privacy of minors. Looking at the importance of protecting the privacy of minors, CCAOI, Consumer Unity & Trust Society (CUTS) and Internet Society Delhi Chapter (ISOC Delhi) organised an online discussion 'Data Protection Bill 2021: Deciphering the Privacy & Rights of Minors', on 18 January 2022.

The objective of the discussion was to discuss the provisions related to processing of data related to minors, identify areas that need to be refined and then deliberate on what constructive regulations/ codes of practice should look like for minors' privacy.

Moderated by Ms **Amrita Choudhury**, CCAOI, the keynote speakers were Hon'ble Members of Parliament (MPs), Mr **Manish Tewari**, MP Lok Sabha and Dr **Amar Patnaik**, MP Rajya Sabha, who are also members of the JPC on PDPB'19. Other speakers were Ms **Aparajita Bharti**, Young Leaders for Active Citizenship, Ms **Sreenidhi Srinivasan**, Ikigai Law, Ms **Uthara Ganesh**, Snapchat; Mr **Nikhil Pahwa**, MediaNama, Mr **S. Chandrasekhar**, K&S Partners; and Mr **Amol Kulkarni**, CUTS who shared their perspectives on various provisions related to privacy of minors. Mr **Sidharth Narayan**, CUTS, presented the perspective of minors and parents on select provisions of the bill, based on the findings from a pan-India survey. The presentation is available here, while the complete findings are available here.

The session was attended by over 120 participants on Zoom and 60 people in live stream, belonging to different stakeholder groups from across the country. The recording can be viewed using this link.

Important Provisions with respect to Minors in the DPB 2021

- Anyone below 18 years is defined as a child in the bill (Clause 3.8)
- Mandates data fiduciaries to obtain parental consent (Clause16.2)
- All data fiduciary barred from profiling and or tracking children (Clause 16.4)
- Government to come up with rules to get individuals consent when they turn 18 years to withdraw their consent within 3 months.

Summary of Discussions:

Children are a vulnerable section of the society. There is a need to protect the data of children by adopting a nuanced approach that protects both, the privacy and rights of children.

Since children require special attention, there needs to be a separate public discussion and legislation on ensuring a safe online experience for them, rather than superficially touching upon the issue within the DPB 2021.

The age of consent and complexity related to it, the issue of age verification and how there may be some tensions with broader objectives of data protection were highlighted by most speakers.

The key issues discussed by the speakers are given below.

Age of minor

A need to adopt a graded approach in defining the age of a minor was emphasised unanimously.

Tewari cautioned against adopting a one size fits all approach in specifying the age of a child. Patnaik highlighted the need to account for the diverse geographical and cultural differences prevailing across the country, for fixing the age threshold for classifying children.

Srinivasan substantiated the claim of reducing the age of minors by referring to the age of child in other jurisdictions citing the United States of America's (US) Children's Online Privacy Protection Act (COPPA) where it is 13 years and the European Union's (EU) General Data Protection Regulation (GDPR) where it is 13-16 years.

Pahwa suggested adopting a graded approach between people below 13 and above 13 as independence and maturity increase with age, while Chandrashekhar opined the age of consent should be around 15 years. Narayan pointed out that the CUTS survey revealed that both parents and young users believe that children start using online services independently from the age of around 14 years.

Age verification or Age gating

The challenges of age verification were highlighted.

Reference was made to the complexity in age verification citing UK ICO opinion (Ganesh) and CNIL in France (Choudhury). Ganesh added that this may be the reason for government across the world not rushing for age verification requirements.

Kulkarni suggested adopting innovative age verification process through technology, and cautioned against focusing on ID based verification, given that it may infringe privacy of users. He highlighted CUTS briefing paper titled 'Global Technological Developments in Age Verification and Age Estimation' (available here), which compares different technology driven age verification mechanisms on various consumer facing parameters like ease of use, privacy, scalability etc.

The fiction between the age verification requirement with certain other provisions specifically data minimisation requirements or provision of Clause 16.4 that prevents profiling, tracking behavioural monitoring was pointed by Ganesh. She added that this provision has tensions with the requirement of age verification in Clause16.2 as you need to process the data of children for age assurance. She opined that there may be similar tensions with data minimisation requirement.

Parental Consent

Challenges and issues related to parental consent were highlighted by all speakers, including lack of understanding of many parents of internet and digital technology.

While there should be no harmful processing of children's data, however there is a need for young adults to have more autonomy over processing of their data, opined Ganesh. Bharti cautioned that since girls face more scrutiny with parents wanting to be extra careful with girls, they may deny them access to many things online.

Tewari cautioned against mandating parental consent and suggested having a differential approach wherein the threshold for requiring parental consent of processing children's data be different for different categories of content and services.

Narayan shared that CUTS' research reveals that many parents believe their children know more than them about practises to adopt for a safe online experience, and consider children to be capable to provide consent to the terms and conditions of services providers. Further, most young users do not want their parents to monitor all their online activity.

Contrasting the requirement of parental consent with other frameworks, Srinivasan shared that while the Indian law extends requirement to organisations that interact with all, the COPPA extends to websites or 'online services' directed at children and the GDPR to 'Information society services' - online service directed at children.

Ganesh added that parental consent may discourage many businesses from providing beneficial contents and services to children owing to the complexity of creating an obligation of parental consent. She added that there may be some challenges in creating the parental consent flow. For example, many parents are not online and are not using online platforms. In such cases, parental consent will have to be taken off the platform, such as through email which could be a mechanism to get the consent. Such interventions will be manual processes requiring reengineering of resources so that consent flow can be built.

Tracking and Profiling

While there is a need to restrict tracking and profiling that causes significant harm to children a complete ban may not be in the best interest of a child.

Srinivasan pointed that a blanket ban could restrict beneficial profiling such as predictive profiling for ensuring precautionary measures for children. She added that in terms of profiling, monitoring etc., COPPA allows profiling and tracking with parental consent (though there are restrictions in other laws) and the GDPR has a provision to conduct impact assessment.

Chandrashekar pointed that while a lot of the emphasis is being given to impact of age gating with respect to social media, children's data is collected and processed by

various other entities such as schools, edutech companies etc. with parental consent, which is being overlooked. He stressed on the need to know what kind of cookies are collecting children's data when they are online,. Tracking becomes an issue only when it may lead to children being pushed towards undesirable content..

Pahwa expressed that not all tracking is bad and a blanket prohibition of tracking children's online activities by service providers may do more harm than good. He cited the example of the use of artificial intelligence in education which is based on behavioural tracking and monitoring the performance of the child. Narayan also highlighted that the CUTS study reveals that young users and parents are generally comfortable in behavioural tracking of children, but only for the valid purposes of ensuring their online safety.

From a business perspective, Ganesh and Chandrashekhar brought forth the importance of platforms adopting the principle of privacy by design through practices like data minimisation, purpose limitation, among others, which will help in ensuring the privacy of children online.

Bharti added that since data fiduciaries are different in nature, it is important for each platform to look at what privacy by design looks like in their platform.

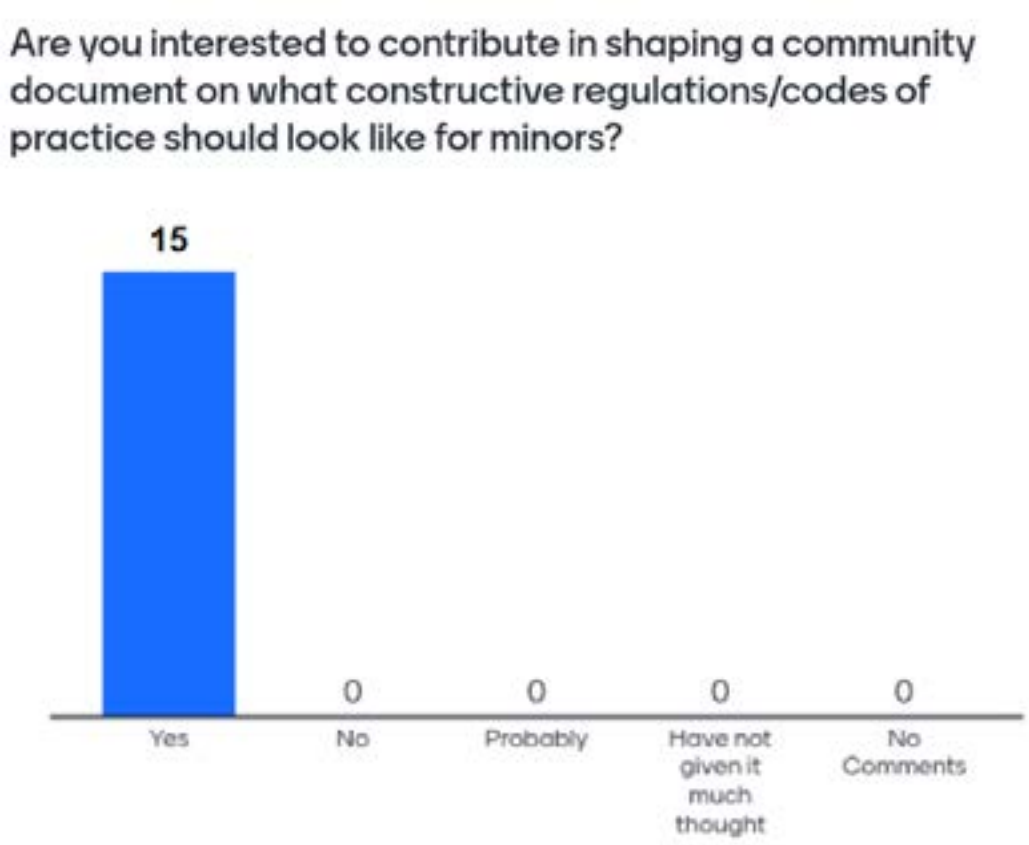
In terms of harms, it is important to determine whether platform is monetising processing of data or monetising data itself. Where platform is monetising processing of data, a little bit of nuanced approach is required, suggested Chandrashekar. He further suggested the need for consultation to list what platforms cannot do and once there is an accepted list, the platforms should accordingly abide by it.

Other Points discussed

- Caution was expressed that any new regulation should not cause friction for a child to access the internet.
- While Patnaik supported taking out the concept of "best interests" of child which was mentioned in the PDPB'19, Bharti shared that the term "best interest" is a globally accepted terminology in many frameworks like the UN standard on what "best interest" means and the UK age-appropriate design code which defines "best interest". There is a need to delve a bit more on best interest of child and rights of child, she opined.
- Reference was made to few good practices that are being adopted for ensuring children's online safety, such as content moderation, as well as age verification of users using technology, in a least privacy intrusive manner by Ganesh and Chandrashekhar.
- The importance of engaging with credible civil society organisations and consumer groups, to create awareness and build capacity of children to safely navigate the online world was emphasised by Kulkarni.
- Kulkarni and Bharti stressed on importance to involve young adults in regulation-making on issues impacting them.

- A risk-based codes of practice or approach should be adopted, suggested Srinivasan.
- Issue related to cost of compliance burden, especially for startups was emphasised by Tewari.
- Competing interests in the provisions was pointed out by Srinivasan, such as: creating safe spaces for children vis a vis giving them more autonomy; data minimisation vs collecting more data for age verification.
- Patnaik questioned the rationale of not including children's data stored in a non-digitized form, by schools and colleges, under the ambit of the DPB 2021.
- Child Sexual Abuse Material (CSAM) and all issues related to child need to be taken separately, suggested Pahwa.
- Pahwa expressed concern that a lack of nuanced approach and technical understanding will disfranchise children and young adults from the benefits which the internet provides.
- Need for separate legislation or code for how children's data is collected, managed and processed was emphasised by Bharti.
- If there are any changes being made in the rules, it has to be done through inclusive stakeholder consultation, opined Kulkarni.
- Whenever a new regulation is discussed, a cost benefit analysis needs to be done to ensure that the costs of regulation do not outweigh its intended benefits, suggested Kulkarni.

Community Response during the session:



Next Steps

Based on the inputs received during the session, we are working to create a community document, where all interested organizations and individuals can contribute (and will be attributed) on what constructive regulations or codes of practice should look like when dealing with data of minors.

Annexure: Extracts from the DPB'21

Definition of a child

Section 3.8: "Child" means a person who has not complete 18 years of age

Chapter IV: Personal Data of a child

16.1: Every data fiduciary shall process the personal data of a child in such manner that protects the rights of the child.

16.2 The data fiduciary shall, before processing of any personal data of a child, verify his age and obtain the consent of his parent or guardian in such a manner as may be specified by regulations.

16.3 The manner for verification of the age of child under sub-section (2) shall take into consideration-

a. the volume of personal data processed

b. the proportion of such personal data likely to be that of child;

c. the possibility of harm to child arising out of processing of the personal data and

d. such other factors as may be prescribed.

16.4: The data fiduciary shall be barred from profiling, tracking or behavioral monitoring of, or targeted advertising directed at children and undertaking any other processing of personal data that can cause significant harm to the child.

16.5: The provision of subsection (4) shall apply in such modified form to the data fiduciary offering counselling or child protection services to a child, as the Authority may by regulations specify.


CCAOI
CUTS
International
Internet
Society
Delhi Chapter