ARE INDIA'S CHILDREN SAFE?

Pallav Arora[*]

ABSTRACT

This article aims to analyse the contemporary developments in the sphere of child privacy in India while comparing it with the International policy on the matter. It seeks to initiate a discourse on why it is vital to deal with children exclusively to ensure data privacy. The article initially examines the existent privacy protection regimes in various jurisdictions around the world, followed by the recently tabled Personal Data Protection Bill in India. It identifies pertinent issues concerning the bill, such as blanket age characterization, easy-to-circumvent mechanisms and the issue of universal parental consent. It thereafter analyses the effect of the aforementioned on the privacy protection mechanisms in the country. The article draws a parallel between the provisions of the Bill and those which are followed in other jurisdictions, such as the Child Online Privacy Protection Act in the United States and the General Data Protection Regulations in the European Union. A comparison is drawn between the two jurisprudential paradigms to derive the best

[*]Pallav Arora is a first-year student at West Bengal National University of Juridical Sciences, Kolkata. The author can be reached at pallav220096@nujs.edu.

practices prevalent in this field. It takes inspiration from the well-functioning systems of child privacy and discusses their application in the Indian context. Finally, recommendations to enhance the character of the Bill and surrounding discourses are made to further the scope of online protection for children in India.

Keywords- Personal Data, Online Environment, Age Characterization, Parental Consent, Age Grating

I. INTRODUCTION

It is estimated that one in three internet users in the world is a child under the age of 18.[1] The use of the internet is becoming increasingly popular among children, especially amidst the COVID-19 pandemic. However, due to a lack of cognitive ability and maturity, children are more susceptible to be misled and influenced by online sources.[2] Therefore, children present a vulnerable group that requires a heightened level of protection concerning their personal information.[3]

Previously, most information privacy laws were formulated with no specific emphasis on any particular age group. However, with increasing reports of child data abuse, states are taking up the necessary task of addressing the issues for the most sensitive stakeholders.

[1]Sonia Livingstone, 'One in Three: Internet Governance and Children's Rights' (2015) Global Commission on Internet Governance Paper Series No. 22 <https://www.cigionline.org/sites/default/files/no22_2.pdf> accessed 28 October 2020.

[2]Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's personal data in the EU: Following in US footsteps?' (2017) 26 Information & Communications Technology Law 2 <http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096> accessed 28 October 2020.

[3]Ibid.

However, studies conducted across the European Union ("**EU**") have highlighted instances of personal data misuse and reputational damage (such as hacking social media accounts, creation of fake accounts, and impersonation), that are affecting children.[4] Additional issues, such as non-child-tailored privacy policies, excessive collection of personal data from children and its unexpected disclosure for third party gains have also been observed.[5] Therefore, several countries have recognised the need to ensure a safe environment for all children surfing through the internet.

The scope of this article is to focus on the seldomly talked about issue of creating a safe space for the children of India. To that end, the article analyses the provisions of the Personal Data Protection Bill, while comparing it with the practises followed in foreign jurisdictions.

II. INTERNATIONAL SPHERE

Right to privacy finds its international genesis in the Universal Declaration of Human Rights ("**UDHR**") adopted in 1948 which states that "*[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.*"[6]This was subsequently reaffirmed in the International Covenant on Civil and Political Rights ("**ICCPR**") in

[4]Giovanna Mascheroni and Kjartan Ólafsson, 'Net Children Go Mobile: Risks and Opportunities' (2nd edn Educatt, Milan 2014) <https://www.researchgate.net/publication/283320908_Net_Children_Go_Mobile_risks_and_opportunities_Second_edition_Milano_Educatt> accessed 20 June 2021.

[5]The Global Privacy Enforcement Network Committee, *2nd GPEN Annual Report* (2016) <https://www.privacyenforcement.net/system/files/Annual%20Report%20for%202015_0.pdf> accessed 20 January 2021.

[6]Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) ("UDHR") art 12.

1976.[7] It has since also been incorporated into other conventions including the Convention on the Rights of the Child ("**CRC**").[8]

There has been an evolution in the understanding of the right to privacy which is reflected in key United Nations Resolutions and discussions.[9]

Article 16 of the CRC, read with the language of ICCPR and UDHR, makes it clear that this right should be specifically extended tochildren. It therefore ensures an equal level of protection for their privacy as adults.[10]

Private-sector data collection in the international sphere presents a complicated set of questions for regulators to draw a demarcation between what is allowed and what is not. There is little universality about an agreed mechanism for ensuring this protection specifically to children. In Europe, companies may be constrained only by piecemeal sectoral legislation and self-regulatory initiatives.It is nearly impossible to assess data collection practises of the leading online companies based in the United States owing to their vastly diverse models of data collection.[11] Therefore, let us delve into the specific legislations dealing with child privacy in the various countries.

A. United States of America

Children's Online Privacy Protection Act ("**COPPA**") was one of the first legislations to deal exclusively with the protection of children on the internet, enacted in 2000. It was brought in as a backdrop tothe

[7]International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 ("ICCPR"), art 17.
[8]Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 ("CRC"), art 16.
[9]UNHCR (20th Session), 'Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet' (29 June 2012) UN Doc A/HRC/20/L.13.
[10]United Nations International Children's Emergency Fund, *Privacy Protection of Personal Information and Reputation Rights* (Discussion Paper Series: Children's Rights and Business in a Digital World) <http://defenddigitalme.com/wp-content/uploads/2018/02/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf>.
[11]Ibid.

Federal Trade Commission ("**FTC**") investigation on the practices of website KidsCom.com for deceptive malpractices.[12] COPPA puts parents in control of what information commercial websites collect from children below the age of 13[13] and requires parental consent for services directed towards children in manners prescribed by the FTC.[14]

B. Europe

The European Union General Data Protection Regulation ("**GDPR**") recognises that children need more protection than adults as they may not be responsive to the risks online services entail. The EU GDPR has established parental consent requirement on websites, that offer information society services[15] directly to children under the age of 16.[16] However, states have set up age thresholds contrary to the GDPR owing to its lack of consensual rules. For instance, Spain provides that subjects over the age of 14 are eligible to give their independent consent.[17]

C. Australia

Australia's Privacy Act provides that consent may be obtained from an individual if they have the capacity to consent. An organisation may presume that the individual has the capacity to consent unless there is

[12]Joshua Warmund, 'Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act' (2001) 11 Fordham Intell. Prop. Media & Ent LJ 189 <https://ir.lawnet.fordham.edu/iplj/vol11/iss1/7>.
[13]Children Online Privacy Protection Act 1998 (US).
[14]Ibid.
[15]Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations andof rules on Information Society services (codification) [2015] OJ L 241/1, art 1(1)(b).
[16]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, art 8.
[17]Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights 2018 (Spain).

something to suggest otherwise. The Act does not prescribe an age threshold after which an individual can make their informed consent.[18] If an organisation is handling the personal information of an individual under the age of 18, and knows this, the organisation must determine whether that individual has the capacity to provide consent on a case-by-case basis.[19] If the organisation is unable to do so, and the individual is above 15 years of age, he/she is automatically deemed to have the capacity.[20]

D. United Kingdom

The United Kingdom Data Protection Act ("**DPA**") does not prescribe an age of consent. However, the Information Commissioner's Office has administered certain guidelines to ensure fair and lawful consent. Those who agree to sharing of their data must know the purpose for its collection. Therefore, with respect to children, the ICO suggests that it is a good practice to ensure that data is collected in a manner in which the audience (the child) is likely to understand and that the amount and nature of data being collected from a child is proportional to their level of understanding.[21]

[18]OAIC, 'Children and Young People' (2018) <https://www.oaic.gov.au/privacy/your-privacy-rights/children-and-young-people/> accessed 20 June 2021.

[19]OAIC, 'Australian Privacy Principles Guidelines: Privacy Act 1988' (2014) <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/> accessed 28 December2020.

[20]OAIC, 'Children and Young People' (2018) <https://www.oaic.gov.au/privacy/your-privacy-rights/children-and-young-people> accessed 28 December 2020.

[21]ICO, 'Personal Information Online: Code of Practice' (2010) <https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf> accessed 3 January 2021.

III. PERSONAL DATA PROTECTION BILL

The Personal Data Protection ("**PDP**") Bill saw its inception along with the report of the Srikrishna Committee set up after the pronouncement of the right to privacy as a fundamental right. The draft submitted by the Committee of Experts to the Ministry of Electronics and Information Technology was deliberated upon after consulting with the stakeholders and was finally introduced at the PDP Bill 2019.[22] It was subsequently submitted to the Joint Parliamentary Committee under Smt. Meenakshi Lekhi, the Report of which is still awaited.

Chapter IV of the Bill deals with the protection of a child's privacy. It creates an obligation on data fiduciaries to obtain parental consent for age verification.[23] However, it does not elucidate the methods for obtaining this consent. It states that the regulations shall take into consideration several parameters such asthe volume of personal data processed, the propensity of the data to belong to a child, the possibility of harm deriving from its processing, and other factors as may be prescribed.[24]

It also encompasses a provision to label certain fiduciaries as 'guardian' fiduciaries who deal with personal data of children or operate services directed towards children.[25] Such fiduciaries would also be barred from profiling, tracking behavior, targeting advertisements, or indulging in any manner harmful to the children.[26] It also enlists an exemption to parental consent for guardian fiduciaries dealing in child counselling or child protection services.[27]

[22]ORF Technology and Media Initiative, *The Personal Data Protection Bill 2019: Recommendations to the Joint Parliamentary Committee*, (ORF Special Report No. 102, 2020).
[23]Personal Data Protection Bill 2019 (India).
[24]Ibid, s 16(3).
[25]Ibid, s 16(4).
[26]Ibid, s 16(5).
[27]Ibid, s 16(6).

IV. ISSUES WITH THE BILL

A. Blanket age characterization

The PDP defines 'child' as any person who has not completed the age of eighteen.[28] There has been an increasing discontentment among service providers dealing with children of this particular bracket. These include gaming industries as well as social media platforms. The Bill does not differentiate between a thirteen-year-old and a sixteen-year-old and considers both to be equally vulnerable to online menace. This becomes a problem in a time when the internet has become the greatest educator for young minds. For instance, according to research conducted by Wigley and Clarke in 2000, the percentage of children using the internet in the United Kingdom in 2000 was around 75%.[29] BMRB's Youth TGI (2001) showed that the most common uses are studying/homework accounting for 73% of the total.[30] This widespread use has increased manifold in the last two decades. In 2016, approximately 44 million children in India were between the ages of 16 and 18.[31]

It thus becomes essential to weigh the interest of the children with the restrictions such a policy brings. The Bill fails to consider that privacy may mean different things for a thirteen-year-old and a seventeen-year-old. While it means parental oversight for the thirteen-year-old, it might as well mean privacy from parents for the seventeen-year-old. The classification needs to take into account the maturity and understanding

[28]Ibid, s 3(8).
[29]Sonia Livingstone, 'Children's Use of the Internet: Reflctions on the Emerging Research Agenda' (2003) LSE Research Online <http://eprints.lse.ac.uk/archive/00000415> accessed 20 June 2021.
[30]Ibid.
[31]Rajesh Bansal, 'Reconciling a child's right to privacy and autonomy' *Hindustan Times* (India, 18 December 2019) <https://www.hindustantimes.com/analysis/reconciling-a-child-s-right-to-privacy-and-autonomy/story-FbpCPhr377diNTkawu5x6K.html> accessed 08 January 2021.

of the child, synonymous with the provisions of the Juvenile Justice Act for the age group 16-18.

Such a blanket characterization may disincentivize industries having children between 14-16 as their target audience,[32] the video game industry, being a good example of the same. Unless extensive age verification methods are made, this industry might have to exclude serving this category overall or make separate versions for adults and children to counter the problem. The Interactive Software Federation of Europe, which represents the gaming industry in Europe, highlighted the need for a flexible interpretation of a child by not putting the threshold as a number.[33] Moreover, the age prescribed under GDPR in Europe is 16 years which is still narrower than the one in PDP.[34]

B. Restrictions on tracking behaviour

While 'behavioural advertising' provides a way for companies to offer consumers greater convenience, this brings a concomitant risk to users' privacy, as behavioural profiling incentivizes the collection of increasingly larger amounts of personal data.[35] A company might not only track how users engage with their online services, but also how

[32]Aditi Chaturvedi, 'Children's Online Privacy Must Be Protected, But Not All Are Equally Vulnerable On Internet' *The Print* (India, 1 January 2021) <https://theprint.in/opinion/childrens-online-privacy-must-be-protected-but-not-all-are-equally-vulnerable-on-internet/577165/> accessed 18 June2021.

[33]Interactive Software Federation of Europe, 'The Information Commissioner's Public Consultation on the Code for Age-Appropriate Design' (2020) <https://www.isfe.eu/wp-content/uploads/2019/06/ISFE-response-to-the-ICO-consultation-on-the-Code-for-Age-Appropriate-Design.pdf> accessed 29 January 2021.

[34]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[35]UNICEF, *Privacy Protection of Personal Information and Reputation Rights* (Discussion Paper Series: Children's Rights and Business in a Digital World).

they behave elsewhere on the internet, how they use their mobile devices, where they are located, and even how they use their cursor.[36]

Moreover, children's increased susceptibility to advertised messages poses a greater risk of influenced behaviour without the child even noticing it.

However, these restrictions may distort the functioning of certain industries, the fundamentals of which involve data collection.One of the most essential characteristics of gaming is to track user behaviour and facilitate subsequent awards for a better user experience. A hindrance in the tracking mechanism might erode the value of this experience.

The 'Ed-tech sector' will also be adversely affected,since tracking a child's progress is one of the key services that it entails. Startups like Byjus which reported a 150% surge during the pandemic will bear the brunt of such a regulation.[37] Equally, there can be arguments for the interference with the privacy of these children in light of their ongoing physical or mental development. For instance, the invasion of a child's physical privacy can be expected to ensure necessary health requirements and medical care. By the same token, while preventing children from engaging with the world without supervision can curtail their freedom, it can also create safe spaces for them to play, learn and communicate in ways that are central to their growth and empowerment.

[36]Van Alsenoy, Brendan, et al., 'From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms' (2015) <www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf> accessed 9 January 2021.

[37]Mrinal Mohit, 'BYJU'S witnesses 150% surge in new students' *Economic Times* (India, 07 April 2020) <https://cio.economictimes.indiatimes.com/news/enterprise-services-and-applications/byjus-witnesses-150-surge-in-new-students/75020127> accessed 13 January 2021.

However, the Bill makes way for ensuring accountability for start-ups which carry a lot of sensitive information. The privacy breach at Facebook backed Unacademy compromising the data of 22 million child users including their name, email address and mobile numbers show the risk posed by such data collection.[38] In the United States, three senators expressed concern over the functioning of these Edtech companies to the Federal Trade Commission to ensure accountability.[39]

Moreover, the Bill identifies certain data fiduciaries which are more likely to be processing children's data as 'Guardian Fiduciaries'. However, this demarcation is not put to optimal use as there are no added obligations (greater accountability, data protection impact assessments, creative information sorting, etc.) on these fiduciaries except a bar on profiling, tracking, and monitoring children's data. It is not clear why the bar is limited to Guardian fiduciaries and whether the fiduciaries outside this threshold are allowed to breach it.

C. Parental consent

The Bill proposes age verification techniques like age-gating methods that help differentiate between adults and children. It is very difficult to verify the age of a child using an online service.[40] Most of these mechanisms lack face-to-face value and website operators may find it

[38]Anadi Chandrashekhar, 'Unacademy database of 22 million users hacked' *Economic Times* (India, 8 May 2020) <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/unacademy-database-of-22-million-users-hacked-up-for-sale/articleshow/75594089.cms?from=mdr> accessed 10 January 2021.

[39]Senators Markey and others, 'Letter to FTC Commissioners on COPPA and Children's Privacy', 4 October 2019 <https://www.markey.senate.gov/imo/media/doc/Markey%20letter%20to%20FTC%206(B)%20on%20children%27s%20privacy.pdf> accessed 12 January 2021.

[40]European Commission, *Article 29 Data Protection Working Party, Opinion 15/2011 on the Definition of Consent* (2011) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> accessed 24 December 2020.

difficult to verify the identity of its users.[41] The difficulty of coming up with effective mechanisms was highlighted in the Report of the Justice Srikrishna Committee.[42] The Bill brings within its fold almost every website, which will be required to collect more data about users than it does to carry out age verification processes.[43] However, the process to ensure this verification remains to be seen considering the wide range of websites that are brought within the purview. It will understandably become really difficult to ensure rigorous verification mechanisms such as age-bearing certificates or the use of parental cards for all the websites concerned. The United States' Children's Online Privacy Protection Act serves as a better example by narrowing its approach only for those websites which are specifically directed towards children.[44] These online portals are required to ask for a parent's government-issued ID, credit card details, provide a call-centre number, or use any other method as evidence to verify consent.[45]

Implementing effective age-grating mechanisms has been an existent problem since most of the in-place systems can be easily circumvented. Reliance can no longer be placed on 'Simple checkboxes' or 'Captcha'.

[41]Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's personal data in the EU: Following in US footsteps?' (2017) 26 Information & Communications Technology Law 2 <http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096> accessed 28 October 2020.

[42]MeitY, *A Data Protection Framework for India* (White Paper of the Committee of Experts) <https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf> accessed 28 October 2020.

[43]Aditi Chaturvedi, 'Children's Online Privacy Must Be Protected, But Not All Are Equally Vulnerable On Internet'*The Print* (India, 1 January 2021) <https://theprint.in/opinion/childrens-online-privacy-must-be-protected-but-not-all-are-equally-vulnerable-on-internet/577165/> accessed 19 January 2021.

[44]Children Online Privacy Protection Act 1998 (US).

[45]Federal Trade Commission, 'COPPA Guidance Policies' (2016) <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step4> accessed 20 January 2021.

There has been an added emphasis on how this parental interruption may prevent the children from employing their rationale skills as an individual to access services online. The internet can be used to create a safe space for children to expand their cognitive skills which may be hampered by the restrictions their parents place on them.[46] Perhaps most concerning, parents who threaten their children's safety may use their power to cut off digital lifelines for seeking outside assistance.[47] Moreover, parents might unintentionally affect the reputation of the child on an online platform. The parents may find it a common practice to share information about their child online with the child lacking the reasonability to scrutinise the information which leaves a lasting mark on their digital footprint.[48]

V. RECOMMENDATIONS

The guardian fiduciaries may be equated to other obligations of significant data fiduciaries so that harm can be minimised. As the name suggests, a significant data fiduciary is an information fiduciary, but they fall under a 'significant' category according to the data privacy and cybersecurity authorities depending on the type of personal data and its risks, and how sensitive it is. Another important detail is that data fiduciaries that fall under the significant category have to fulfil all the special accountability requirements.

The guardian fiduciaries can be made liable to certain additional compliances of significant data fiduciaries such as data protection impact assessments to help identify unique ways in which a child can be harmed through data processing.

[46]Elena Pearl, 'Internet Safety' (*KidsHealth*, April 2018) <https://kidshealth.org/en/parents/net-safety.html> accessed 25 April 2021.
[47]Sonia Livingstone, 'Children's privacy online: experimenting with boundaries within and beyond the family' in Kraut Robert, Malcolm Brynin and Sara Kiesler (eds), *Computers, Phones, and the Internet : Domesticating Information Technology. Humantechnology interaction series* (OUP 2006) 145.
[48]UNICEF, *Privacy Protection of Personal Information and Reputation Rights* (Discussion Paper Series: Children's Rights and Business in a Digital World).

A differentiated age approach may be adopted to take into account the capacity of each age group to act reasonably. With a vast majority of children using the internet today, it becomes imperative to recognize the unique harms carried by these services for unique age categories. Such an approach has also been recognized by National Commission for Protection of Children's Rights which provides separate guidelines to older children in its guide to online safety for children.[49] The regulations must look over the concerns of both the child's privacy as well as their freedom to navigate the internet. For instance, a graded approach like the United States' COPPA can be adopted with a requirement to obtain parental consent for children below the age of 13 and limiting this consent to certain services for a child above this age. This will not only serve the interests of a child's freedom, but also ensure that industries serving the target population of 14-18 years remain intact. The United Kingdom model can also be followed by allowing consent by children on a case-by-case basis through the use of specialised tests and regulations. At the same time, parental consent can be made mandatory for access to conditioned services for the child. While the exception for counselling and child protective services is useful in this context, practical concerns regarding the accessibility of such services and the relevance of harm in these contexts need to be accounted for.

To circumvent the problem of ensuring that concrete age grating measures are observed, inspiration can be taken from the USA's COPPA which only targets websites that specifically cater to children or have the knowledge of their services being used by children. Such a targeted approach will ensure that instead of resorting to simple checkboxes due to regulatory lapses, the specific category can use concrete evidence of age verification. For instance, online portals are required to ask for a parent's government-issued ID, credit card details,

[49]NCPCR, 'Being Safe Online: Guideline and standard for raising awareness among children, parents, educators and general public' (2017).

provide a call-centre number, or use any other method as evidence to verify consent in the United States. The regulations for age-grating must entail tests that account for maturity. The present system of simple checkboxes and undertakings must be done away with. This will ensure accountability since the present regulations can be circumvented by a child on his own. For instance, an age verification system that relies on arithmetic tests, could in theory verify the age of the person consenting, if there is an expectation that children will not be able to make such calculations, but this may not be the case for older children.[50] However, it must be ensured that data protection principles are maintained in these tests as well so that they do not end up obtaining more personal information than required.

VI. CONCLUSION

While the introduction of the PDP Bill is a step in the right direction for ensuring child safety online, it still suffers from a lack of regulative and semantic structure. Problems like the absence of maturity consideration mechanisms, inadequate regulation techniques, and over-reaching restrictions plague the objectives the legislation aims to achieve. Concomitantly seen with the existing technological uses, the Bill fails to give viable alternative for children. It uses the static age threshold for formulating policy which does not seem relevant in the current age of technology. It still has a lot to cover in terms of progressive measures to be able to work as well as the United States' COPPA or European Union's GDPR which cater well to the stakeholders. It becomes highly important in the current scenario where the internet serves as the leading educator for children. With the pandemic lingering, this onset of online importance seems relevant for the near future. Parents find themselves faced with the choice of either

[50]Smitha Krishna Prasad, 'Personal Data Protection Bill, 2019: Protecting Children's Data Online' (*Medianama*, 16 January 2020) <https://www.medianama.com/2020/01/223-pdp-bill-2019-children-protection> accessed 28 January 2021.

ensuring a safer environment, or helping their children make optimal use of the facility. Enhancing the age grating mechanisms by resorting to a differentiated model as proposed, might provide the required balance between 'security' and 'utility'. Further, inclusion of additional compliances for the data fiduciaries might seem to be a step in the right direction to ensure accountability. It therefore lies upon the standing committee to recommend the key changes to ensure the creation of a safe as well as a conducive environment online for children in India.