Working Paper on Safeguarding Children's Informational Privacy in India: An Assessment of the Framework under the PDP Bill, 2019

April 2022

This working paper is a non-commissioned report prepared by the Centre of Applied Law & Technology Research (ALTR), at the Vidhi Centre for Legal Policy, an independent think-tank doing legal research to help make better laws and improve governance for the public good.

About the author

Trishee Goyal is a Research Fellow working with the Centre for Applied Law & Technology Research (ALTR) at Vidhi.

The author would like to thank Ameen Jauhar, Team Lead, ALTR for insightful comments. The author acknowledges the excellent research assistance provided by our intern Dhruv Holla (National Law School of India University).

.

Table of Contents

Safeguarding Children's Informational Privacy in India: An Assessment of the Framework under the PDP Bill, 2019

Introduction

Children today represent the first generation that has been born into a digital age. Their parents are the first to rear "digital children".[1] Personal information of children can be shared by their guardians and by themselves i.e. the personal information *of* children and personal information *by* children respectively. In the early years, a child's digital identity is largely shaped through the data that their family shares. The earliest instance of this is usually the *in utero* images shared by parents and families on social media. As such, it has been seen that 80 percent of children in some western countries have a digital footprint before they are 2 years old.[2]

However, when data privacy legislation refers to child privacy, it is mostly in the context of personal information *by* children. This unauthorised use of children's data occurs in many ways. The more visible and discussed instances of this include copying of images and using them in a disreputable manner, sharing of personal contact details or collating various information made publicly available and posting them on an unauthorised website (such as combining images with contact details).[3] While these instances involve unauthorised use of personal data, the harms that arise from them in terms of risk to reputation, unsolicited contact that may lead to cyberbullying, online harassment or sexual abuse are covered under generic cyber law offences. This paper concentrates on harms relating to informational privacy that arise from unauthorised use of personal data.

Children are connected to the internet in a number of ways. This takes place through connected devices that children own or have access to (such as their parents' or devices in school). Apart from their own personal connected devices, children also use connected technology and devices in their households such as smart TVs, voice

[1] United Nations Special Rapporteur for Privacy, "Artificial Intelligence and Privacy, and Children's Privacy" Human Rights Council (2021) available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement (last accessed April 6, 2022).
[2] National Authority for Data Protection and Freedom of Information, "Key to the World of the Net" as submission by Hungarian National Authority for Data Protection and Freedom of Information to the UN Special Rapporteur for Privacy, Page 42 2016 available at https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/privacy-child/NHRI-Ombusman-Commissions/5-Hungary-DPA-I.pdf (last accessed April 6, 2022).
[3] National Authority for Data Protection and Freedom of Information, "Key to the World of the Net" as submission by Hungarian National Authority for Data Protection and Freedom of Information to the UN Special Rapporteur for Privacy, Page 9 2016 available at https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/privacy-child/NHRI-Ombusman-Commissions/5-Hungary-DPA-I.pdf (last accessed April 6, 2022).

controlled speakers, internet enabled thermostats and internet enabled security systems.[4] Moreover, children's participation online now occurs at earlier ages than before.[5] For example, between the ages of 9 to 10 and 11 to 12, it has been observed that social media usage doubles from 34 percent to 69 percent.[6] The pandemic has accelerated this trend considerably. During the pandemic, the daily active accounts on Facebook's Messenger Kids grew by 350 percent between March to September 2020.[7] This immersion in the continually increasing range of digital applications generates enormous amounts of personal data. The processing of this personal data is enhanced using artificial intelligence, machine learning applications and facial and speech recognition technologies.

And this processing is not always optimal. As early as 2012, the FTC's review of 400 kids' apps revealed that most of them lacked transparency and clear disclosures about data protection.[8] Given that such violations were found in a jurisdiction that was at the time probably the only one to have child specific privacy legislations, and almost 12 years into its enforcement, it can be assumed that privacy protections for children in other jurisdictions would be even more lax. In 2015, a review of almost 1500 applications and websites directed towards children led to similar findings. There were issues concerning excessive collection of personal data from children and frequent disclosure of children's data to third parties. It was also found that only 15 percent of these websites had any age gating mechanisms, and quite a few of them allowed access even after determining that the user was underage.[9]

Regulators as well as data subjects are still trying to grapple with the implications that newer forms of data processing have on their rights of autonomy and privacy. Therefore, it is all the more important to develop nuanced regulatory thinking for children's privacy. This is because children are in an especially precarious position when it comes to regulation of data processing. Even as children are becoming increasingly familiar with the digital environment, given their developmental stage, they are not in a position to understand the long term implications of their actions online. They are

[4] Future of Privacy Forum, "The State of Play: Verifiable Parental Consent and COPPA" (2021) page 5 available at https://fpf.org/wp-content/uploads/2021/11/FPF-The-State-of-Play-Verifiable-Parental-Consent-and-COPPA.pdf (last accessed April 6, 2022).
[5] The results of the European EU Kids Online 2020 survey shows that the time young people spend online has almost doubled since 2010. See, Smahel et al, "EU Kids Online 2020: Survey Results from 19 Countries" (2020) available at https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf (last accessed April 6, 2022).
[6] Economic Commission for Latin America and the Caribbean (ECLAC), "Submission to the UN Special Rapporteur for Privacy on Online Independence and Autonomy, and the Privacy Rights of Children and Adolescents in Latin America" Table 1, Page 2 (2020) available at https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/privacy-child/Regional-Org-and-UN/2-ECLAC.docx (last accessed April 6, 2022).
[7] Facebook, "Submission to the UN Special Rapporteur for Privacy, A Better Understanding of Privacy: Children's Right to Privacy" (2020).
[8] Federal Trade Commission, "Mobile Apps for Kids: Disclosures Still Not Making the Grade" (2012) available at https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf (last accessed April 6, 2022).
[9] Global Privacy Enforcement Network, Sweep-Children's Privacy' (2015) available at http://194.242.234.211/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf, (last accessed April 6, 2022).

also not equipped to discern deceptive practices online and protect themselves.[10] This leads regulatory frameworks to endow them with none or limited agency in relation to their own privacy. But this capacity and their need for privacy evolves at a fast and often differential rate making it counter productive to treat them as a homogenous group. There are differences of capacity not only between different age groups but also within the same age group depending on the particular context of the child. This poses significant challenges in developing an effective approach.

It is in this context that this working paper tries to contribute to the discourse of children's informational privacy in India. In the first section, prevalent threats to children's right to privacy are examined. This provides context to understand the nature and sources of harm that a regulatory framework concentrate on. The first level in this analysis is to assess the overarching legal principles that should govern the exercise of this right. Accordingly, the second section deals with an understanding of children's informational privacy as per the UN Convention on the Rights of the Child. Given that it is one of the foundational rights based framework for children which is widely adopted across jurisdiction, discussion of this framework helps in understanding the principles in a jurisdiction neutral manner. The third section then undertakes a multi jurisdictional survey with the aim of understanding how these principles are adopted in the respective jurisdictions, as also to understand the position of law.[11] This provides a useful framework to understand the nuances of the Indian framework. It needs to be noted that most jurisdictions, like India, are still at a very early stage in developing their regulatory approach on the issue. Nonetheless, their limited experience is also useful for us. The fifth section evaluates the common regulatory solutions that emerge from the foregoing analysis. In light of all this, in the sixth section the paper outlines some immediate focus for India's proposed Data Protection Authority for it to develop an effective regulatory. The paper then concludes. The final draft of the paper will be updated with a section focusing on harms arising from unregulated processing of health and education data of children.

[10] Milda Macenaite and Eleni Kosta, "Consent for Processing Children's personal data in the EU: Following in US footsteps?", 26(2) Information & Communications Technology Law Journal (2017) available at http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096, (last accessed April 6, 2022).
[11] One of the areas of updation in the working paper will be inclusion of more jurisdictions in the final draft.

I. *Threats to children's privacy*

Privacy is essential for the development of children. Research indicates that privacy related media literacy skills are interrelated with a range of development areas for children. These include autonomy, identity, intimacy, responsibility, pro social behaviour, resilience, sexual exploration and critical thinking.[12] The threats to children's privacy are dynamic in nature, evolving as they do, with the prevalent technology and emerging situations. For instance, in the recent times, the pandemic has greatly accelerated digitalisation of records and online activity of children. While new areas of threat emerge, such as the edu-tech sector, there are some traditional actors that pose threat to children either because of the nature of activities they undertake (businesses, governments) or the way in which they are juxtaposed with children in the digital environment (guardians). While discussing an effective framework for regulation of children's privacy, it is relevant to discuss the technology agnostic threats that underlie children's privacy.

(1) Businesses

Digital service providers today have the capability to constantly monitor and process information about users' communications, activities and behaviour online.[13] The personal data so collected has significant monetary value in the "attention economy"[14] where it is used to modulate behaviour for various purposes beneficial to service providers such as maximising engagement, triggering impulsive behaviours and influencing decision making.[15]

Children today constitute the largest proportion of users of digital technologies.[16] It is estimated that more than 72 million pieces of data are collected per child by online advertising companies before they are 13 years old.[17] This massive data collection raises concerns about these digital tracks that can be used for affecting their access to even basic services such as education, employment, health care and financial services.

[12] Peter and Valkenburg, 2011; Raynes-Goldie and Allen, 2014; Pradeep and Sriram, 2016; Balleys and Coll, 2017.
[13] United Nations Special Rapporteur for Privacy, "Artificial Intelligence and Privacy, and Children's Privacy" Human Rights Council (2021) available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement (last accessed April 6, 2022).
[14] D. Vivrekar, "Persuasive Design Techniques in the Attention Economy: User Awareness, Theory, and Ethics" (2018) available at: https://stacks.stanford.edu/file/druid:rq188wb9000/Masters_Thesis_Devangi_Vivrekar_2018.pdf (last accessed April 6, 2022).
[15] United Nations Special Rapporteur for Privacy, "Artificial Intelligence and Privacy, and Children's Privacy" Human Rights Council page 14 (2021) available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement (last accessed April 6, 2022).
[16] UNICEF (2017). Children in a Digital World, The State of the World's Children 2017, p.1. Available at: https://www.unicef.org/publications/files/ SOWC_2017_ENG_WEB.pdf
[17] ABC News Breakfast, "How Your Child's Online Profile is Being Captured and Shared" (2018) available at https://www.abc.net.au/news/2018-06-15/how-your-childs-online-data-is-being-captured-and-shared/9869272 (last accessed April 6, 2022).

There are three ways in which commercial processing of personal data can harm children. First, pervasive profiling can lead to more incisive behavioural predictions and nudging techniques. This can significantly impair self development and autonomy in children by predetermining their choices.[18] These concerns are accentuated when automated decision making with opaque algorithms are deployed for such profiling. For example, automated decision making can discriminate against certain characteristics such as gender, language, age, ability and socio economic status resulting in digital racism.[19] Second, locking user attention is incentivised through the creation of "filter bubbles" and echo chambers can limit the development of children's critical thinking.[20] Moreover, attention retention techniques also means that children are unable to maintain a healthy balance between offline and online activities.[21] Third, behavioural advertising and promotion of in-application purchases can also lead to commercial exploitation of children, especially for younger children.[22] Younger children are vulnerable to targeted marketing because they have reduced capacity to differentiate between advertised and non-advertised content, as well as to understand the persuasive nature of advertising.[23] It is easy to exploit their experiences online through thinly veiled marketing strategies such as gamified advertisements, use of child influencers, placing advertisements on video platforms and online games.[24] For example, micro-transactions in games and mobile applications are common, and are often designed to be hard for young persons to resist.[25] Commercial exploitation of children can often have negative effects on their health. In a study conducted in Brazil, it was estimated that positive economic results ranged from 61 - 75 million USD in terms of physically or psychologically healthier population for under 12 children, if there was a full ban on advertising for 15 years.[26]

---

[18] United Nations Special Rapporteur for Privacy, "Artificial Intelligence and Privacy, and Children's Privacy" Human Rights Council page 14 (2021) available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement (last accessed April 6, 2022).

[19] Pedro Hartung, "The Children's Rights-by-Design Standard for Data Use by Tech Companies" Issue Brief No. 5 Good Governance of Children's Data Project (UNICEF) Page 5 (2020) available at https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf (last accessed April 6, 2022).

[20] CNIL, "Submission to the UNSRP on the Subject of Privacy Rights of Minors" page 4 (2020).

[21] UK Information Commissioner's Office, "ICO Answer to the Call for Submissions of the UNSRP" Page 5 (2020).

[22] An EU study of 2016 on the impact of online marketing found that online marketing resulted in higher rates of snack consumption and an increase in the spending of in app purchases.
Study on the impact of marketing through social media, online games and mobile applications on children's behaviour. Available at https://ec.europa.eu/info/sites/default/files/online_marketing_children_final_report_en.pdf

[23] Research shows that children upto the age of 8 years do not differentiate between advertising and content. Similarly, upto about 12 years of age, they do not have the necessary judgement to distinguish between fiction and reality. European Commission, "Study on the impact of Marketing through Social Media, Online Games and Mobile Applications on Children's Behaviour" (2016) available at https://ec.europa.eu/info/publications/study-impact-marketing-through-social-media-online-games-and-mobileapplications-childrens-behaviour_en. (last accessed April 6, 2022).

[24] Pedro Hartung, "The Children's Rights-by-Design Standard for Data Use by Tech Companies" Issue Brief No. 5 Good Governance of Children's Data Project (UNICEF) Page 5 (2020) available at https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf (accessed April 6, 2022).

[25] Parent Zone, "The Rip-Off Games: How the New Business Model of Online Gaming Exploits Children" (2019) available at https://parentzone.org.uk/the-rip-off-games (last accessed April 6, 2022).

[26] Concern has been expressed by the American Academy of Pediatrics that targeted marketing campaigns can lead to health disparities among vulnerable children and population. It has recommended limiting advertising to older children and to ban all commercial advertising for children younger than 7 years of age. See, The Economist Intelligence Unit, "The Impacts of Banning Advertising Directed at Children in Brazil" (2017) available at: http:// criancaeconsumo.org.br/wp-content/uploads/2014/02/TheEconomist_EN.pdf (last accessed April 6, 2022).

These concerns have been aggravated with internet-of-things, which allows more collection of personal data, through microphones and cameras, than was previously possible.[27]

(2) Parents / Guardians

Children's privacy has been typically considered an issue for adults to determine. In fact, it is argued that children may be more concerned at their privacy being violated by parents than businesses and governments.[28] There are atleast three ways in which parents may negatively impact their children's right to privacy. First, children's privacy needs can differ and indeed, be in conflict with those of their parents. Sharenting is one such example. Sharenting refers to parents' increased sharing of information about their children on the internet, particularly social media. This shapes a child's online identity before the child has consent on whether or not they want to create their digital footprint. This can bring the parents' right to freedom of expression in conflict with the child's right to privacy.[29]

Second, to exercise their right to consent to provide consent on behalf of the child, parents may want access to their child's private spaces (such as emails, gaming accounts, social network accounts). They may also use the child's account to familiarise themselves with these online spaces to make an adequate evaluation of whether or not they should provide their consent to the particular online service provider for processing their child's personal data.[30] Providing consent on behalf of the child because they may not have the capacity to understand the implications of personal data processing is different from the right to access these private spaces once that consent has been provided and could violate a child's privacy.

Third, in the context of risks to online safety, surveillance by parents online is often framed in terms of "good parenting". Moreover, this surveillance increases with a child's age i.e. it typically increases at a time when young people may choose to become more independent. This can undermine the evolution of autonomy, privacy and independence.[31] As children grow, their expectation of privacy from their parents also

[27] UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) page 20 available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (accessed April 6, 2022).
[28] Rajesh Bansal and Arjun Kang Joseph, "Reconciling a Child's Right to Privacy and Autonomy" (2019) available at https://www.hindustantimes.com/analysis/reconciling-a-child-s-right-to-privacy-and-autonomy/story-FbpCPhr377diNTkawu5x6K.html (last accessed April 6, 2022).
[29] In 2017, a survey conducted of 10-12 years old found that more than 1 in 4 children said that they felt anxious, embarrassed or worried when their parents posted pictures of them online. See,
BBC Newsround, "'Sharenting': Are you OK with what your parents post?" (2017) available at https://www.bbc.co.uk/newsround/38841469 (last accessed April 6, 2022).
[30] Lina Jasmontaite and Paul De Hert, "The EU, Children under 13 years, and Parental Consent: a Human Rights Analysis of a new age based bright line for the protection of children on the internet" page 29 (2015) Vol. 5(1) International Data Privacy Law.
[31] South Australia Comissioner for Children and Young People, "Submission to the United Nations Special Rapporteur on Children's Right to Privacy" (2020) (last accessed April 6, 2022).

grows. In a survey conducted, it was seen that the expectation of privacy of children aged between 15 - 17 differed significantly from those in the lower age groups.[32]

(3) Governments

When it comes to government surveillance, there are no differences in the safeguards applicable to adults and children.[33] Surveillance of children is often explained away as a necessary safeguard for children's own interests.[34] A recent report of Privacy International found that "a significant number of local authorities" use overt and covert social media monitoring for intelligence gathering and investigations in the area of "children's social care".[35]

Collection of biometric data has significantly higher adverse consequences for children especially in terms of increased error rates because of difficulty in capturing the biometric data (iris scan of very young children) and relatively poor performance of these traits among younger age groups (facial recognition).[36] Notwithstanding these issues, there have been reports that such collection is rampant. For example, NYPD has uploaded thousands of photos of arrests of children and teenagers into facial recognition databases.[37] Moreover, increased deployment of digital technologies, declining cost of technology and data storage will lead to collection of unmatched levels of data on children throughout their lifetimes. The processing of such voluminous data itself will lead to unpredictable outcomes.[38]

One such area of increased deployment of digital technologies has been schools. This has been exacerbated since 2020, when the pandemic led to suspension of physical

---

[32] Digital Education Working Group, "Report – October 2020" Global Privacy Assembly Page 25 (2020) available at https://globalprivacyassembly.org/wp-content/uploads/2020/10/DEWG-2019-2020-Annual-Report-GPA-20200921-finalannexes_Oct-2020_final-en-211020-1.pdf (last accessed April 6, 2022). In a consultation undertaken by the Data Protection Commissioner in Ireland, it was found that in response to when children felt they should be able to exercise their own data protection rights, it was found that the older the age of the respondents the greater was their insistence on managing their own personal data. See, Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 34 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (last accessed April 6, 2022).

[33] Committee of Experts, "White Paper of the Committee of Experts on a Data Protection Framework for India" Ministry of Electronics and Information Technology Page 87 (2017) available at https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf (last accessed April 6, 2022).
Privacy protecting legislations for children are focused on protection of their data from private corporations rather than surveillance undertaken by governments.

[34] Steven Feldstein, "State Surveillance and Implications for Children" Issue Brief No. 1 Good Governance of Children's Data Project (2020) available at https://www.unicef.org/globalinsight/media/1101/file/UNICEF-Global-Insight-data-governance-surveillance-issue-brief-2020.pdf (last accessed April 6, 2022).

[35] https://privacyinternational.org/report/3584/when-local-authorities-arent-your-friends

[36] UNICEF, "Faces, Fingerprints and Feet: Guidance on Assessing the Value of Including Biometric Technologies in UNICER Supported Programmes" (2019) available at https://data.unicef.org/resources/biometrics/# (last accessed April 6, 2022).

[37] Joseph Goldstein and Ali Watkins, "She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database", The New York Times (2019) available at https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html (last accessed April 6, 2022).

[38] UNICEF, "Faces, Fingerprints and Feet: Guidance on Assessing the Value of Including Biometric Technologies in UNICER Supported Programmes" (2019) available at https://data.unicef.org/resources/biometrics/# (last accessed April 6, 2022).

schooling and learning activities largely shifted online. This led to digitalisation and storing of learning data at an unprecedented level. This shift was abrupt and unaccompanied with the requisite regulatory response. This is especially concerning considering the high volume of learning data that is generated. It includes thinking characteristics, learning trajectory, engagement score, response times, pages read, videos viewed etc.[39] In the UK, it was found that government's guidance to schools resulted in imposing online filtering and monitoring software.[40] As per the testimony of the provider of the service, the monitoring of "behaviours we detect are not confined to the school bell starting in the morning and ringing in the afternoon; it is 24/7 and it is every day of the year."[41] Similarly, in Russia, facial recognition systems have been deployed to "keep tabs on students' comings and goings and identify strangers who attempt to enter school grounds". Such surveillance has led to the apprehension that children's speech and political expression will be negatively impacted.[42] Other examples of such surveillance include gunfire detection microphones by schools in New Mexico and use of iris recognition technology by officials in New Jersey.[43]

It needs to be noted that consent in an educational setting is of a different nature because the refusal or withdrawal of consent, might lead to denial of educational services, and by itself have huge implications on the development of children. This was also recognised by the Swedish Data Protection Authority. The Swedish DPA censured the school authorities for processing facial data to monitor attendance and levied a penalty. It did not agree with the school authorities' submission that the facial data was processed after taking consent and therefore the processing was lawful. It held that within the public sphere the scope for voluntary consent is limited. Students and their guardians are dependent on the school for education, grades, student grants, loans and future employment.[44] Although surveillance measures may be deployed for legitimate purposes, the purpose and intent is often not circumscribed by such legitimate purposes nor is it sufficiently explained to those being surveilled.[45]

---

[39] Digital Education Working Group, "Report – October 2020" Global Privacy Assembly Page 4 (2020) available at https://globalprivacyassembly.org/wp-content/uploads/2020/10/DEWG-2019-2020-Annual-Report-GPA-20200921-finalannexes_Oct-2020_final-en-211020-1.pdf (last accessed April 6, 2022).

[40] Jen Persson, "Child Safeguarding Cloaks State Surveillance and Data Exploitation" Open Democracy (2017) available at https://www.opendemocracy.net/en/digitaliberties/children-are-at-forefront-of-state-surveillance/ (last accessed April 6, 2022).

[41] Parliament of UK, "Examination of Witnesses" (2016) available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html (last accessed April 6, 2022).

[42] Matthew Luxmoore, "Yes, Big Brother IS Watching: Russian Schools Getting Surveillance Systems Called 'Orwell'" Radio Free Europe/ Radio Liberty (2020) available at https://www.rferl.org/a/russian-schools-getting-surveillance-systems-called-orwell-/30676184.html (last accessed April 6, 2022).

[43] United Nations, "United Nations Treaty Collection", available at https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4&clang=_en (last accessed April 6, 2022).

[44] Swedish Data Protection Authority *Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 - facial recognition used to monitor the attendance of students* Page 4 (2019) available at https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf (last accessed April 6, 2022).

[45] Steven Feldstein, "State Surveillance and Implications for Children" Issue Brief No. 1 Good Governance of Children's Data Project (2020) available at https://www.unicef.org/globalinsight/media/1101/file/UNICEF-Global-Insight-data-governance-surveillance-issue-brief-2020.pdf (last accessed April 6, 2022).

Apart from specific actors, there are also certain kinds of data that pose greater privacy risks for children than others. Two such areas are health data and learning / education data processed by the edtech industry. The pandemic has been a primary enabler in propelling for much higher degree of collection of personal data under both these categories. Commercialisation of health and education data enhances the scope of surveillance and erosion of non commercial spaces. A more detailed section on the both these sectors will appear in the final draft of this working paper.

(4) Health data

Health data sets are considered sensitive and are accorded more information given the kinds of personal details they can reveal about an individual. Advances in technology for collection of this data (wearables, digital health care and well being applications), increased uses of this data (automated decision making for health insurance and predictive analysis) and dilution of safeguards by governments on its use and sharing in the face of the pandemic have pushed the boundaries of privacy for children.[46] Given that such personal data will be shared for a much longer duration for children, as compared to adults, the ways in which it can be processed and the potential harms from it are still unclear.

(5) Edtech

It is estimated that pandemic related school closures led edtech being used in one form or the other for 268 million children. The uses of edtech are varied. It may used to increase efficiency in discharging administrative functions of the school, enabling virtual learning and monitoring student behaviour through parameters such as student performance and attendance.[47] The kinds of personal data collected with the deployment of technology for these activities can lead to invasive tracking from an early age. Moreover, edtech seems to be pushed vigorously under the guise of personalised learning without sufficient scrutiny of their pedagogical efficacy.[48] This often leads parents / guardians to trade in privacy standards in return for enhanced access to these services.[49]

---

[46] UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) page 20 available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (last accessed April 6, 2022).

[47] India Today Web Desk, "State Governments, Edutech Platforms Join Hands to Maintain Learning Continuity for School Students" (2020) available at https://www.indiatoday.in/education-today/featurephilia/story/state-governments-edutech-platforms-join-hands-to-maintain-learning-continuity-for-school-students-1685876-2020-06-05 (last accessed April 6, 2022). Also see, Article 29 Data Protection Working Party, "Working Document 1/2008 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools) (2008) available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf (accessed April 6, 2022).

[48] Bulger, "Personalized Learning: The Conversations We're Not Having", Data & Society, Working Paper (2016) available https://datasociety.net/pubs/ecl/ PersonalizedLearning_primer_2016.pdf (last accessed April 6, 2022).

[49] UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) page 20 available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (last accessed April 6, 2022).

An examination of the common sectors of threat allows provides context to understand how well the legal framework for children's informational privacy holds up to these threats. Before engaging in a multi jurisdictional analysis, the next section elucidates on the legal principles that should ideally underline the legislations and regulatory frameworks for protection of children's personal data.

II. *Principles underlying the right to privacy for children*

The UN Convention on the Rights of the Child (CRC) is the most foundational and widely endorsed body of law on child rights. It has 196 ratifications / accessions. Given that India is a signatory to the CRC it is legally bound to inculcate its legal principles in the regulatory structures.[50] The centrality of the CRC to the child rights framework led to demands that it be formulated in the context of the digital environment. Accordingly, in 2021, the UN Committee on the Rights of the Child (UN Child Rights Committee) brought forth Comment No. 25 to provide State parties guidance on the implementation of the CRC in the digital environment.[51]

Article 16 of the CRC guarantees that "no child shall be subject to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attack on his or her honour or reputation". In General Comment No. 25, the UN Child Rights Committee lays down the fundamental obligations of State parties with regard to children's privacy. These include requiring State parties to take "legislative, administrative and other measures to ensure that children's privacy is respected and protected by *all organisations and in all environments that process their data* (emphasis added)". It further enumerates some of the principles that need to be incorporated in these measures to ensure children's privacy. These are data minimisation, proportionality, transparency, privacy by design and free consent. Further, digital surveillance and associated automated processing of children's personal data should not be conducted routinely, indiscriminately or without the children's consent.

These principles are applicable not only to state parties, but also private entities. This can be concluded both from General Comments No. 25 and 16 of the UN Child Rights Committee. The latter states that the provisions of the CRC are also "directly applicable to business enterprises that function as private or public social welfare bodies by providing any form of direct services for children ….".[52] Internet platforms are increasingly being recognised as a public utility.[53] The UN has recognised the internet as a "key means" to exercise human rights. This means the internet can be understood as a "key direct welfare service for children" and the CRC would also be applicable on data controllers as they participate in the digital environment.[54] It has been argued that

[50] Article 253, Constitution of India, 1950.
[51] United Nations Committee for Rights of the Child, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment" (2021) available at https://digitallibrary.un.org/record/3906061?ln=en (accessed April 6, 2022).
[52] United Nations Committee for Rights of the Child, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment" (2021) available at https://digitallibrary.un.org/record/778525?ln=en (accessed April 6, 2022).
[53] K Sabeel Rehman, "Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities" (2018) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3220737. Also see, Astrid Krisch and Leonhard Plank, "Internet Platforms as Infrastructures of the Digital Age" (2019) available at https://www.researchgate.net/publication/333084183_Internet_Platforms_as_Infrastructures_of_the_Digital_Age (accessed April 6, 2022).
[54] Pedro Hartung, "The Children's Rights-by-Design Standard for Data Use by Tech Companies" Issue Brief No. 5 Good Governance of Children's Data Project (UNICEF) Page 5 (2020) available at

the actions of business enterprises have a direct or indirect impact on children's rights in the digital environment. Therefore, they play the role of social welfare private institutions and would be bound by the CRC.[55]

However, the application of the rights provided for in the CRC is not often as straightforward. There are situations where one set of rights competes with the fulfilment of others. Under the CRC there are three main categories of rights - the rights to provision, protection and participation. This conflict is classically seen to exist between the protective and participative rights. Protective rights are of the nature that guarantee children safety from all forms of abuse, neglect, exploitation and violence.[56] These rights stem from the vulnerability of children, their dependence on adults and the need for physical and psychological care. Article 16 which provides children the right to privacy belongs to this category. However, there have been concerns whether children's developmental challenges are overemphasised to the exclusion of other rights. It could lead to sub par mobilisation of their strengths. This often leads to undermining of the second set of children's rights i.e. participation rights.[57] Participatory rights stem from children's claim to self determination and include various decision making rights. These include children's right to express their views and have access to adequate information;[58] freedom of thought, conscience and religion;[59] association and peaceful assembly;[60] and access to information from diverse national and international sources.[61] This is also recognised by the UN Child Rights Committee. It cautions that privacy and data protection legislation should not arbitrarily limit children's other rights such as right to freedom of speech and expression.[62] To resolve these conflicts between protection and empowerment rights, the CRC provides for two principles of interpretation.

https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf (accessed April 6, 2022).

[55] Alana Institute, "Submission of comments on the draft of the General Comment on Children's Rights in relation to the Digital Environment" (2020) Page 4 available at https://www.ohchr.org/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/2020/others/alana-institute-2020-11-17.docx (accessed April 6, 2022).

[56] Articles 19, United Nations Convention on the Rights of the Child.

[57] Casares et. al., "Children's Right to Participation and Protection in International Development and Humanitarian Interventions: Nurturing a Dialogue" Vol. 21(1) The International Journal of Human Rights (2017). Also see, South Australia Comissioner for Children and Young People, "Submission to the United Nations Special Rapporteur on Children's Right to Privacy" (2020) (last accessed April 6, 2022).

[58] Article 13, United Nations Convention on the Rights of the Child.

[59] Article 14, United Nations Convention on the Rights of the Child.

[60] Article 15, United Nations Convention on the Rights of the Child.

[61] Article 17, United Nations Convention on the Rights of the Child.

[62] United Nations Committee for Rights of the Child, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment" (2021) page 12 available at https://digitallibrary.un.org/record/778525?ln=en (accessed April 6, 2022).

(a) Best interests of the child

Article 3 of the UN CRC provides that "in all actions concerning children .... the best interests of the child shall be a primary consideration".[63] In the context of the digital environment, the UN Committee for Child Rights provides that in considering the best interests of the child, regard shall be had to all other rights of child including their participative rights.[64] This has been adopted as the standard approach various agencies for children's rights in the digital environment. The UNICEF Manifesto for Governance of Children's Data recognises that the best interests of the child should be the primary consideration in data governance.[65] In its Recommendation of the Council on Children in the Digital Environment, the Organisation for Economic Cooperation and Development lays down that the fundamental value that actors while engaging with children in the digital environment need to adhere to is to "uphold the child's best interest as a primary consideration".[66] The European Union adopts this principle in its own guidelines on the rights of the child in the digital environment. It states that one of the fundamental principles of the guidelines is that best interests of the child would be a primary consideration. The determination of this best interest would be made by balancing and reconciling the child's right to protection with other rights.[67] Similarly, Article 29 Working Party (the predecessor) of the European Data Protection Board, in its 2009 Opinion stated that the principle of best interest must be respected by all entities *public or private* while making decisions relating to children".[68] It further accords primacy to best interests in cases where the right to privacy is in conflict with the best interests of the child.[69]

(b) Evolving capacity

Article 5 of the UN CRC provides that for States to issue directions for the exercise of the right of the child, the responsibilities of parents and guardians in protecting the child's interests should be balanced along with the evolving capacity of children

[63] Article 3, United Nations Convention on the Rights of the Child.
[64] United Nations Committee for Rights of the Child, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment" (2021) Page 3 available at https://digitallibrary.un.org/record/778525?ln=en (accessed April 6, 2022).
[65] UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) page 20 available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (accessed April 6, 2022).
[66] OECD, "Recommendation of the Council on Children in the Digital Environment" (May, 2021) available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389%20 (accessed April 6, 2022).
[67] Council of Europe, "Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment" European Union (2018) Page 12 available at https://rm.coe.int/guidelines-to-%20respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881aIbid (accessed April 6, 2022).
[68] Article 29 Data Protection Working Party, "Working Document 1/2008 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools) (2008) Page 4 available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf (accessed April 6, 2022).
[69] Article 29 Data Protection Working Party, "Working Document 1/2008 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools) (2008) Page 5 available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf (accessed April 6, 2022).

themselves.[70] This formulation allows children to be co-determinants of their interests.[71] Similar to the best interests principle, the principle of "evolving capacity" has also been recognised universally in children's data governance frameworks.[72] This essentially means that children live in extremely diverse circumstances and with varying degrees of parental support.[73] Regulatory responses should be built as per evolving capacities of children including those who are differently abled or in vulnerable positions. This would also include recognising that regulatory responses for adolescents would "differ significantly" from those designed for young adults.[74]

Another important aspect of data governance frameworks derives from Article 12 of the CRC. Article 12 provides that States shall allow a child who is capable of forming his or her own views the right to express those views freely in matters affecting the child. Further, the views of the child should be given due weightage in accordance with the age and maturity of the child. In its General Comment No. 12, the UN Child Rights Committee states that child participation is 'ongoing processes, which include information-sharing and dialogue between children and adults based on mutual respect, and in which children can learn how their views and those of adults are taken into account ….'[75]

In its submission to the UN Special Rapporteur on the Right to Privacy, the Council of Europe submits that the right of the child to be heard is required to enhance autonomy and independence of children.[76]

Dynamic self determinism. Eekelaar has sought to tie these principles together by proposing the principle of dynamic self determinism.[77] This principle seeks to resolve the inherent contradiction between children's best interest and children being right bearers. The principle of children's best interests should not give another individual the right to hold complete power to determine what is in the child's best interests. The

[70] Article 5, United Nations Convention on the Rights of the Child.
[71] J.C. Buitelaar, "Child's Best Interest and Informational Self Determination" What the GDPR can Learn from Children's Rights" Vol. 8(4) International Data Privacy Law (2018).
[72] See, United Nations Committee for Rights of the Child, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment" (2021) available at https://digitallibrary.un.org/record/778525?ln=en (accessed April 6, 2022); UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (accessed April 6, 2022); OECD, "Recommendation of the Council on Children in the Digital Environment" (May, 2021) available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389%20 (accessed April 6, 2022); Council of Europe, "Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment" European Union (2018) available at https://rm.coe.int/guidelines-to-%20respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881albid.
[73] UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) page 60 available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (accessed April 6, 2022).
[74] Council of Europe, "Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment" (2018) page 12 available at https://rm.coe.int/guidelines-to-%20respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881albid.
[75] United Nations Committee for Rights of the Child, "General Comment No. 12 (2009) on The Right of the Child to be Heard" (2009) available at https://www2.ohchr.org/english/bodies/crc/docs/advanceversions/crc-c-gc-12.pdf (accessed April 6, 2022).
[76] Council of Europe, "Contribution prepared by the Secretariat of the Council of Europe on the subject of the right to privacy of children, in response to the consultation carried out by the UN Special Rapporteur on the right to privacy (UNSRP)" Page 3 (2020).
[77] J. Eekelaar, "The Role of the Best Interests Principle in Decisions Affecting Children and Decisions about Children" (2015) 23 The International Journal of Children's Rights 3.

principle of dynamic self-determinism creates a mechanism for the principle of children's best interests to interact with the principle of evolving capacities and participation. Dynamic self-determinism states that as children grow up, they can contribute meaningfully to the outcome of their situation. The principle uses the concept of "dynamic" to emphasise that the optimal decisions for choices involving a child cannot be determined just once at the time of decision, but need to be revisited at appropriate intervals. In the context of informational privacy this becomes all the more important. Informational self determination is an important part of informational privacy.[78] Because children exercise their rights through another individual, this principle allows children to increasingly participate in the determination of their best interests.

While thus far, the principles along which the right to privacy is to be applied, it is also useful to consider how other rights provided in the CRC can be formulated in a data protection context. Even though it was adopted more than 30 years ago, the universal nature and forward looking principles of the CRC allow for the formulation of the rights of children in diverse contexts. In a data protection context, child rights will be interpreted in the following ways:

a. ***Non discrimination*** - Article 2 of the UNCRC provides that a child's rights should be ensured without any discrimination on the basis of "race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth or other status".[79] In the context of data protection this would mean that children's data should not be used to discriminate in a manner that diminishes their well being or access to information and digital opportunities or perpetuates bias and digital racism.[80] Children's data should not be used to algorithmic models with biased data or assumptions that can be used to discriminate against them or adversely affect their well being, access to information or digital opportunities.[81]

   Additionally, the level of data protection available to children based in different countries should be uniform. It has been seen that children in the Global South are not granted as rapid access to new and safer technologies as children in the

[78] J.C. Buitelaar, "Child's Best Interest and Informational Self Determination" What the GDPR can Learn from Children's Rights" Vol. 8(4) International Data Privacy Law (2018).
[79] Article 2, United Nations Convention on the Rights of the Child.
[80] Pedro Hartung, "The Children's Rights-by-Design Standard for Data Use by Tech Companies" Issue Brief No. 5 Good Governance of Children's Data Project (UNICEF) Page 5 (2020) available at https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf (accessed April 6, 2022).
[81] UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) page 19 available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (accessed April 6, 2022).
It has been found that AI used for assigning scores in criminal risk assessments have habitually recommended more severe sentences and lower likelihoods of parole for black children. *See*, Angwin, J. et al. (2016). "Machine Bias" ProPublica (2016) available at https://www.propublica.org/article/machine-bias-riskassessments-in-criminal-sentencing (accessed April 6, 2022).

European and North American countries.[82] This is also advocated for by the UNICEF / ITU Guidelines for Industry on Child Online Protection issued in 2015. It advocates that for states that lack the requisite legal framework for protection of children's right to privacy, data controllers should incorporate enhanced due diligence measures to ensure that policies and practices are in line with international law.[83]

b. ***Right against exploitation*** - Article 19 of the UNCRC guarantees children a right against "all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation including sexual abuse .... while in the [custody] of any other person who has the care of the child".[84] For data controllers this would mean not allowing for persistent identifiers that leads to unwarranted contact exposure to children leading to sexual abuse and ensuring safe transit of children's personal data.[85]

c. ***Right against economic exploitation*** - Article 32 of the UNCRC requires that children be protected against economic exploitation. This would include commercial exploitation by data controllers through monetising of personal data and its use for automated decision making, targeted advertising and profiling.[86]

d. ***Right to freedom of expression*** - As per article 13 of the CRC, a child is guaranteed the freedom to "seek, receive and impart information and ideas of all kinds, regardless of frontiers".[87] Article 17 further requires that children should have "access to information and material from a diversity of national and international sources".[88] The CRC takes cognisance of the fact that children are more vulnerable than adults. They are at a developmental stage where they are still discovering and deepening their identities.[89] In a data protection context, this would mean that data controllers should not create echo chambers and self

[82] Alana Institute, "Submission of comments on the draft of the General Comment on Children's Rights in relation to the Digital Environment" (2020) Page 4 available at https://www.ohchr.org/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/2020/others/alana-institute-2020-11-17.docx (accessed April 6, 2022).
[83] UNICEF and ITU, "Guidelines for Industry on Child Online Protection" (2015) page 11 available at https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf (accessed April 6, 2022).
[84] Article 19, United Nations Convention on the Rights of the Child.
[85] Pedro Hartung, "The Children's Rights-by-Design Standard for Data Use by Tech Companies" Issue Brief No. 5 Good Governance of Children's Data Project (UNICEF) Page 5 (2020) available at https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf (accessed April 6, 2022).
[86] UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) page 21 available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (accessed April 6, 2022).
[87] Article 13, United Nations Convention on the Rights of the Child.
[88] Article 17, United Nations Convention on the Rights of the Child.
[89] UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) page 21 available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (accessed April 6, 2022).

referential information bubbles.[90] Further they should also have the freedom to safely experiment with ideas without being subject to surveillance.[91]

e. ***Right to freedom of thought*** - The child's right to "freedom of thought, conscience and religion" would mean that data controllers should not use opaque nudge techniques and persuasive technologies that lead to behavioural modulation and manipulation.[92]

f. ***Right to rest and leisure*** - Article 31 of the CRC provides that the child has a right to rest and leisure and to engage in age appropriate play and recreational activities. In a digital environment, this would translate as the right to rest and disconnect. Nudge techniques should not pose barriers to the children's access to enjoyment of the outdoors and face to face interpersonal relationships which are pivotal to their development.[93]

The discussion in this section is helpful in understanding the foundational principles and rights that should underlie personal data governance of children by different jurisdictions. The next section considers the framework in different jurisdictions (most of which are signatories to the CRC, except the US).

[90] Pedro Hartung, "The Children's Rights-by-Design Standard for Data Use by Tech Companies" Issue Brief No. 5 Good Governance of Children's Data Project (UNICEF) Page 5 (2020) available at https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf (accessed April 6, 2022).

[91] UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) page 21 available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (accessed April 6, 2022).

[92] UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) page 21 available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (accessed April 6, 2022).

[93] Alana Institute, "Submission of comments on the draft of the General Comment on Children's Rights in relation to the Digital Environment" (2020) Page 6 available at https://www.ohchr.org/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/2020/others/alana-institute-2020-11-17.docx (accessed April 6, 2022).

III. *Regulatory framework for children's privacy in parallel jurisdictions*

The digital environment was not originally designed keeping in mind. However, it plays an increasingly significant role in children's lives. This is gaining recognition across jurisdictions. In trying to protect the informational privacy of children, States adopt varying regulatory models. This section undertakes an examination of some of the prominent jurisdictions in the field of children's data protection. Given that India is at the brink of its formulating its data protection law, it is useful to consider the experience of these jurisdictions.

(1) United States

The United States has a specific online privacy legislation provided for children, despite the absence of a generic federal privacy law. The rapid increase of the internet in the 1990s prompted the Federal Trade Commission to set forth principles that would apply to the information of young users collected by websites. These included the requirement of providing notice to parents, getting parental consent and purpose limitation.[94] Following this, a year later in 1998, the Children's Online Privacy Protection Act was introduced in the Senate. It proposed obtaining parental consent for processing children's data for children below 12, providing access to parents to their children's personal data, establishing and maintaining reasonable procedures relating to confidentiality, security, accuracy and an opt out mechanism for parents for controlling processing of children's data aged between 13 to 16.[95]

- ***Age of consent.*** The passed version of COPPA excluded the rule allowing parents to opt out from controlling processing of children's data aged between 13 to 16 because of concerns that this would reduce the privacy that teens deserve. Therefore, an individual below 13 years of age is considered a "child" as per COPPA.[96]

- ***Applicability.*** COPPA regulates online service providers that are "directed towards children". These can be either those "targeted to children" or where the online service providers have "actual knowledge" that it is processing personal information *from* a child.[97]

[94] Future of Privacy Forum, "The State of Play: Verifiable Parental Consent and COPPA" (2021) available at https://fpf.org/wp-content/uploads/2021/11/FPF-The-State-of-Play-Verifiable-Parental-Consent-and-COPPA.pdf (accessed April 6, 2022).
[95] Ariel Johnson, "13 Going on 30: An Exploration of Expanding COPPA's Privacy Protections to Everyone" (2019) available at https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1168&context=shlj (accessed April 6, 2022).
[96] Rule 312.2, Children's Online Privacy Protection Rule, 1998.
[97] The distinction of personal information being collected "from" a child, instead of "of" a child is an important qualifier to understand that laws relating to children's privacy are limited to dealing with information provided by the children themselves.

- *"Targeted towards children"* - A website is considered to be targeted towards children depending on an extrinsic examination of the site. Factors that go into its consideration include visual content, use of animated characters, music or other audio content that would attract children, presence of child celebrities or models who would appeal to children.[98]

  However, even in cases where the extrinsic examination makes a website seem as "targeted towards children", but does not target children as its primary audience ***and*** does not process personal information without appropriate consent (in this case parental consent), it will not be considered targeted towards children. This means that to be on the safe side, websites should have age screening mechanisms and not process any information if the user is below 13 years without parental notice and consent.

- *Actual knowledge* - A website that has actual knowledge that it is processing information of children cannot avoid liability on the grounds that the website was not directed towards children.[99] This extends to those online service providers also that are collecting personal information directly from users of another website. These would include providers of plug-ins, advertising networks and other third party service providers.[100] However, because the Rule does not define "actual knowledge", there is a high degree of uncertainty as to what this means.[101] The FTC provides limited informal guidance for this to mean websites that ask and receive information determining age of the user (age identifying questions). In case of third parties, actual knowledge may be deemed where ads or plug-ins are made available on child directed sites or the representative recognises child directed nature of the site.[102]

---

[98] Rule 312.2, Children's Online Privacy Protection Rule, 1998.

[99] United States of America v. Yelp Inc., Case No. 3:14-CV-4163 available at https://www.ftc.gov/system/files/documents/cases/140917yelpstip.pdf (accessed April 6, 2022).
In 2014, Yelp settled a children's privacy case with the FTC for violating COPPA. Yelp does not promote itself as a place for children and is not considered a website directed towards children. However, Yelp's mobile application, during registration, provided for an optional data field of providing date of birth. The FTC's case was that Yelp had therefore collected personal information on "several thousand individuals" who indicated that they were between 9 and 13 years old. Yelp settled the case with FTC for $450,000 and also agreed to make appropriate changes to its privacy policy to make it COPPA compliant. *See*, Adi Robertson, "Yelp Pays $450,000 in FTC Lawsuit After Letting Children Sign Up for Accounts" The Verge (2014) available at https://www.theverge.com/2014/9/18/6386231/yelp-pays-450000-in-ftc-lawsuit-after-letting-children-sign-up (last accessed April 6, 2022).

[100] Cynthia Larose, "Guide to Compliance with the Amended COPPA Rule" available at https://www.jdsupra.com/post/contentViewerEmbed.aspx?fid=f2e69fb4-a85a-4259-a0cc-7f53ec191dbb (last accessed April 6, 2022).

[101] John P. Feldman, "COPPA Update: Ask and Ye Shall Receive ..... Actual Knowledge" Reed Smith (2014) available at https://www.reedsmith.com/en/perspectives/2014/09/coppa-update-ask-and-ye-shall-receiveactual-knowle (last accessed April 6, 2022).

[102] FTC, "Children's Online Privacy Protection Rule: Not Just for Kids' Sites" available at https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-not-just-kids-sites#when (last accessed April 6, 2022).

There are also exceptions provided to the obtaining of verifiable parental consent. These include cases where the sole purpose of collecting contact information from the child is to respond to a child on a one time basis and where the information is not used to recontact the child, where the processing of children's information is to protect the information, when a persistent identifier is collected with the purpose of providing support to the internal operations of the website and does not collect any other personal information etc.[103] In practice, most of the child directed services interpret themselves to be under one of these exceptions that allows a one time use or multiple online contact with simply a notice to the parent (along with the opportunity to opt out) or email plus.[104]

An additional concern in the COPPA regulatory framework is that there is considerable confusion regarding websites that are considered to be directed towards children, general audience websites and mixed audience websites. First, general audience websites such as YouTube, Facebook and Google although not directed towards children under 13 are often in practice used by a substantive number of young children. These general audience websites can simply plead ignorance of the fact that they did not have "actual knowledge" that the users were below 13.[105] As a result, the young users are treated as adults and presented with the same information and privacy settings. Second, many general audience can have childish themes. For example, the Angry Birds app, while having child appealing, animated characters seems to meet the FTC's criteria for being directed at children, is in fact widely used by adults.[106] Mixed audience websites, even if not directed towards children primarily, are considered as "child directed" websites and have the same obligations under COPPA. Ex post facto determination by the FTC of which category the website falls into leads to regulatory uncertainty.

- ***Age verification.*** What follows from the above discussion on applicability is that there is no requirement as such under the COPPA Rule to institute age verification mechanisms. Websites either directed towards children below 13 or those that have actual knowledge of its users being below 13 have to comply

[103] Rule 312.5(3)(c), Children's Online Privacy Protection Rule, 1998.
[104] Macenaite and Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps" Vol. 26 (2) Information and Communications Technology Law (2017).
[105] Although the FTC has expanded the actual knowledge test to means of acquiring passive knowledge by operators such as responding to emails, age provided in feedback options, processing of facial data (in case of photo apps) etc it is easy for the website to prove that they did not have such knowledge by purposefully not engaging in monitoring.
[106] Paul Sawers, "Nielsen Reveals Most Popular Android Apps by Age. Angry Birds Appeals Most to over 35s", December 12, 2011 available at https://thenextweb.com/news/nielsen-reveals-most-popular-android-apps-by-age-angry-birds-appeals-most-to-over-35s#:~:text=It%20turns%20out%20that%20Android,the%20three%20age%2Dgroup%20demographics (last accessed April 6, 2022).

with COPPA. In both these situations there is no mandatory requirement for instituting age verification mechanisms.[107]

- ***Notice.*** There is a stringent requirement on the regulated websites to provide notice to the parent before obtaining verifiable parental consent. The Rule further provides that "reasonable efforts" as per the state of technological advancement to ensure that the parent receives a direct notice. Along with a direct notice, the website is also required to post a "prominent and clearly labelled link to an online notice of its information practices".[108]

- ***Verifiable parental consent.*** The Rule provides that an online service provider is required to obtain verifiable parental consent ***before*** processing personal data of children. Additionally, the parent must have the option to consent to their child's data processing without their own data being disclosed to third parties. It provides an illustrative list of these methods to include - consent form signed by the parent provided through email; undertaking monetary transaction (through online payment systems, debit and credit cards) such as to notify the primary account holder; toll free telephonic facilities, video conferencing with trained personnel and government IDs where the information of the parent is deleted after verification is complete.[109]

- ***Parents' right to review.*** A parent has been given the right to acquire from the website a description of the types or categories of personal information collected from their children. Further, a parent also has the right to withdraw consent and direct the website to delete the child's personal information. [110]

Being a specialised law for children's protection, enforcement actions under the COPPA Rule have been more than that in other jurisdictions. An analysis of around 29 orders of the FTC shows that barring 3 orders, all the orders pertained to unauthorised processing of children's personal data.[111] Children's personal data was either collected without obtaining parental consent or was collected even where consent was denied. A remarkable exception in these orders is FTC's order against YouTube. Unlike other cases that only dealt with unauthorised processing of children's personal data, the

[107] It is only in the limited circumstance where a website that extrinsically seems directed towards children but does not have children as its primary audience wants to be eligible for the exception, that it may screen the age of its users and not process their personal information.
[108] Rule 312.4, Children's Online Privacy Protection Rule, 1998. The Rule further provides the contents of different kinds of notices. This includes notice of collection of parent's information, that information of the child will not be processed without parental consent, the kinds of information that the online service provider intends to collect from the child, means for providing verifiable consent, means to delete such information etc.
[109] Rule 312.5, Children's Online Privacy Protection Rule, 1998.
[110] Rule 312.2, Children's Online Privacy Protection Rule, 1998.
The criticisms of the COPPA will be updated in the final draft of the working paper.
[111]

order in Youtube focused on behavioural advertising. This has been discussed later in the paper.

(2) European Union

Unlike the US, the EU does not have an independent law for children's privacy. Since 1995, children's data protection has been regulated under age generic data protection provisions. It was only with the newly adopted General Data Protection Regulation, 2016 that special provisions for children's data protection were incorporated.[112] Recital 38 of the GDPR states that children require specific protection for personal data processing as they may be less aware of the risks, consequences and safeguards available to them in this context.[113]

Article 6 of the GDPR provides that the interests or fundamental rights of a data subject will prevail over the legitimate interest of a data controller, particularly where the data subject is a child.[114] Unlike COPPA, since GDPR is mostly a principles based law, it sets out the regulations for children's data processing in very broad terms, leaving member States to fill in much of the details.

- ***Age of consent.*** Under Article 8, GDPR provides member states with a range to set the age of consent between 13 to 16 years of age. It needs to be noted that GDPR addresses the confusion that may arise in relation to providing a different age of consent in the data processing context from that of providing contractual capacity to consent. Therefore, it clearly specifies that the lowered age of providing consent for data processing would not affect the general contract of the member States.[115] The EPDB Guidelines on Consent further elaborate this. It states that the GDPR considers valid consent for the use of data of children as separate from national contract law. It further clarifies that article 8 on the age of consent is not applicable to the ability of a minor to conclude online contracts.[116] This establishes that the EU considers agreement for processing of personal data as a legal artefact different from a contract.

- ***Parental consent.*** One of the grounds for lawful processing of data is that it should be based on lawful processing. In the case of children, for lawful processing, consent must be taken from their parents or a person exercising parental responsibility over them. GDPR requires the data controller to make

[112] Directive of European Parliament on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 95/46/EC (1995).
[113] Recital 38, General Data Protection Regulation, 2016.
[114] Article 6, General Data Protection Regulation, 2016.
[115] Article 8(1), General Data Protection Regulation, 2016.
[116] European Data Protection Board, "Guidelines 05/2020 on Consent under Regulation 2016/679" (2020) Page 29 available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (last accessed April 6, 2022).

"reasonable efforts" taking into consideration the available technology, to verify that consent is given by a holder of parental responsibility over the child.[117]

- ***Information provisioning to minors.*** Article 12 of the GDPR provides that information and communication concerning processing of children's person should be made available in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" especially when that information is specifically addressed to a child.[118]

- ***Barring certain data processing practices.*** The GDPR does not bar any specific data processing practices specific to children. This is a deviation from the Council of Europe's "Guidelines to respect, protect and fulfil the rights of the child in the digital environment", issued in 2018. The Guidelines had recommended that profiling of children "which is any form of automated processing of personal data …. particularly in order to take decisions concerning the child or predict or analyse his or her personal preferences, behaviours and attitudes, should be prohibited by law."[119] This may have been excluded due to the overbroad nature of processing that it prohibits, thereby making beneficial processing also unlawful.

  It needs to be noted that although in the text of Article 22, GDPR there is no specific emphasis on children,[120] the accompanying recital mentions that the exceptions to automated decision making will not be applicable to children and as such they cannot be subject to automated decision making.[121] This means that profiling which feeds into a wider decision making process with a human element is not barred.

- ***Parents' right to review.*** The GDPR does not provide an explicit right to parents for accessing their child's data. It may, however, be interpreted as a requirement for exercising effective consent by parents on their children's data processing by individual DPAs. The right to access and rectification do not provide a distinction between child and adult data subjects.

- ***Right of erasure.*** The GDPR specifically provides that the data subject has the right to ask the data controller to erase their personal data without undue delay when a child has given the consent for data processing was taken under article 8(1). This means that if the data subject has consented to processing of his

[117] Article 8(2), General Data Protection Regulation, 2016.
[118] Article 12, General Data Protection Regulation, 2016.
[119] Council of Europe, "Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment" (2018) Page 12 available at https://rm.coe.int/guidelines-to-%20respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881albid (last accessed April 6, 2022).
[120] Article 22, General Data Protection Regulation, 2016.
[121] Recital 71, General Data Protection Regulation, 2016.

personal information (as an individual aged between 13-16 depending on the age of consent), they should be able to ask for erasure of that information even when they are no longer a child. This is provided for taking into account the fact that the child may not be fully aware of the risks involved in data processing.[122]

- ***Data protection impact assessments.*** The European Data Protection Board has included the criteria of processing of minors' data among the criteria to be taken into account to identify processing operations that may be subject to a data protection impact assessment.[123]

Since the EU provides a high level principle based framework, it is instructive to consider how these principles have been incorporated in domestic legislations of the Member States.

(a) France

The French Civil Code provides that everyone has a right to privacy. Its data protection is governed by the GDPR, and its domestic legislation – Information Technology, Data Files and Civil Liberties, 1978.[124]

- ***Age of consent.*** Pursuant to the age range provided under the GDPR i.e. 13-16 years, the Law on Information Technology and Freedoms sets the age of consent for personal data processing at 15.[125] Below this, a double consent mechanism is introduced whereby processing of personal data is lawful only if the consent is given *jointly* by the minor and the holder of parental authority.[126]

  While the age of majority (contractual capacity to consent) is still 18, the age of 15 was set to make the data protection law consistent with other legislations which provide that a 15 year old individual can request their doctor not to disclose medical information related to them.[127]

---

[122] Recital 66, General Data Protection Regulation, 2016.
[123] Article 35, General Data Protection Regulation, 2016. Although article 35 does not mention specifics, it is elaborated on by informal official guidance on the GDPR. See, GDPR.EU, "Data Protection Impact Assessments" available at https://gdpr.eu/data-protection-impact-assessment-template/ (last accessed April 6, 2022).
[124] Information Technology, Data Files and Civil Liberties, 1978.
[125] Article 45, Information Technology, Data Files and Civil Liberties, 1978, english translation available at https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf (accessed April 6, 2022).
[126] CNIL, "Submission to the UNSRP on the Subject of Privacy Rights of Minors" page 4 (2020). It is instructive to note that within the French framework there are three legal techniques that offer gradual autonomy to the minor. The first is an assistance scheme based on the idea of joint consent of the minor and their parents. The second is to allow for pre-majority thresholds in certain matters. For example, children can exclude parents from decision making power on matters that affects the child's intimacy. Third, is to allow for islands of capacity for children that enable the juvenile to learn to exercise their autonomy.
[127] Article 58, Information Technology, Data Files and Civil Liberties, 1978 english translation available at https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf (last accessed April 6, 2022). See, Points 2 and 3 of Article L. 1121-1 of the Code of Public Health.
Also see, Article 70, Information Technology, Data Files and Civil Liberties, 1978 english translation available at https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf (last accessed April 6, 2022).

- ***Obligations of data controllers.*** Further, the data controller is required that all information and communication made with the minor data subject is in a clear and plain language that the child can easily understand.[128] Additionally, even in cases where the personal data of children below the age of 15 is being processed (with the consent of their parent), the data controller still has to convey the requisite information to the child in "clear and easily accessible language".[129]

- ***Right of erasure.*** Information Technology, Data Files and Civil Liberties, 1978 provides the right to erasure exclusively for information collected by the data subject if at the time of collection the data subject was a child.[130] Further, the data controller has to take reasonable steps to inform the third party controller that the data subject has requested erasure.[131]

The CNIL also undertook two studies in 2020 on the issue to effectively understand the "uses, needs and expectations of all the actors concerned".[132] First, it conducted a survey of around 1,000 parents and 500 children between the ages of 10 to 17, to understand the digital practices of minors and the role of parents in minors accessing the internet. Second, after taking inputs from the survey, it conducted a public consultation on the issue of data protection of minors.[133] There were almost 700 responses to this consultation from children, digital companies and civil society groups. The exercise was concluded with the CNIL proposing eight recommendations for better protection of children's privacy. These recommendations have been referred to throughout the document, as and where required.

(b) Ireland

In Ireland, a new data protection legislation - the Data Protection Act, 2018 - was introduced to incorporate the GDPR in its data protection regime.

- ***Age of consent.*** The Data Protection Act, 2018 defines a child to be a person below the age of 18 years.[134] However, the age of consent to information

[128] Article 45, Information Technology, Data Files and Civil Liberties, 1978 english translation available at https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf (last accessed April 6, 2022).
[129] Article 48, Information Technology, Data Files and Civil Liberties, 1978 english translation available at https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf (last accessed April 6, 2022).
[130] Article 40, Information Technology, Data Files and Civil Liberties, 1978 english translation available at https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf (last accessed April 6, 2022).
[131] Article 51, Information Technology, Data Files and Civil Liberties, 1978 english translation available at https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf (last accessed April 6, 2022).
[132] CNIL, "Digital Rights of Minors: the CNIL Publishes the Results of the Survey and the Public Consultation" (2021) available at https://www.cnil.fr/fr/droits-numeriques-des-mineurs-la-cnil-publie-les-resultats-du-sondage-et-de-la-consultation-publique (last accessed April 6, 2022).
[133] CNIL, "Digital Rights of Minors: the CNIL Publishes the Results of the Survey and the Public Consultation" (2021) available at https://www.cnil.fr/fr/droits-numeriques-des-mineurs-la-cnil-publie-les-resultats-du-sondage-et-de-la-consultation-publique (last accessed April 6, 2022).
[134] Section 29, Data Protection Act, 2018 (Ireland).

society services has been fixed at 16 years,[135] in keeping with the GDPR age range. The Data Protection Commissioner has, however, pointed out that given the variation in cognitive development of children of the same age, it does not consider it appropriate to set a general age threshold as the point for when children should be able to exercise rights on their behalf.[136] Apart from age, it states that the data fiduciary should consider the maturity of the child (as demonstrated by interactions with it); the type of request made (erasure, modification, access, objection to processing); the context for the processing (medical, social media platform, learning platforms); the type of personal data at hand (photographs, medical data, contact details) and whether enabling the child to exercise these rights is in its best interests.[137]

- ***Right to be forgotten.*** A data subject who had consented to processing of his personal data as a child has the right to ask the data controller to erase their personal data.[138]

- ***Prohibition of certain data processing practices.*** The law prohibits companies and corporate bodies from processing personal data of a child i.e. an individual below the age of 18 years, for the purposes of direct marketing, profiling or microtargeting.[139] Doing so is considered an offence.

The Commissioner for Data Protection in Ireland recently undertook an extensive consultation on child privacy in 2021. It then published "14 Fundamentals" that organisations should incorporate in their data processing practices to enhance protections for children.[140]

(c) Other jurisdictions

In 2021, Germany amended the Protection of Young Persons Act, 2002 to provide increased protections to the youth in their interactions online.[141] Although the

[135] Section 31(1), Data Protection Act, 2018 (Ireland).
[136] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 33 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (last accessed April 6, 2022).
[137] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 34 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (last accessed April 6, 2022).
[138] Section 33, Data Protection Act, 2018 (Ireland).
[139] Section 30, Data Protection Act, 2018 (Ireland).
[140] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 34 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (last accessed April 6, 2022).
[141] Protection of Young Persons Act, 2002 (Germany).

amendment does not specifically focus on privacy and data protection, it introduces the concept of "provider prevention". This means that providers of internet services, with more than one million users in Germany, that are aimed at or used by children or adolescents will be required to put in place such measures that allow them to participate online in a "carefree manner". Providers will be required to install default settings which protect children from tracking and profiling.[142]

In Sweden, the Data Protection Authority censured the processing of biometric information of children to monitor attendance by schools.[143] The DPA held that the use of facial recognition for the purposes of attendance in school was in breach of the GDPR on three counts. First, it processed more personal data than was necessary for the specified purpose, second, attendance was not considered a valid reason for derogation from the biometric data, and third, the implementing authority did not conduct an impact assessment and prior consultation with the Swedish DPA.[144] The Swedish Government argued that the processing of facial data was lawful since it was based on the consent of guardians. However, the DPA did not agree with this argument. It held that in an educational context there exists "substantial imbalance" between the guardians and school authorities. There is a dependence on the school authorities for grades, student grants, student loans and education. Therefore, consent even if taken from the guardians, cannot be understood to have been valid.[145] As a result, the Swedish DPA imposed a fine to the tune of 375,000 euros on the Board of Education in the City of Stockholm.[146] In another case it pointed out that consent would have been a suitable basis for processing of facial data of children for non core activities such as creating electronic school catalogues and to document activities at preschools or schools.[147]

In Spain, the AEPD (Spanish DPA) imposed a fine of 10,000 euros on a data controller for incorrectly providing that the minimum age for obtaining valid consent for lawful

[142] Draft Second Act amending the Protection of Young Persons Act, 2002 (BT-Drs. 19/24909) english version available at https://perma.cc/4NUK-AASY (last accessed April 6, 2022).
[143] There was a similar enforcement action by the Swedish DPA against a school for running a pilot that used facial recognition to monitor the attendance of students. See, Swedish Data Protection Authority *Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 - facial recognition used to monitor the attendance of students* Page 5 (2019) available at https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf (last accessed April 6, 2022).
[144] Swedish Data Protection Authority *Supervision according to the EU Data Protection Regulation 2016/679 – against the Board of Education in the City of Stockholm* Page 5 (2019) available at https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-stockholms-stad.pdf (last accessed April 6, 2022).
[145] Swedish Data Protection Authority *Supervision according to the EU Data Protection Regulation 2016/679 – against the Board of Education in the City of Stockholm* Page 5 (2019) available at https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-stockholms-stad.pdf (last accessed April 6, 2022).
[146] Swedish Data Protection Authority *Supervision according to the EU Data Protection Regulation 2016/679 – against the Board of Education in the City of Stockholm* Page 5 (2019) available at https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-stockholms-stad.pdf (last accessed April 6, 2022).
[147] Swedish Data Protection Authority *Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 - facial recognition used to monitor the attendance of students* Page 4 (2019) available at https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf (last accessed April 6, 2022).

processing of personal data on subscription of the newsletter is 13 years of age.[148] Since the age of consent according to the Protection of Personal Data and Guarantee of Digital Rights Law, 2018 is 14 years of age, it was held that the data controller fell foul of the law.[149]

The Danish Data Protection Authority has passed important orders on issues involving children's privacy. The age for consent for personal data processing in Denmark has been set at 13 years of age.[150] In an order pertaining to Falck Danmark A / S, a data controller conducting health tests, it was found that although the data controller was compliant with the Danish law in disclosing its privacy policy it should ensure that the privacy policy is being effectively communicated to the parents.[151] In another case, it has held that a school cannot access a student's personal search history without the prior consent of parents.[152]

Its most recent order in 2021, was regarding the setting of G-Suite accounts by a municipality for schoolwork purposes without parental consent. Google had provided the Helsingor Municipality with Chromebooks that could be used by students on the creation of school accounts. When students' school accounts was created, data was retrieved from the school administration system that included the student's full name and the class they were in. Later, with the expansion of G-suite to include add ons such as Youtube, which allowed students to comment, it was found that posting comments on Youtube published the child's name and the school he studied in. It was held that the Helsingor Municipality fell foul of the GDPR because it did not seek parents' consent for such expansion in access on the G-Suite and did not conduct a data protection impact assessment for the resultant loss of confidentiality of students. It directed the municipality to contact the parents of registered children to carry out anonymisations or deletions of the registered personal data, as parents could not do so at their because the database from which the personal details of children were shared was with the school administration. It was further directed to not share personal data of students for supplementary programs without carrying out requisite data protection impact assessments. [153]

---

[148] AEPD - Sanctioning Procedure PS/00438/2019 available at https://www.aepd.es/es/documento/ps-00438-2019.pdf (last accessed April 6, 2022). *Also see*, GDPR Hub, AEPD – PS/00438/2019 available at https://gdprhub.eu/index.php?title=AEPD_-_PS/00438/2019 (last accessed April 6, 2022).

[149] Article 7, Protection of Personal Data and Guarantee of Digital Rights Law, 2018.

[150] Section 6(2), Danish Data Protection Act, 2018 english translation available at https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf (last accessed April 6, 2022).

[151] Datatilsynet Order number 2021-431-0142 available at https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/tilsyn-med-iagttagelse-af-oplysningspligten-ved-hurtigtest-i-grundskolen- (last accessed April 6, 2022).

[152] Datatilsynet Order number 2016-216-0569 available at https://www.datatilsynet.dk/afgoerelser/historiske-afgoerelser/2017/jan/kritik-af-skoles-gennemgang-af-elevers-soegehistorik (last accessed April 6, 2022).

[153] Datatilsynet Order number 2020-431-0061 available at https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/afgoerelse-vedroerende-brud-paa-persondatasikkerheden (last accessed April 6, 2022).

(3) United Kingdom

Following its exit from the EU, the UK gave effect to the UK GDPR to maintain continuity of data protection provisions domestically.[154] This is supplemented with the Data Protection Act, 2018.[155] The legislative approach of the UK to protect children's privacy is similar to those of GDPR jurisdictions.

- ***Age of consent.*** Section 9 of the Data Protection Act, 2018 provides that the age of consent for a child for personal data processing is 13 years of age.[156] However, "child" is defined as an individual below the age of 18 years.

- ***Obligation of data fiduciaries.*** The UK GDPR sets out the rights for data subjects in chapters III and IV. There is no distinction per se drawn between adult and child data subjects. Special consideration is given to children in case of provisioning of information.[157]

- ***Right to be forgotten.*** The UK GDPR provides children with the right to erasure the same as adults. The UK ICO states that this right is more likely to succeed in so far it is exercised for personal data given by the data subject when they were a child because there is an assumption that they gave this data without fully understanding the implications of doing so.[158]

- ***Age appropriate design code.*** The UK has issued an Age Appropriate Design Code under section 123 of the Data Protection Act, 2018.[159] Section 123 requires the ICO to prepare a code of practice that contains guidance on what is considered appropriate for age appropriate design of standards for the "relevant information society services which are likely to be accessed by children". In designing of this Code, it provides that the ICO should have consideration to the following principles:

[154] UK General Data Protection Regulation, 2018.
[155] Data Protection Act, 2018.
[156] Section 9, Data Protection Act, 2018.
[157] Article 12, UK GDPR, 2018.
[158] Article 17, UK GDPR, 2018. See, UK ICO, "How Does the Right to Erasure Apply to Children" available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/how-does-the-right-to-erasure-apply-to-children/ (last accessed April 6, 2022)
[159] Section 123, Data Protection Act, 2018.

- should be prepared in consultation with children, parents, representatives of children's interests, child development experts and trade associations[160]
- should have regard to the fact that children have different needs at different stages[161]
- defer to the UK's obligations under the CRC[162]

The Code came into force in September, 2020 and is required to be followed by data controllers from September, 2021. It sets out 15 interlinked standards of design that provide how data protection provisions are to be translated into practice by data controllers.

(4) Australia

In Australia, the Privacy Act, 1988 protects an individual's personal information.[163] The Privacy Act, 1988 does not distinguish between children and adults and does not grant any special data protection rights to children. A data controller processing the personal information of an individual under the age of 18, should make an assessment of the capacity of the individual based on the specific case. The approach of the Office of Australian Information Commissioner has been that where it is not practical for a data controller to undertake a case by case assessment, the data controller "may assume an individual over the age of 15 has capacity".[164] If the data controller is unsure that of whether the individual has capacity, it should not rely on the individual's consent for data processing but must consider a guardian for consent.[165]

Australia is considering the "Online Privacy Bill" to modernise the Privacy Act, 1988. It defines "child" to be an individual below the age of 18 years. It further provides that the Online Privacy Code developed under the law[166] should provide that regulated data controllers should take "all reasonable steps" to verify the age of individuals to whom it is providing an online service. Further, parental consent would be required for a child below 16 years of age before their personal data can be collected, used or disclosed.[167]

---

[160] Section 123(3)(a), Data Protection Act, 2018.
[161] Section 123(4)(a), Data Protection Act, 2018.
[162] Section 123(4)(b), Data Protection Act, 2018.
[163] Privacy Act, 1988 (Australia).
[164] Office of the Australian Information Commissioner, "Children and Young People" available at https://www.oaic.gov.au/privacy/your-privacy-rights/children-and-young-people (last accessed April 6, 2022).
Also see, Attorney General's Department, "Explanatory Paper, Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill, 2021 Page 10 available at https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-explanatory-paper.pdf (last accessed April 6, 2022).
[165] Office of the Australian Information Commissioner, "Consent to the Handling of Personal Information" available at https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information#AlertConsen (last accessed April 6, 2022).
[166] Section 26 KC, Online Privacy Bill, 2021 (Australia).
[167] Section 26 KC(6), Online Privacy Bill, 2021 (Australia).

(5) China

In 2019, China brought into effect "Provisions on the Cyber Protection of Children's Personal Information"[168] to "ensure children's personal information security and to promote healthy growth of children".[169] This along with the recently enacted Personal Information Protection Law, 2021 constitutes the regulatory framework for children's personal data.

Age of consent. Under article 28, the Personal Information Protection Law designates the personal data of minors under the age of 14 as "sensitive personal information".[170]

Regulated entities. The law applies to the processing of personal information of children below 14.[171] This means that the law will apply to every data fiduciary that processes children's data[172] unlike the US where such application is limited to online services "directed to children" or where the provider has "actual knowledge". There is, however, a carve out for such collection of information that is automatic in the network and which alone cannot be used to determine whether the information is related to a child.[173] This is possibly directed towards general audience websites that cannot identify or determine whether the information is related to a child without user registration and login to the website. However, for online service providers that host content which will likely attract children, it is arguable that the safe harbour provision would not apply.[174]

.

Parental consent. Article 31 provides that for processing the personal information of children below 14, consent of the parent will be required.[175]

---

[168] Provisions on the Cyber Protection of Children's Personal Information, 2019 (China) english translation available at https://www.managebac.com/files/Provisions-on-the-Cyber-Protection.pdf (last accessed April 6, 2022).
[169] Article 1, Cyber Protection of Children's Personal Information, 2019.
[170] Article 28, Personal Information Protection Law, 2021 english translation available at https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/mainland_law.html#8 (last accessed April 6, 2022).
[171] Article 2, Cyber Protection of Children's Personal Information, 2019.
[172] Article 3, Cyber Protection of Children's Personal Information, 2019.
[173] Article 28, Cyber Protection of Children's Personal Information, 2019.
[174] Gil Zhang and Kate Yin, "China has Released its Version of COPPA" (2019) available at https://iapp.org/news/a/china-has-released-its-version-of-coppa/#:~:text=China%20has%20finally%20released%20its,1 (last accessed April 6, 2022).
Yan Luo et. al., "CAC Releases Regulation on the Protection of Children's Personal Information Online" Vol. 31(10) Intellectual Property and Technology Law Journal available at https://www.cov.com/-/media/files/corporate/publications/2019/10/cac_releases_regulation_on_the_protection_of_childrens_personal_information_online.pdf (last accessed April 6, 2022).
[175] Article 31, Personal Information Protection Law, 2021.

Obligations on data fiduciaries. The Provisions on the Cyber Protection of Children's Personal Information do not seem to levy any additional measures for children's personal data as compared to generic data protection obligations. It only phrases these generic data protections as being applicable to children's personal. This is possibly because in 2019, the Personal Information Protection Law which otherwise provides for these generic data protection provisions in China had not come into effect, and the Provisions on the Cyber Protection of Children's Personal Information had to codify these specifically for children.

Restrictions on online activity. In 2021, China adopted the Law on the Protection of Minors. This introduced certain restrictions on the online activity of minors. These include prohibition on opening live broadcasting for children under 16, restriction of online gaming to one hour on the weekends and national holidays. It also recommends that social networking, gaming and online media entertainment be in "minor protection mode".[176] This restriction on online activity would have an incidental effect by reducing the volume of personal data generated by minors.

(6) Singapore

The Personal Data Protection Act, 2012 provides for a regulatory framework for data protection in Singapore.[177] There are no specific provisions regarding children's privacy. However, the Personal Data Protection Commission published the "Advisory Guidelines on the Personal Data Protection Act for Selected Topics" which provides guidance for the personal data protection of minors.[178]

Age of consent. The age of majority in Singapore is 21. The PDPC notes that ages at which minors may conduct different types of activity on their own varies across legislation. In the context of data protection, it observes, that there is no uniform age of consent that is made appliable. The PDPC also makes reference to the *Gillick* test which sets out that a minor may provide consent if they have sufficient understanding to fully understand what has been proposed. However, since the Gillick test has not been applied by the Courts in Singapore, it makes reference to the age provided for in various contemporaneous legislations. Considering the age provided for in employment statutes (for light work) and cinematography statutes (film and video classification ratings) is 13, it takes the view that 13 would be considered a suitable age

[176] Future of Privacy Forum, "The State of Play: Verifiable Parental Consent and COPPA" (2021) page 15 available at https://fpf.org/wp-content/uploads/2021/11/FPF-The-State-of-Play-Verifiable-Parental-Consent-and-COPPA.pdf (accessed April 6, 2022).
[177] Personal Data Protection Act, 2012 (Singapore).
[178] Personal Data Protection Commission, "Advisory Guidelines on the Personal Data Protection Act for Selected Topics" (2022) available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-PDPA-for-Selected-Topics-310322.ashx?la=en (last accessed April 6, 2022).

for considering that a minor has sufficient capacity.[179] It is important to highlight these considerations of the PDPC to shed light on the regulatory thinking that leads regulators to opt for a particular age of consent.

Even though the PDPC considers 13 to be an age of sufficient understanding, it does not adopt a bright line approach by specifying it as a blanket age for consent, like the COPPA. It maintains that while 13 may be the default age for age of consent, a data fiduciary has to take "appropriate steps to ensure that the minor can effectively give consent on his own behalf". If the data fiduciary has reason to believe that the minor does not have sufficient understanding then consent is to be obtained by the guardian.[180]

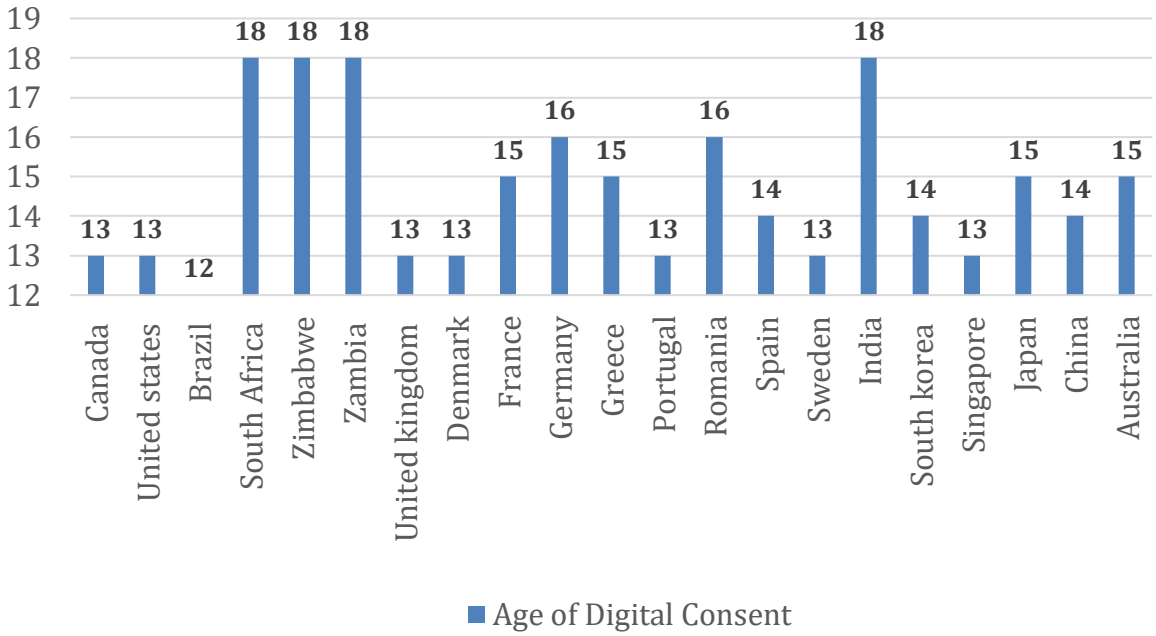
Obligations on data fiduciaries. The PDPA, 2012 does not provide any special provisions for personal data processing of children. The PDPC, in its guidance, states that data fiduciaries could consider taking extra steps while processing children's personal data. This includes taking extra care where relying on deemed consent of the child that the child has sufficient understanding, providing privacy policies in clear language, anonymising personal data before disclosure and taking extra steps to verify accuracy of personal data.[181] However, the reference to these are made in the nature of best practices rather than enforceable obligations.

A survey of some of the more prominent jurisdiction in children's data protection law shows that the regulatory enforcement is still at nascent stages.[182] Given that most jurisdictions are only now either retrofitting special provisions for child's informational privacy in their data protection laws or have only recently brought into effect their own data protection laws, the position of law on various aspects of this issue are still developing. Most legislations do not accord children's data with special protections apart from age verification and parental consent. In fact, one of the main perceptible differences in most jurisdictions for laws between data protection laws for adults and minors is only regarding the age of digital consent, and not their approach to its regulation. In that light we are left with the question of whether better enforcement of children's right to informational privacy requires a change in approach or would it be better achieved by strengthening enforcement of the present approach. Although we are too early in the regulatory journey to definitively comment on it, it is an interesting question considering the approach of data protection regulators. Even though

[179] Personal Data Protection Commission, "Advisory Guidelines on the Personal Data Protection Act for Selected Topics" (2022) page 54 available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-PDPA-for-Selected-Topics-310322.ashx?la=en (last accessed April 6, 2022).
[180] Personal Data Protection Commission, "Advisory Guidelines on the Personal Data Protection Act for Selected Topics" (2022) page 54 available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-PDPA-for-Selected-Topics-310322.ashx?la=en (last accessed April 6, 2022).
[181] Personal Data Protection Commission, "Advisory Guidelines on the Personal Data Protection Act for Selected Topics" (2022) page 54 available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-PDPA-for-Selected-Topics-310322.ashx?la=en (last accessed April 6, 2022).
[182] The jurisdictions of South Korea, Brazil, Canada and South Africa will be covered in the final draft of the working paper.

legislations do not provide for much nuance, data protection regulators of specific jurisdictions have invested considerable regulatory resources in trying to develop guidance for the industry to bring more clarity to the regulatory enforcement that can be expected on these issues. These exercises conducted by data protection regulators in UK, France and Ireland have been referred to in the subsequent sections. The next section will consider the Indian approach on the issue.

Table 1: Comparative age of digital consent across jurisdictions



IV. *Development of the law of children's privacy in India*

The issue of children's informational privacy in India has gained currency with the legislative journey of the Personal Data Protection Bill, 2019. Prior to 2018, the discourse on children's informational privacy was either limited to context specific legislations or often overshadowed by emphasis on other harms stemming from the digital environment possibly because they were perceived to be more immediate and impactful.

An instance of the first circumstance are legislations such as the Protection of Children from Sexual Offences Act, 2012 and the Juvenile Justice (Care and Protection of Children) Act, 2015. Both these legislations contain prohibit media reports from disclosing personal data of the child under protection of the law. This includes the child's name, address, photograph, family details, school, neighbourhood which can lead to the identification of the child.[183] Further, the law specifies the manner in which the trial and attendant proceedings should take place so that the identity of the concerned children is protected.[184] These privacy provisions are seen to be in furtherance of India's obligations under Article 16 of the Convention for the Rights of Child provides children the right to privacy.[185]

Courts have taken a serious view of this limited right to privacy and enforced it strictly.[186] One of the more significant cases in this regard is *Nipun Saxena and another* v. *Union of India and others*.[187] The question before the Court was how should the identity of children who are victims of social abuse should be protected. One of the submissions made before the Court was that the name and photograph of the victim should be permitted to be disclosed or published to use it as a rallying point to prevent other sexual offences. The Court held that this was not a valid reason for disclosure of identity, especially when the child concerned may not want to become a rallying point.[188] Further, on the question of who is to be considered the "next of kin" for allowing for disclosure of identity, the Court held that there could be cases where the "next of kin", such as even parents, may have interests different from that of the

[183] Section 23, Prevention of Children from Sexual Offences Act, 2012 and section 74, Juvenile Justice Act, 2015.
This is accompanied with a broader obligation under POCSO, 2012 on persons even other than those associated with the media such that "*no person* (emphasis added) shall... present comments... on *any child* (emphasis added) ... which may have effect of... infringing upon his privacy".
[184] Section 23(2), Prevention of Children from Sexual Offences Act, 2012.
[185] Gangadhar Narayan Nayak v. State of Karnataka, 2022 SCC OnLine SC 337.
[186] Bijoy v. State of West Bengal, 2017 SCC OnLine Cal 417; Subhash Chandra Rai v. State of Sikkim, 2018 SCC OnLine Sikk 29.
In *Sampurna Behura* v. *Union of India and others*, the Supreme Court prohibited the media from telecasting or broadcasting the images of children who were victims of sexual abuse even in blurred or morphed forms.
[187] Nipun Saxena and another v. Union of India and others, 2018 SCC OnLine SC 2772.
[188] Para 17, Nipun Saxena and another v. Union of India and others, 2018 SCC OnLine SC 2772.

victim.[189] The Court also recognises that the details that can be disclosed will be contextual in nature, depending on whether they can lead to the identification of the victim. It observes that when the child belongs to a small village, the disclosure of the name of the village itself can lead to identification of the child, as opposed to victims based in larger cities where further details such as colony and the area in which the child is living can lead to identification.[190] More importantly, it extends this right of privacy to deceased children also, thereby recognised a right to post mortem privacy.[191]

The protection of the child's right to privacy, in these limited contexts, did not however amplify to a more generic right to privacy in the digital environment. Discourse surrounding the harms resulting from children's interactions with the digital environment have focused on harms other than that of informational privacy.

In 2017, the "Blue Whale Challenge" brought the public's attention to the harms that online games were causing to children. Concerned about the encouragement of self-harm and suicide that the game was leading to, the issue was brought up in Parliament leading to a flurry of enforcement actions.[192] This was followed by the matter being taken up *suo motu* by the Madras High Court.[193] The directions of the Court were in relation to blocking illegal or harmful content, ensuring timely assistance intermediaries to law enforcement agencies and creating awareness.

Another child related issue before Courts with the increase in internet penetration has been the availability of child sexual abuse material online. The Supreme Court in *Re: Prajwala*[194] and *Kamlesh Vaswani* v. *Union of India*[195] issued directions to intermediaries to deploy filters, establish reporting mechanisms and proactively identify rogue sites that circulate such content. While these cases do relate to informational privacy to the extent that they make available the personal data of children without consent (of the guardian / child), that was not the issue that the Court was concerned with in these matters. Similarly, while reports flag the rising internet addiction among the youth, these more often than not do not refer to profiling and nudge techniques that are enabling factors in such addiction.[196] Most references to children, in *Puttaswamy (I)* also

[189] Para 18, Nipun Saxena and another v. Union of India and others, 2018 SCC OnLine SC 2772.
[190] Para 33, Nipun Saxena and another v. Union of India and others, 2018 SCC OnLine SC 2772.
[191] Para 34, Nipun Saxena and another v. Union of India and others, 2018 SCC OnLine SC 2772.
[192] Parliament of India, "Need to Discourage Youngsters from Playing Blue Whale Game: Ratna De" Matters under Rule 377 (December 19, 2017) available at https://eparlib.nic.in/handle/123456789/781007?view_type=browse (last accessed April 6, 2022); Ministry of Information and Technology, "Advisory on Blue Whale Game Challenge" (September 12, 2017) available at https://www.meity.gov.in/advisory-blue-whale-challenge-game; PTI, "Demand in Rajya Sabha against Online Games Like Blue Whale" (August 3, 2017) available at https://indianexpress.com/article/india/demand-in-rajya-sabha-against-online-games-like-blue-whale-4780459/ (last accessed April 6, 2022).
[193] Registrar (Judicial) v. The Secretary to Government, Union Ministry of Communications, 2017 SCC OnLine Mad 25298.
[194] In re: Prajwala Letter Dated 18.2.2015 Videos of Sexual Violence and Recommendations, 2018 SCC OnLine SC 389.
[195] Kamlesh Vaswani v. Union of India, 2016 SCC OnLine SC 860.
[196] Joseph et al., "Prevalence of Internet Addiction Among College Students in the Indian Setting: A Systematic Review and Meta Analysis" (2021) available at https://www.ijpn.in/article.asp?issn=2231-1505;year=2018;volume=15;issue=1;spage=61;epage=68;aulast=Maheshwari https://gpsych.bmj.com/content/34/4/e100496 (last accessed April 6, 2022).

were made in reference to the privacy of adults (parents) in matters of child bearing and paternity tests.

Even in 2019, an order of the Madras High Court, fails to sufficiently elude to the concept of children's privacy in the context of banning an application called TikTok.[197] A PIL was brought to ban TikTok for "containing degrading culture and encouraging pornography besides causing pedophiles (sic) and explicit disturbing content, social stigma and medical health issues between (sic) teens". The order of the Madras High Court focused on harms other than children's informational privacy, even as Tiktok had been fined to the tune of $5.7 million by the FTC, for violating children's informational privacy.[198] The kinds of harm for which the Madras High Court ordered an interim ban of Tiktok, without any reference to underlying privacy concerns, were risk of exposure of children to sexual predators, people being made subject of mockery which "would amount to violation of the privacy", addictive tendencies of Tiktok, "future of youngsters and mindset of the children being spoiled", "possibility of the children contacting strangers directly and luring them" and physical safety of individuals being endangered while making TikTok videos.[199]

Limited and indirect protection to children's privacy can be interpreted to be provided for in the recently notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[200] Rule 3(1) provides that a "significant social media intermediary" is required to inform its users to not "host, display, upload, modify, publish, transmit, store, update or share any information" that can be harmful to a child.[201] Since this is a provision directed towards the users of the significant social media intermediary, this is a provision that aims primarily at content regulation on these platforms. However, due to the lack of other legislative protection it may be used for the time being to protect children's informational privacy, in so far as the offending content violates it.

It is clear that the discourse on children's informational privacy is still at a very nascent stage in India, even as the concept of informational privacy generally as a fundamental right has become prominent in legal and policy circles. This section discusses the development of the law in India in relation to children's informational privacy to understand where the law currently stands and how it compares to the children's privacy frameworks in other jurisdictions.

Goel et. al., "A Study on the Prevalence of Internet Addiction and its Association with Psychopathology in Indian Adoloscents" Vol. 55(2) Indian Journal of Psychiatry (2013) available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3696236/ (last accessed April 6, 2022).

[197] S. Muthukumar v. Telecom Regulatory Authority of India, 2019 SCC OnLine Mad 24317.

[198] United States of America v. Musial.ly corp and others, Case no. 2:19-cv-1439 available at https://www.ftc.gov/system/files/documents/cases/musical.ly_proposed_order_ecf_2-27-19.pdf (last accessed April 6, 2022).

[199] Paras 5 and 6, S. Muthukumar v. Telecom Regulatory Authority of India, 2019 SCC OnLine Mad 24317.

[200] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

[201] Rule 3(1), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

(1) Information Technology Act and Rules thereunder

In India, children's informational privacy has been considered as an extension of the generic right to privacy and data protection. The Information Technology Act, 2000, (IT Act, 2000) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPD Rules, 2011) which currently determine the framework for data protection in India do not specifically refer to children's right to informational privacy. Instead, both the Act and the Rules adopt two broad models of data privacy. First, when the information is disclosed without the consent of the person and second, when the offending individual has come into possession of that information without

In the IT Act, 2000, section 72 lays down the penalty for "breach of confidentiality and privacy", and only protects privacy in a limited way. It provides that a person becomes liable to be punished if he has gained unauthorised access to any computer resource, in pursuance of the powers conferred under the Act, and discloses that information without the consent of the person concerned.[202] Second, section 72A provides for punishment for "disclosure of information in breach of a lawful contract". It provides that a person is liable to be punished if he discloses personal information that he has access to under a lawful contract without the consent of the person or such disclosure is in breach of the contract. It needs to be noted that both these provisions do not refer to "personal information" per se, and would include all kinds of information.[203] This framework has two implications on children's privacy. First, given that section 72A relies on "lawful contract", it would mean that a minor would require their legal guardian to execute the contract, and cannot exercise their right to privacy through themselves. Second, in relation to section 72, it leaves the question open whether consent under that section is different from valid consent under section 72A, such that a minor could also exercise his rights therein.[204]

The SPD Rules, 2011 are different from the IT Act, 2000 in that they lay specific emphasis on "personal information" rather than information simpliciter. Rule 3 while defining "personal information" includes information relating to certain fields, when that information is received under a "lawful contract or otherwise". However, in the subsequent rules, there is a dissonance as to the role of consent and lawful contracts in exercising the rights of informational privacy.[205]

[202] Section 72, Information Technology Act, 2000.
[203] Section 72A, Information Technology Act, 2000.
[204] An overview of cases showed that there have been no cases pertaining to child's personal information under these sections.
[205] Rule 3, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Rule 4 provides that body corporates should make available their privacy policy to persons who have provided their information under a "lawful contract". Rules 5 and 7 provide that consent of a person is required for collection and / or transfer of the personal information respectively.[206] As such, similar conceptual issues arise with respect to the SPD Rules, 2011 also i.e. whether consent is independent of the ability to lawfully contract. There is no general definition of consent under the Indian law. If the SPD Rules, 2011 are to be read harmoniously, it will imply that "consent" would probably be as defined under the Contract Act, 1872. In such a case, the legal guardians of these individuals would be providing contractual consent for the purposes of data collection, transfer or processing on their behalf.

The determination of whether consent is tied to contractual capacity is important to understand whether individuals below 18 years of age can exercise their rights of privacy themselves or through a legal guardian. As seen in the previous section, the capacity to give valid consent to online service providers in relation to data processing is not tied to contractual capacity in other jurisdictions.

(2) AP Shah Committee on Privacy and Data Protection

Apart from the extant regulatory framework, the thinking on privacy of children has been minimal in concurrent committee reports. The erstwhile Planning Commission had, in 2012, constituted a committee of experts under the chairmanship of Justice A.P. Shah to lay down principles for the framework of a Privacy Act. While the Report surveys data privacy regulatory frameworks in other jurisdictions it does not make a reference to child privacy specific legislations, such as the Children's Online Privacy Protection Act, 1988. The Report adopts "choice and consent", as one of the fundamental principles for privacy legislation.[207] The Report does not seem to make valid consent contingent on contractual capacity. This is further illustrated by the fact that in discussing the shortfalls of relying completely on consent, it mentions that "in executing the choice and consent principle", organisations should provide due care to more vulnerable categories such as the "poor, illiterate … children, differently abled citizens etc".[208] While the Report does not explicitly make this distinction, it can be presumed that it does not tie contractual capacity to being able to give valid consent for data processing.

[206] Rules 5 and 7, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[207] Group of Experts on Privacy, "Report of the Group of Experts on Privacy chaired by Justice A.P. Shah", Planning Commission of India page 22 (2012).
[208] Group of Experts on Privacy, "Report of the Group of Experts on Privacy chaired by Justice A.P. Shah", Planning Commission of India page 23 (2012).

(3) *Puttaswamy I*

The discourse on privacy made a definite move beyond contractual protections in the case of *Justice K.S. Puttaswamy* v. *Union of India*.[209] The Supreme Court recognised the right to informational privacy as a fundamental right under articles 19 and 21 of the Constitution of India. While leaving the scope of the right undefined so as to not unduly restrict its ambit, Justice Chandrachud's judgement observed that "privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy".[210]

Through the multiple opinions there are a number of observations which lead to the understanding that the right to privacy has a horizontal application against non-state actors as well. For instance, one of the arguments made by the respondent i.e. the Union of India, in this case was that the right to privacy should be considered a common law right, at best, and not a fundamental right guaranteed by the Constitution.[211] In his judgement, Bobde J., refutes this argument. Per him, the only difference between common law rights and fundamental rights is that while common law rights are enforceable against private entities, fundamental rights are enforceable against a state actor.[212] The content of the right can be exactly similar, only the incidence of the duty to respect that right and the forum in which the failure has to be addressed may differ. He held that a right could be both a common law right and fundamental right.[213] With respect to the right to privacy, he concludes

> *"Privacy has the nature of being both a common law right as well as a fundamental right. Its content, in both forms, is identical. All that differs is the incidence of burden and the forum for enforcement for each form."*[214]

Kaul J. lays down that the right to privacy is claimed *qua* the state and non state actors. For its enforcement against non-state actors, he opines that there is a need for legislative intervention by the State.[215] Chandrachud J. makes a similar observation. He concludes that information privacy, which is a facet of the right to privacy, faces dangers both from state and non-state actors and asks the government to put in place a robust data protection regime.[216]

---

[209] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[210] Para F, Part T, Page 263 (Chandrachud J.), Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[211] Para 11, Page 319 (Bobde J.), Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[212] Para 17, Page 325 (Bobde J.), Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[213] Para 18, Page 319 (Bobde J.), Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[214] Para 18, Page 319 (Bobde J.), Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[215] Para 12, Page 502 (Kaul J.), Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[216] Part T, Page 263 (Chandrachud J.), Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

These determinations about the nature of the right to privacy take it beyond the realm of just being exercisable under a valid contract. As pointed out by Sapre J., right to privacy is a natural right and inheres in every human being by birth.[217] This means that for an individual to exercise their right to privacy, their capacity to consent need not necessarily be tied with their contractual capacity to consent.

As the question before the Court was whether there was a right to privacy or not, the Court understandably did not go into the specifics of the formulation of the right. In relation to children's right to privacy, it is only Kaul J.'s judgement that makes a passing reference to it. He states that special protection will be required for protection of children's privacy, such that they should not be punished for the consequences of their "childish mistakes and naivety, their entire life".[218]

(4) *Puttaswamy II*

The Court had an opportunity to apply the principles laid down in *Puttaswamy (I)*, in relation to the Unique Identification Authority of India's data processing practices. The petitioners, in *Puttaswamy and others* v. *Union of India*, challenged the constitutionality of the Aadhaar Act, 2016. Since per *Puttaswamy I* the right to privacy had been established as a fundamental, one of the grounds for the constitutional challenge that the manner of collection, storage and transfer of demographic and biometric data violated this right in a number of ways.

In relation to the privacy of children specifically, the petitioners challenged the order of the Ministry of Human Resource Development, which made Aadhaar mandatory for gaining admission in schools and to avail scholarships.[219] The Court held that the right to education for children in the ages of 6 - 14, is a constitutional right, and availing it cannot be curtailed by the Aadhaar Act, 2016. the question of whether or not Aadhaar should be mandatory for children. In relation to the right to privacy it held that given that alternative means for enrolling in schools are available, the insistence on Aadhaar would not satisfy the test of proportionality.[220]

Since the Court lays down that enrolling with Aadhaar should be consent based, Sikri J. discusses the capacity of children to consent. He holds that making Aadhaar mandatory for children is disproportionate because "children are incapable of giving consent".[221] To support this assertion, references are made to the Indian Contract Act,

[217] Para 25, Page 487 (Sapre J.), Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[218] Para 66, Page 530 (Kaul J.), Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[219] Para 323, Page 392 (Sikri J.), Justice K.S. Puttaswamy v. Union of India, (2018) 1 SCC 809.
[220] Para 325, Page 394 (Sikri J.), Justice K.S. Puttaswamy v. Union of India, (2018) 1 SCC 809.
[221] Para 327, Page 395 (Sikri J.), Justice K.S. Puttaswamy v. Union of India, (2018) 1 SCC 809.

1872,[222] Banking Regulation Act, 1949[223] and the Insurance Act, 1938.[224] On the basis of these, it is held that since a minor is "not in a position to negotiate her rights", mandating Aadhaar would "lead to an inviable inroad into the fundamental rights under article 21". Incidentally, the judgement also makes reference to section 82 of the Indian Penal Code, 1860 which provides the age of valid consent for the purposes of the Code to be 12 years of age.

Based on the observation that there is absence of legal capacity for a child to give consent, it was held that to enrol children under the Aadhaar Act, 2016, the consent of the parent / guardian would be essential.[225] Additionally, on attaining majority, children who have been enrolled under the Act with parental consent, are required to be given an option to exit the Aadhaar system.[226] This holding is uniform across the three judgements rendered in *Puttaswamy II*.[227]

The implication of this case on the development of child privacy law is that, in the Indian context, it unequivocally equates consent in an informational privacy context, to the capacity of the individual to contract.

(5) Justice Srikrishna Committee Report and the Personal Data Protection Bill, 2019

Simultaneous to the *Puttaswamy* cases, the Ministry of Electronics and Information Technology (MeitY), in August 2017, constituted a Committee of Experts under the Chairmanship of Justice Srikrishna Committee (JSK Committee) to draft a model privacy law for India. The Committee released a White Paper on the data protection framework for India.[228] This was followed by a round of extensive stakeholder consultations. This process was culminated with the putting forth of the draft Personal Data Protection, 2018 along with the JSK Committee Report. Subsequently, MeitY after due consideration of the draft Bill, put forth the Personal Data Protection Bill, 2019 (PDP Bill, 2019). While there were some substantial differences between the proposed 2018 draft and the Bill laid down by the government in Lok Sabha, there is no perceptible difference in the clauses dealing with children's privacy. Therefore, the JSK Report and the PDP Bill, 2019 have been dealt with together.

---

[222] Section 11, Contract Act, 1872.
[223] Section 45ZA, Banking Regulation Act, 1949.
[224] Section 39, Insurance Act, 1938.
[225] Para 332(a), Page 401 (Sikri J.), Justice K.S. Puttaswamy v. Union of India, (2018) 1 SCC 809.
[226] Para 332(b), Page 401 (Sikri J.), Justice K.S. Puttaswamy v. Union of India, (2018) 1 SCC 809.
[227] Para 308, Page 1338 (Bhushan J.), Justice K.S. Puttaswamy v. Union of India, (2018) 1 SCC 809.
[228] Committee of Experts, "White Paper of the Committee of Experts on a Data Protection Framework for India" Ministry of Electronics and Information Technology (2017) available at https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf (last accessed April 6, 2022).

The JSK Report which was submitted in July 2018, discusses the issue of children's privacy at considerable length. Up until now, as shown above, the authoritative legal discourse on children's privacy was limited around children's capacity to consent to data processing. The JSK Report takes this discourse further by proposing a regulatory framework to safeguard children's privacy.

(a) Age of consent

On the issue of the age of consent, the JSK Report takes forward the position established in *Puttaswamy II*. The Committee succinctly states that the principle to be adhered to while determining the age of consent for data protection is "protecting the child from harm while ensuring that she can autonomously participate in her own development".[229] However, it determines the age of valid consent to be 18 with a view that since "the provision of consent for data sharing *is often intertwined (emphasis added)* with consent to contract", and therefore, should be compliant with the age of majority in the Contract Act, 1872.[230] It needs to be noted that it ties age of consent to the capacity of contract so strongly, that it posits that this age of consent could be reduced only if there is a similar reduction in the capacity of contract.[231]

There are two interconnected concerns that need to be highlighted. First, whether age of consent needs to be tied to contractual capacity of the individual. Second, the consequence of the age of consent being pegged at 18 as result of this typing up.

- **Tying the age of consent to contractual capacity**

Tying the age of consent for personal data processing to that of contractual capacity seems to be peculiar to India. The GDPR specifically distinguishes between consent for online contracts and consent for data processing.[232] It provides that the age of consent set by the member states for data processing in an online context will not affect the general contractual law of the countries. In all 27 member states of the EU, the age of majority is 18. A similar practice is also reflected in other jurisdictions of United States, Canada and Australia. In countries such as South Korea and Japan, where the age of majority is higher at 19 and 20 years respectively, the age to consent for personal data

[229] Committee of Experts under the Chairmanship of Justice Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (2018) page 43 available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last accessed April 6, 2022).
[230] Committee of Experts under the Chairmanship of Justice Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (2018) page 44 available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last accessed April 6, 2022).
[231] Although, to its credit, the Committee points out that this age may be too high from the perspective of the potential autonomous development of the child. See, Committee of Experts under the Chairmanship of Justice Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (2018) page 44 available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last accessed April 6, 2022).
[232] European Data Protection Board, "Guidelines 05/2020 on Consent under Regulation 2016/679" (2020) Page 29 available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (accessed April 6, 2022).

processing is 14 and 15 respectively.[233] In this light, the Committee's reason for tying the age of consent to contractual capacity being that "data sharing is often intertwined with consent to contract" may require reconsideration.

This peculiar approach of India is also problematic because it seems to reduce the fundamental right to privacy to a contractual protection. As pointed out above, *Puttaswamy (I)* had squarely taken out the concept of informational privacy beyond contractual protection of information, as provided for under the IT Act and Rules. It recognised that the right to privacy was a natural right, and in recognising it as a fundamental right, the Court held that it would be applicable against private entities (statutorily) as much as the State. But the JSK report, and the PDP Bill, 2019 subsequently, by relying on the *way* in such protection is generally exercised dilutes the nature of the right itself.

Additionally, it also seems to contradict the Committee's progressive understanding of the data fiduciary's obligations. India is the only country that operationalises the concept of fiduciary to strengthen data protection. The Committee's reason for doing so was that the relationship between an individual and the entities with whom data is being shared is based on a "fundamental expectation of trust".[234] It posits that "*notwithstanding any contractual relationship*, (emphasis added) an individual expects that her personal data will be used fairly, in a manner that fulfils her interest and is reasonably foreseeable".[235] For children the characterisation of the relationship of the individual and the data processing entity has two implications. First, it means that data protection obligations of the data fiduciary are not limited to contractual stipulations when it comes to protection of the interests of the data subject. This means that even if it is presumed that a minor has not understood the full implications of consenting to their personal data being processed, it cannot be processed in a manner that is inimical to the child's interests.[236] Second, fiduciary relationships between children and guardians (in this case data fiduciaries) are not based on the children's capacity to contract. Therefore, the argument for tying age of consent to contractual capacity because "data sharing is intertwined consent to contract" may not hold. This more so, when one considers the consequences of setting the age as high as 18.

[233] Article 22(6), Personal Information Protection Act, 2011 (Korea); Guidelines for the Protection of Personal Information Law, 2016 (Japan).
[234] Committee of Experts under the Chairmanship of Justice Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (2018) page 44 available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last accessed April 6, 2022).
[235] Committee of Experts under the Chairmanship of Justice Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (2018) page 8 available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last accessed April 6, 2022).
[236] Processing in accordance with a child's best interest is a well established standard.

- **Setting the age of consent at 18**

As a consequence of tying the age of consent to contractual capacity, the age of consent has been pegged at a relatively high age of 18. The Joint Parliamentary Committee received representations against this which have advocated that it may be reduced to either bring it in compliance with the US standard (13 years) or the GDPR standard (13-16 years).[237]

In 2015, when the GDPR was in its formation stages, the European Council had proposed the age of consent to be increased to 16 years from European Commission's suggested 13. This led to public outrage among various stakeholders such as children's rights activists, companies and children themselves. It was argued that if the age of consent was 16 it would effectively ban children from social media. The GDPR allowed for a compromise such that the age of consent was set between 13 to 16 years, with flexibility to member states.

The concerns that were raised during the GDPR formulation are relevant to understand why designating 18 as the age of consent may be counterproductive.[238] First, it was considered that providing for an age of consent which is not in touch with reality would encourage children to lie about their ages, often with the parents agreeing to such deception. This deception makes it difficult for online service providers to provide age appropriate guidance to children for a safe experience and results in lesser protections for children's personal data.[239] Second, it would lead online service providers to reduce their investment for products / service aimed at children, given that regulatory compliance with parental consent will lead to increased costs.[240] Third, youth, who are vulnerable, such as sexual minorities, those in abusive situations, will have even lesser opportunity to access the requisite information online.[241] Fourth, it will affect the development of critical thinking skills among children. Parents my refuse consent because they may not want to indulge the children's curiosity in areas such as religion and politics.[242]

---

[237] Joint Parliamentary Committee on the PDP Bill, 2019, "Report of the Joint Committee on the Personal Data Protection Bill, 2019" Lok Sabha Page 70 (2019) available at http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 (last accessed April 6, 2022). Also see, Team Inc42, "Joint Parliamentary Panel on PDP Bill Discuss Children's Privacy Rights" (2020) available at https://inc42.com/buzz/law-firm-raises-red-flag-over-pdp-bill-during-joint-parliamentary-panel-discussions/ (last accessed April 6, 2022).

[238] The concerns with parental consent outlined here are in context of the age of consent being pegged at 18. General concerns with parental consent, irrespective of the age of consent, have been outlined in a later section.

[239] https://medium.com/@janicerichardson/european-general-data-protection-regulation-draft-the-debate-8360e9ef5c1#.k5efblkx5

[240] https://www.zephoria.org/thoughts/archives/2015/12/18/europe-age.html

[241] https://medium.com/@janicerichardson/european-general-data-protection-regulation-draft-the-debate-8360e9ef5c1#.cq6w94jqb

[242] https://www.huffpost.com/entry/europe-could-kick-majorit_b_8774742

It needs to be noted that these concerns were also buttressed by the White Paper on Data Protection in the Indian context. The White Paper had pointed out that it would be difficult to keep children from accessing the internet, merely because the age of consent was set at 18.[243] It had also pointed that relying solely on parental consent to access internet till the child attains majority would "have a chilling effect on the child's opportunity to freely use the internet as a medium of self expression, growth and education".[244]

An additional problem of this approach is that it does not recognise "evolving capacity" of children.[245] The White Paper had pointed out that setting the age at 18 would ignore the fact that as a child becomes older, it gains maturity and capacity to understand the purposes for which their information may be used.[246] However, the PDP Bill, 2019 pegs the age of consent at 18. This treats children of various age groups under 18 homogenously. An adolescent is bestowed the same capacity as a toddler to make decisions about processing of their personal data.[247] Even though this is a criticism levied against almost all jurisdictions that use the bright line approach and set numeric age limits,[248] the problem is particularly serious in the Indian context because the age of consent is much higher at 18.

A model to consider is that of the UK where a child has been defined to be an individual under the age of 18 by the Data Protection Act, 2018 yet the age of consent has been set at 13. In Ireland, a similar model has been adopted. A child is an individual under the age of 18, but the age of consent for data processing is 16. This means that persons between the age of 13 / 16 to 18 will be considered capable to consent to personal data processing, ***and*** have specific protections that are available to children. This approach seems to account for their "evolving capacities" whereby they are given the right to consent which is exercised in the environment of enhanced privacy protections. Further, the UK ICO while providing guidance to companies on how to comply with the design features in its Age Appropriate Code, provides distinguishable

[243] Committee of Experts, "White Paper of the Committee of Experts on a Data Protection Framework for India" Ministry of Electronics and Information Technology Page 86 (2017) available at https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf (last accessed April 6, 2022).
[244] Committee of Experts, "White Paper of the Committee of Experts on a Data Protection Framework for India" Ministry of Electronics and Information Technology Page 86 (2017) available at https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf (last accessed April 6, 2022).
[245] Article 5, United Nations Convention on the Rights of the Child.
[246] Committee of Experts, "White Paper of the Committee of Experts on a Data Protection Framework for India" Ministry of Electronics and Information Technology Page 86 (2017) available at https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf (last accessed April 6, 2022).
[247] Nidhi Arora et al., "Ensuring Data Protection for Children under the Personal Data Protection Bill 2019 and on its Impact on the EdTech Sector and Online Businesses" (2021) available at https://www.mondaq.com/india/data-protection/1137092/ensuring-data-protection-for-children-under-the-personal-data-protection-bill-2019-and-its-impact-on-the-edtech-sector-and-online-businesses#:~:text=Restrictions%3A%20The%20PDP%20Bill%20prohibits,significant%20harm%20to%20a%20child (last accessed April 6, 2022).
[248] See, J.C. Buitelaar, "Child's Best Interest and Informational Self Determination" What the GDPR can Learn from Children's Rights", page 8, vol. 8(4) International Data Privacy Law (2018).

approach for compliance for different age groups. These are 0-5 years (pre literate and early literacy); 6-9 years (core primary school years); 10-12 years (transition years); 13-15 years (early teens) and 16-17 years (approaching adulthood).[249]

Even though not as granular, a similar approach that recognises evolving capabilities of children, has been recognised by the National Commission for Protection of Child Rights, in 2017, in its guidelines for children, parents and educators on how to ensure children's safety online. Three of the four guiding principles it recognises were:[250]

(a) To balance children's rights to learn, access information and privacy (best interests' principle)
(b) To provide an active role to children based on their evolving capacity and resourcefulness to promote online safety (participation of children in decision making)
(c) To develop "age appropriate" material should be served to the three age groups of 5-10 years, 11-14 years and 15-18 years (evolving capacities' principle)

Moreover, the White Paper had, in fact, advocated for developing a *Gillick* - like test to gauge the capacity of a child to understand the consequences of their actions. Civil society in India has also argued that when the law recognises this differing capacity in various contexts such as employment law[251] and criminal law,[252] there is no reason to not incorporate this in the data protection context.[253] Given that *Puttaswamy (I)* has pointed out that the right to privacy inheres in an individual from birth, legal capacity to delay exercise of that right to 18 years of age is arguably overprotective.

[249] UK ICO, "Age Appopriate Design: A Code of Practice for Online Services" (2020) 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/13-nudge-techniques/ (accessed April 6, 2022).
[250] National Commission for Protection of Child Rights, "Being Safe Online: Guideline for Raising Awareness Among Children, Parents, Educators and General Public" Page 13 (2017) available at https://www.ncpcr.gov.in/showfile.php?lang=1&level=1&&sublinkid=1637&lid=1661 (last accessed April 6, 2022).
The POCSO Guidelines also imbibe the "evolving capacity" principle. They provide that emphasis that the "older the child the more weightage should be given to the child's instructions". See, Ministry of Women and Child Development, "Model Guidelines under section 39 of the Protection of Children from Sexual Offences Act, 2012" (2013) Page 71 available at https://wcd.nic.in/sites/default/files/POCSO-ModelGuidelines.pdf (last accessed April 6, 2022).
[251] The Child Labour (Prohibition and Regulation) Act, 1986 recognises the concept of adolescents (age 14 - 18) and provides a graded approach of the sectors children of different age groups can engage in.
[252] Section 82 of the Indian Penal Code provides that a child below 7 years of age will not be culpable of any offence. Section 83 provides that a child between 7 – 12 years of age will be culpable depending on their understanding of the consequences of their Act. The Juvenile Justice Act, 2015 controversially allowed 16-18 year olds to be tried for heinous offences if it is determined that they had the maturity of understanding the consequences of their actions.
[253] Aparajita Bharti and Nikhil Iyer, "In Children We Must Trust" (2021) available at https://www.thehindubusinessline.com/blink/know/in-children-we-must-trust/article34018705.ece (last accessed April 6, 2022).

(b) Age verification and parental consent

Clause 16(2) of the PDP Bill, 2019 requires data fiduciaries to verify a minor's age and obtain parental consent ***before*** processing their personal data. Therefore, all data fiduciaries are required to put in place age verification mechanisms. The nature of these verification mechanisms will be specified by the DPA, after taking into account the volume of personal data processed, the proportion of such personal data which is likely to be that of the child, the possibility of harm arising out of the processing and any other factors that may be "prescribed". While the DPA is the regulating authority, allowing for additional factors for consideration to be "prescribed" gives the government also a say in the process. It needs to be considered the way in which clause 16(2) and (3) have been phrased the factors listed in clause 16(3) seem to pertain to only age verification. It needs to be considered that age verification and parental consent is a conjunctive exercise. Therefore, mechanisms for obtaining parental consent should also be designed keeping in mind these factors.

Given the kind of user friction and compliance costs that can arise from age verification mechanisms,[254] it is important that a risk based approach is followed in determining the nature and level of verification that online service providers are required to incorporate.

(i) Data fiduciaries that have to provide for age verification

A crucial difference between the Indian approach as compared to other jurisdictions is that it requires ***all*** data fiduciaries to have age verification and parental consent. This is unlike other jurisdictions where only a specified class of data fiduciaries is required to comply with these requirements. The COPPA Rule, in US, is made applicable to a certain class of online service i.e. those that provide services directed towards children or have actual knowledge that they are processing children's data.[255] Similarly, the GDPR under article 8 identifies this class as "information society services are offered directly to a child". "Directly offered" services have been interpreted by the UK ICO to mean services that are either not offered through an intermediary (such as a school) or

[254] Nidhi Arora et al., "Ensuring Data Protection for Children under the Personal Data Protection Bill 2019 and on its Impact on the EdTech Sector and Online Businesses" (2021) available at https://www.mondaq.com/india/data-protection/1137092/ensuring-data-protection-for-children-under-the-personal-data-protection-bill-2019-and-its-impact-on-the-edtech-sector-and-online-businesses#:~:text=Restrictions%3A%20The%20PDP%20Bill%20prohibits,significant%20harm%20to%20a%20child (last accessed April 6, 2022).
Rahul Matthan, "There's a Better Way to Protect the Online Privacy of Kids" (2021) available at https://www.livemint.com/opinion/columns/theres-a-better-way-to-protect-the-online-privacy-of-kids-11615306723478.html (last accessed April 6, 2022).

[255] The difference between the Indian approach and COPPA though is that while the former requires all data fiduciaries to be aware whether or not they are dealing with children's data through the institution of age verification measures, the latter does not depend on age verification measures to regulate the online service providers.

is made available to all age users or in case of age restrictions are made available to those below 18.[256]

It needs to be noted that requiring age verification by all data fiduciaries helps to avoid the "general audience / mixed audience v. child directed" websites confusion that has plagued the regulatory framework in the US. However, there may be scope for some ambiguity as to which data fiduciary will be a guardian data fiduciary depending on how well "directed at children" is defined. Therefore, there is a need to frame these regulations will sufficient clarity such that the scope for *ex post facto* determination and regulatory uncertainty is reduced.

(ii) Verify consent versus verifiable consent

Different standards for the consent to be obtained are provided for under the COPPA and the GDPR. While COPPA requires "verifiable consent" to be obtained by making reasonable efforts,[257] GDPR requires the data controller to make "reasonable efforts to verify". While COPPA specifies the means that may be used to provide consent, member states interpret "reasonable efforts" of the GDPR in relation to the "risk inherent in processing and the technology that is available".[258]

It needs to be noted that a distinction has been drawn between "verifiable consent" and consent that is verified.[259] The duty on the data controller to "verify" consent is a one time verification. "Verifiable consent" on the other hand, would refer to consent that should be amenable to re-verification (i.e. an ongoing possibility of re-verifying). Therefore, the burden on the data controller in the EU seems to be lower than that of those in the US. The Indian approach seems to follow the one in GDPR.

(iii) Reasonable efforts

The PDP Bill, 2019 does not provide a specific standard such as "reasonable efforts" to ensure that the individual consenting is the holder of parental responsibility over the child, apart from mentioning that it should be as "specified by regulations". It would be worthwhile to rethink whether these standards need to be specified in the text of the

[256] UK ICO, "Children and the GDPR" available at https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf (last accessed April 6, 2022).
[257] 312.2, Children's Online Privacy Protection Rule, 1998.
[258] The UK ICO illustrates this with an example. If an information society service is collecting the email id from a child only for the purposes of sending them content they have subscribed, then a simple self declaration would suffice as opposed to if the child is being allowed to post personal details on an unmonitored chat room, which would require more stringent ways of verifying consent. See, UK ICO, "Children and the GDPR" available at https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf (last accessed April 6, 2022).
[259] The original European Commission Proposal required parental consent to be verifiable. It stated that the "controller shall make reasonable efforts to obtain verifiable consent taking into consideration available technology". This was changed in the final text of the GDPR where it states that the "controller shall make reasonable efforts to verify that the consent is given by ..... holder of parental responsibility". See, Macenaite and Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps" Vol. 26 (2) Information and Communications Technology Law (2017).

legislation or delegated to the regulations. While defining the standard, care needs to be taken to supplement this with Codes of Practice developed with adequate industry consultation, such that the "reasonable efforts" is not left as a vague standard.[260]

Lastly, in specifying age verification mechanisms, the DPA should take care of certain design principles, which have been discussed in a later section.

(c)Obligations on data fiduciaries

The PDP Bill, 2019 adopts the regulatory approach proposed by the JSK Report. Keeping in mind that additional safeguards are required to ensure informational privacy for children, the Committee had proposed a two layer protection. The Committee creates a new subset of guardian data fiduciaries from the larger and more generic set of data fiduciaries. It then places a differential set of obligations on both these sets of data fiduciaries.

(i) Generic data fiduciaries

Clause 16 of the PDP Bill, 2019 provides that every data fiduciary is required to process the personal data of a child in such a manner that "protects the rights of, and is in the best interests of, the child". Additionally, before processing children's data, all data fiduciaries are required to take parental consent.

This means that while processing children's personal data, there are two main obligations on data fiduciaries. First to do so in a manner that protects the rights provided for under the PDP Bill, 2019 and second, to process it in a manner that protects the best interests of the child.

- **Rights of the child**

The PDP Bill, 2019 does not make any distinctions between the data protection rights of the child and adults (except, as discussed later, that certain data processing practices are barred for children). A child's personal data can be processed after obtaining valid parental consent. Similar to adults, a child has the right to confirmation and access, right to correction and erasure, right to data portability and the right to be forgotten. Similarly, the legal bases on which the child's personal data can be processed is also similar to that of adults.

[260] The Bavarian DPA has commented that developing mechanisms "it will be a great challenge both for the service providers to develop such practicable procedures and for the data protection supervisory authorities, to evaluate these procedures". See, Bavarian Data Protection Authority, "Information sheet for the implementation of the GDPR, No. 15" (2017) available at https://www.lda.bayern.de/media/baylda_ds-gvo_15_childs_consent.pdf (last accessed April 6, 2022).

- **Best interests**

The second obligation comes from India being a signatory to the CRC, thereby being legally obligated to ensure that the child's "best interests" are given primary consideration in all actions concerning the child. In the data protection context, taking from the UK ICO's perspective,[261] it can be argued that for the data fiduciaries to adhere to the requirement of "lawful processing" of personal data in the context of children, it would require to be in their "best interests".

Notably, the PDP Bill, 2019 does not define "best interests". It is well accepted that the child's best interest is determined on a case to case basis. Its application is responsive both to the context in which it is being applied (eg. family law, juvenile delinquency) and also to the individualised situation of the child in the same context. In fact, the flexibility of the standard has often led to the indeterminacy of the standard, which has at times, been considered to detract from its utility.[262] In a study undertaken of family law orders, it was concluded that even though "best interest" of the child is considered by the courts, the orders often do not give information regarding the factors to be considered in its determination.[263] Another study that analysed Supreme Court judgments from 1959 to 2000 concluded that in the absence of legislative guidance on what facts should be used assess a minor's best interests, the court has given varied interpretations based on their personal inclinations on what is best for the child, often leading to contradictory orders.[264]

Considering this, it is important to provide legislative guidance on factors that should be considered while determining the best interests of the child in the context of informational privacy. This, especially so, when the "protection versus" empowerment debate figures so prominently in governance of children's personal data. Although the principle of best interests is considered fundamental by many agencies,[265] they do not

[261] UK ICO, "Age Appropriate Design: a Code of Practice for Online Services" (2019) available at https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf (last accessed April 6, 2022).
[262] Law Commission of India, "Reforms in Guardianship and Custody Laws in India" Report No. 257 (2015) available at https://lawcommissionofindia.nic.in/reports/Report%20No.257%20Custody%20Laws.pdf (accessed April 6, 2022).
[263] Asha Bajpai, Custody and Guardianship of Children in India, Vol. 39(2) Family Law Quarterly (2005).
[264] Archana Parashar, Welfare of Child in Family Laws—India and Australia, 1(1) NALSAR Law Review (2003).
[265] Comment no. 25, Council of Europe Recommendations, UNICEF Manifesto, See, Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 19 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
In its Recommendation of the Council on Children in the Digital Environment, the Organisation for Economic Cooperation and Development lays down that the fundamental value that actors while engaging with children in the digital environment need to adhere to is to "uphold the child's best interest as a primary consideration". See, OECD, "Recommendation of the Council on Children in the Digital Environment" (May, 2021) available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389%20 (accessed April 6, 2022).

provide specific formulation of it in the digital environment.[266] In case the PDP Bill, 2019 does provide for a definition,[267] the DPA should undertake this exercise.[268]

(ii) Guardian data fiduciaries

The Committee proposes that data fiduciaries which either process large volumes of children's data or provide services or offer services directed towards children should be designated by the DPA as "guardian data fiduciaries". The PDP Bill, 2019 creates this separate class of data fiduciaries to impose "heightened obligations" given the greater scope of harm to children if personal data is processed by them.[269] In addition to the above mentioned obligations that all data fiduciaries have to comply with, guardian data fiduciaries are required to not indulge in certain kinds of data processing at all. Clause 16(5) provides that the guardian data fiduciaries "shall be barred from profiling, tracking or behaviourally monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child".[270]

Section 16 further allows for exemption or modification of this in special circumstances. First, it allows for those guardian data fiduciaries that provide "exclusive counselling or child protection services to a child" an exemption from requiring parental consent. Second, it provides for modification of the kinds of processing that are barred under 16(5), for "data fiduciary offering counselling or child protection services to a child". The rationale behind this seems to be to allow for beneficial processing of data that helps to identify children-at-risk. It needs to be noted that clause 16(6) uses the term "data fiduciaries" simpliciter, while providing that the kinds of data processing barred in clause 16(5) will be modified where counselling or child protection services are being provided to a child. However, clause 16(5) is applicable to guardian data fiduciaries and not "data fiduciaries", in general. Therefore, this provision requires a drafting correction.

---

[266] Only the UK ICO comes closest to defining it by specifying the rights that should be its constituents. It states that to meet the "best interest" standard for the child, data processors should take into account all the rights guaranteed to a child under the CRC such as safety (from sexual / commercial exploitation); health and wellbeing; developmental needs (physical, psychological and emotional, identity); freedom of expression; privacy and agency to form their own views and be heard. See, https://ico.org.uk/for-organisations/children-s-code-best-interests-framework/; UK ICO, "Age Appropriate Design: a Code of Practice for Online Services" (2019) available at https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf (last accessed April 6, 2022).

[267] Recent legislations in India do define what "best interests" are, even if the definition is generic in nature. See, section 2(9), Juvenile Justice Act, 2015 and section 2(uu), Goa Children's Act, 2003.

[268] In the case of POCSO Act, 2012 even though the legislation does not define "best interests", the Guidelines issued provide a succinct and contextual definition of what best interests under the Act would mean. See, See, Ministry of Women and Child Development, "Model Guidelines under section 39 of the Protection of Children from Sexual Offences Act, 2012" (2013) available at https://wcd.nic.in/sites/default/files/POCSO-ModelGuidelines.pdf (last accessed April 6, 2022).

[269] Committee of Experts under the Chairmanship of Justice Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (2018) page 45 available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last accessed April 6, 2022).

[270] Clause 16(5), Personal Data Protection Bill, 2019.

A more critical drafting issue arises with respect to the scope of processing that is prohibited. Concerns have been raised that the way in which clause 16(5) has been currently drafted leads to prohibition of all kinds of profiling, tracking, behaviour monitoring and targeted advertisements.[271] The scope of prohibition is not circumscribed by processing that can cause "significant harm" to children.

Most jurisdictions do not prohibit certain kinds of data processing specifically for children's personal data. For example, the COPPA does not specifically prohibit any kinds of data processing for children. In the European context, the Recommendations of the Council of Europe provided that automated processing of personal data which consisted of applying a profile to a child for predictive analysis should be prohibited. It provided that this restriction must be lifted if it is in the best interests of the child or in the case of overriding public interest.[272] However, the GDPR, did not incorporate this. It only provides a general prohibition on automated decision making, including profiling, if it can lead to significant consequences for the data fiduciaries.[273] In its adoption by member states, however, some differences have arisen. While some codify their approach in the data protection legislations, but rather occur at the level of the regulator's guidance notes to data fiduciaries. The Irish Data Protection Act, 2018 is probably the strictest in this regard. It makes profiling and micro targeting of children an offence.[274] But the guidance provided by the Irish DPC sates that its position is that data controllers should not profile children "unless they can clearly demonstrate how and why it is in the best interests of children to do so".[275] The UK ICO's stand is more accommodating to the concerns of the industry. In its Age Appropriate Code while recommending that privacy should be off by default, it specifies that it does not mean profiling is banned. Profiling is allowed where it is necessary for the core service that the child has requested and should place safely and fairly.[276]

This approach has been a cause of concern for the industry which argues that data processing such as profiling or tracking should be banned only if it is harmful for the child. The video game industry, for example, argues that profiling helps to improve

[271] Nidhi Arora et al., "Ensuring Data Protection for Children under the Personal Data Protection Bill 2019 and on its Impact on the EdTech Sector and Online Businesses" (2021) available at https://www.mondaq.com/india/data-protection/1137092/ensuring-data-protection-for-children-under-the-personal-data-protection-bill-2019-and-its-impact-on-the-edtech-sector-and-online-businesses#:~:text=Restrictions%3A%20The%20PDP%20Bill%20prohibits,significant%20harm%20to%20a%20child (last accessed April 6, 2022).
[272] Council of Europe, "Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment" European Union (2018) page 17 available at https://rm.coe.int/guidelines-to-%20respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881albid (last accessed April 6, 2022).
[273] Article 22, General Data Protection Regulation, 2016.
[274] Section 30, Data Protection Act, 2018 (Ireland).
[275] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 54 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
[276] Joint Parliamentary Committee on the PDP Bill, 2019, "Report of the Joint Committee on the Personal Data Protection Bill, 2019" Lok Sabha Page 73 (2019) available at http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 (last accessed April 6, 2022).

gaming experience by fixing those areas that prove problematic to progression or by remembering the content that was recently played.[277] Data generated by a player while playing is also used to identify software errors and improve features such as rewarding users.[278] These concerns are also reflected in the submissions that were made to the Joint Parliamentary Committee on the PDP Bill. The Committee states that one of the inputs it received from the stakeholders was that the bar on profiling, tracking etc should be linked to harm and there should not be a complete bar on all activities.[279] Stakeholders inputs asked for specific clarification for its application to educational institutions. These representations hold merit and a balanced approach should be developed with necessary stakeholder consultation.

(6) Joint Parliamentary Committee Report on PDP Bill, 2019

After the PDP Bill, 2019 was laid in the Lok Sabha in December, 2019, it was referred to a Joint Parliamentary Committee (JPC). The JPC submitted its report to the Parliament in December, 2021, after a period of deliberation of almost two years. It made detailed recommendations on various clauses of the PDP Bill, 2019. Its recommendations in relation to children's privacy, though made in good faith, which on balance seem to have an adverse impact on the regulatory framework of children's informational privacy. The JPC makes three main recommendations to clause 16 of the PDP Bill, 2019 which need to be considered in detail. First, it recommends the removal of the concept of "guardian data fiduciaries". Second, it recommends removal of the concept of "best interests of the child". Third, it recommends that a nomination mechanism be made available to children on turning 18.

(a) Removal of "guardian data fiduciaries"

The JPC is of the view that the only difference between an adult and child under the PDP Bill, 2019 is that a child needs a guardian to consent for their data processing. Based on this view, the JPC concludes that creation of guardian data fiduciaries as a separate class is not warranted. It believes that creation of this separate class will lead to dilution of the protections as other data fiduciaries who are not guardian data fiduciaries may violate the law. As such, it recommends that the concept of guardian

[277] FE, "The Information Commissioner's Public Consultation on the Code for Age Appropriate Design: ISFE Response" (2019) Page 6 available at https://ico.org.uk/media/about-the-ico/consultations/aadc/2616668/interactive-software-federation-of-europe-isef.pdf (last accessed April 6, 2022).
[278] ISFE, "The Information Commissioner's Public Consultation on the Code for Age Appropriate Design: ISFE Response" (2019) Page 7 available at https://ico.org.uk/media/about-the-ico/consultations/aadc/2616668/interactive-software-federation-of-europe-isef.pdf (last accessed April 6, 2022).
[279] Joint Parliamentary Committee on the PDP Bill, 2019, "Report of the Joint Committee on the Personal Data Protection Bill, 2019" Lok Sabha Page 70 (2019) available at http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 (last accessed April 6, 2022).

data fiduciaries be removed and all data fiduciaries should be bound by the data protection obligations under clause 16.[280]

This understanding of the JPC is arguably flawed on various levels. First, the difference between an adult and child under the PDP Bill, 2019 goes beyond the need for consent of a guardian. This is because for children's data, there are certain data processing practices that are specifically barred, which is not the case for data processing of adults. Second, the concern of the JPC that creating a distinction between guardian data fiduciaries and other data fiduciaries will lead to dilution of the law is also misplaced. The JSK Committee had created this distinction based on the volume of personal data of children being processed and whether or not these commercial websites are directed towards children to create a proportionate regulatory response. As detailed above, data fiduciaries identified as guardian data fiduciaries on these grounds were barred from carrying out certain types of data processing.

The unintended consequence of doing away with this distinction is that it leads to the age gating of the entire Internet. Although as per clause 16(2) of the PDP Bill, 2019 a data fiduciary is required to verify age and obtain parental consent ***before*** processing personal data of a child, the manner of verification is made dependent on a number of factors specified in clause 16(3) such as the possibility of harm arising to a child. This allowed for proportionate age verification and consent mechanisms. Because these are structures that generally result in user friction on one hand and increase costs of compliance on the other, it is important that these be proportionate to the harm they are aimed at preventing.[281] This means that a travel service providing data fiduciary could have a self declaratory age verification and parental consent mechanism as opposed to an edutech data fiduciary catering to children which would process a higher degree of personal data when continuously used by children. An important point to note here is that the design of age gating and parental consent, under the PDP Bill, 2019, is to be designed as per the harm that arises from p*rocessing of the data* rather than exposure to the content hosted by the data fiduciary.

However, with this distinction being removed, all data fiduciaries will be barred from carrying out data processing activities specified in clause 16(5) in relation to children's data. This would mean that there would be a higher burden placed on data fiduciaries to identify who is a child or not. The result of this would be that age verification and parental consent mechanisms would no longer be dependent on the harm being caused, but of a standard and verifiable nature. This would lead to increased friction in

[280] Joint Parliamentary Committee on the PDP Bill, 2019, "Report of the Joint Committee on the Personal Data Protection Bill, 2019" Lok Sabha Page 73 (2019) available at http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 (last accessed April 6, 2022).

[281] Increased user friction has been reported as a cause for significant rate of abandonment by digital companies. See, CNIL, "Digital Rights of Minors: the CNIL Publishes the Results of the Survey and the Public Consultation" (2021) available at https://www.cnil.fr/fr/droits-numeriques-des-mineurs-la-cnil-publie-les-resultats-du-sondage-et-de-la-consultation-publique (accessed April 6, 2022).

user experience without any corresponding benefit. The distinction was created by the JSK Committee to do away with this pitfall, and should be maintained.

(b) Removal of "best interests"

The opinion of the JPC is that since the entire PDP Bill, 2019 regulates data processing using a rights based approach, the clause for children's data protection should also use a similar rights based language. It further observes that phrases such as "best interests of the child" are "qualifying" in nature and would "dilute the purpose of the provision and give a leeway (sic) to the data fiduciary for manipulation".[282] Therefore, the JPC recommends clause 16(1) be reframed as "every data fiduciary shall process the personal data of a child in such a manner that protects the rights of the child".

This understanding of the JPC seems to stem from an ignorance of the legal concept of "best interest". As mentioned above, "best interests of the child", is a well recognised principle under the UN CRC. Article 3 of the UN CRC provides that "in all actions concerning children .... the best interests of the child shall be a primary consideration".[283] Given that India has adopted the UNCRC it is legally bound to provide for this principle in its regulatory structures.

More worryingly, by removing this, the PDP Bill, 2019 ends up protecting ***only the data protection rights.*** It eliminates the scheme of balancing rights apart from those relating to informational privacy. Given the potential of information, limiting interests arising out of it only to privacy is reductionist in nature. As mentioned above, a number of rights pertaining to access to information, freedom of speech and association and the right to safety have an important bearing on how children's information should be processed. Further, the understanding of limiting data privacy protections only to the rights provided for in the PDP Bill, 2019 runs against the philosophy of enshrining a duty of care on the data fiduciary, by the JSK Committee Report, such that the data fiduciary is required to give primacy to the interests of the data principal.

(c) Revalidation of consent on attaining majority

The JPC observes that it is important to provide children below the age of consent a mechanism to modify / renew / withdraw their consent for data processing after they have attained majority.[284] Accordingly, it recommends that three months before a child

[282] Joint Parliamentary Committee on the PDP Bill, 2019, "Report of the Joint Committee on the Personal Data Protection Bill, 2019" Lok Sabha Page 73 (2019) available at http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 (last accessed April 6, 2022).
[283] Article 3, United Nations Convention on the Rights of the Child.
[284] Joint Parliamentary Committee on the PDP Bill, 2019, "Report of the Joint Committee on the Personal Data Protection Bill, 2019" Lok Sabha Page 30 (2019) available at http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 (last accessed April 6, 2022).
[284] Article 3, United Nations Convention on the Rights of the Child.

attains majority, the data fiduciary should inform them for of the option of modifying / revalidating their consent. The JPC proposes that this be designed as an opt out mechanism such that there is no discontinuity in the service that the child is getting unless consent is withdrawn or given in a modified form.[285]

This is a progressive recommendation which recognises that children's consent can differ from that of their parents / guardians. By providing them an accessible option to exercise their consent, it leads to greater informational autonomy. A similar recommendation has been made by the Irish Data Protection Commissioner, discussed later.[286]

This section aimed at considering all facets of the proposed data protection framework in light of the principles of the CRC as also the experience in other jurisdictions. Granular comments have been given to various aspects of the framework. This principle based assessment of the law is followed by an assessment of regulatory solutions.

[285] Joint Parliamentary Committee on the PDP Bill, 2019, "Report of the Joint Committee on the Personal Data Protection Bill, 2019" Lok Sabha Page 31 (2019) available at http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 (last accessed April 6, 2022).
[285] Article 3, United Nations Convention on the Rights of the Child.
[286] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 61 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).

V. *Assessing proposed regulatory solutions for children's privacy*

A variety of regulatory solutions are being tried out in various jurisdictions - either through their incorporation in legislative instruments or as guidance from respective data protection authorities - to enhance children's privacy. These solutions can be divided into two broad categories depending on the actor on whom the responsibility is placed. The first category of solutions places the onus on the guardians to protect their children's privacy, while the second category of solutions follows a "child rights by design" approach, where increased responsibility is placed on the data controllers when they are processing children's data.

The first category refers to age verification and parental consent mechanisms, whereby the data controller is required to ascertain the age of the user and depending on that age should determine whether or not parental / guardian consent is to be sought. The liability of the data controller is limited to gaining valid consent of the parent / guardian. The second category of regulatory solutions are more onerous on the data controller. They require the data controller to provide for privacy protections that are specifically triggered once it is verified that the user is a minor, and go beyond parental consent.

Usually, most countries rely on a mix of these measures. This is evident in the Indian approach as well. The PDP Bill, 2019 requires age verification and parental consent, but additionally prohibits certain kinds of data processing of children's personal data. It is instructive to discuss the kinds and design of measures undertaken under both such categories.

(a) Age verification and parental consent

One of the earliest and most widely adopted regulatory solutions for children's privacy is the age verification and parental consent mechanism. Essentially, it means that data controllers should ascertain the age of the user, and if the user is underage as per the law of the specific jurisdiction, the data controller would have to seek the consent of the parent before proceeding with the processing of the child's personal data. The Irish DPC explains that the digital age of consent is not for determining whether a child should be able to access a service or not, but only whether a child can give their own consent for data processing by that service. It clarifies that age of consent in this context is not a measure to prevent access to certain websites or an online safety measure.[287]

[287] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 39 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-

There are two main levels of concerns that need to be outlined when it comes to age verification and parental consent. The first set of concerns are at a more principled level and will be discussed in this section. The second set of concerns emerge at an operational level, and are discussed in the next section in relation to the design principles that the DPA should keep in mind while laying down for these mechanisms in its regulations.

- ***Age of consent and verification***

Age verification in the context of data protection allows data controllers to gauge whether a person who is consenting to their personal data processing has sufficient capacity to do so. It is based on the assumption that there is an alignment between chronological age and behaviours. However, using a bright line approach and setting numeric age limits fails to take into account for the UNCRC mandated principle of "evolving capacities" of children which should be incorporated in governance structures.[288] It also follows an "all inclusive approach" and fails to take into account that children develop at different ages. This stems from different needs, capacities of the individual and differing national, historical, cultural and social heritage of the particular jurisdiction. Establishing a precise age limit, therefore, fails to take into account "multiple childhoods" and treats children in a homogeneous manner.[289] Moreover, different online services may carry significantly different risks to a child's privacy. Therefore, it has been suggested that different age limits should be specified for different data processing areas and practices.[290] These issues are enhanced in the Indian context where the age group of treating minors ineligible to provide consent is much higher (18 years of age) than those in comparable jurisdictions.

Regulators such as Singapore[291] and Ireland[292] seem to incorporate the principle of "evolving capacity". Although not provided in the legislation, guidance by regulators in both the jurisdictions emphasises that age alone cannot be the most appropriate benchmark to be taken into account while gauging the capability of a child. A legislation that does take into account differential capacities of children at the same age in the

Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).

[288] Article 5, United Nations Conventions on the Rights of the Child.

[289] Lina Jasmontaite and Paul De Hert, "The EU, Children under 13 years, and Parental Consent: a Human Rights Analysis of a new age based bright line for the protection of children on the internet" page 29 (2015) Vol. 5(1) International Data Privacy Law.

[290] Macenaite and Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps" Vol. 26 (2) Information and Communications Technology Law (2017).

[291] Personal Data Protection Commission, "Advisory Guidelines on the Personal Data Protection Act for Selected Topics" (2022) available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-PDPA-for-Selected-Topics-310322.ashx?la=en (last accessed April 6, 2022).

[292] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 39 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).

context of data protection is the Youth and Family Services Act, 2017 of Ontario. Part X of this Act regulates personal data protection of children in relation to certain welfare programs and services. The legislation recognises that individuals above the age of 16 can provide valid consent[293] to service providers for "collection, use or disclosure" of personal information. However, it makes two exceptions to this which recognised differing capacity of individuals. First, it recognises that an individual may be capable of providing consent for some parts of personal information and incapable for the other parts[294] as also capable at one time but incapable at another.[295] It further states that even in cases where the child is younger than 16, if the child is "capable", the child's decision to give, withhold or withdraw consent would prevail over a conflicting decision made by their guardian.[296] This can be applied in a converse manner also wherein children above the age of consent can still be considered to be not sufficiently equipped to consent to personal data processing. In 2012 i.e. pre-GDPR, in a decision by the Higher Regional Court of Hamm, it was held that it cannot be assumed that children between the ages of 15 – 18 cannot be understood to always possess the required capabilities to oversee the consequences of data processing.[297]

While the legislation in Ontario is a context specific legislation dealing with particular kinds of information, it is instructive to note that these principles can be imbibed for processing of children's personal data by data controllers in certain fields, even as compliance costs would prohibit incorporation of such granularity for the general universe of data controllers.

- ***Parental consent***

It is uncontested that children upto a certain age would require parental supervision when accessing products and services online. Parental controls are tools that allow parents / guardians to monitor and control children's online activity. While this assists the parent to fulfil their responsibility to promote the best interest of the child, after a certain maturity level in children it begins to impact the child's right to privacy as discussed earlier. Parental consent and consequent access to private online spaces can also hamper children's rights of freedom of speech and expression, access information and associate with others. Adolescents believe that having privacy and private spaces allowed them to explore ideas and develop independent views.[298]

[293] Section 301(1), Youth and Family Services Act, 2017.
[294] Section 300 (1), Youth and Family Services Act, 2017.
[295] Section 300 (2), Youth and Family Services Act, 2017.
[296] Section 300 (3), Youth and Family Services Act, 2017.
[297] Due to the existence of 19 different DPAs in Germany, and lack of published information, especially in English, this paper has relied on secondary sources for information on the German jurisdiction.
http://germanitlaw.com/european-data-protection-law-and-minors-no-legal-certainty/
The age of consent under the GDPR in Germany currently stands at 16.
[298] United Nations Special Rapporteur for Privacy, "Artificial Intelligence and Privacy, and Children's Privacy" Human Rights Council (2021) available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement (last accessed April 6, 2022).

There are also concerns that parental consent will result in differential access of internet for children. The consent being discussed here is in relation to processing of personal data of children. But instead of focusing of decisions such as the kind of cookies that should be allowed while the child is browsing the website, an examination of the privacy policy of the online service provider, selecting appropriate privacy settings, this decision is often morphed into deciding what kind of websites that children seek to access. And this is determined by a number of factors. Parental practices differ widely. Within the EU, it has been seen that parents in Scandinavian countries adopt a more liberal approach in the upbringing of their children compared to deeply religious communities such as those in Poland or Italy. Perceptions about the internet differ. While most countries in the EU consider it to be a service provided for money, some member states consider access to the internet as a human right.[299] Threat perceptions also shape up consent. It was seen that adults who have not faced online harms were, in fact, more likely to restrict information access.[300] Older people were more biased against the internet because of their perception of online harms affecting children.[301]

Moreover, the importance attached to parental consent also needs to be revisited considering its lack of effectiveness. The drawbacks of notice and consent framework also percolate to children's data protection.[302] Parents can routinely experience consent fatigue and provide consent to children's personal data being processed. Consent fatigue refers to a phenomenon when an overload of consent requests can make the consenting process a disturbing irritation rather than a serious choice thereby leading parents to consent to everything without discrimination of the child's best interests.[303] This is illustrated by the fact that while parents are concerned about their children's privacy their behaviour can often contradict their concerns. For example, though parents are concerned about their children's digital privacy, almost 81 percent knowingly let their children use Youtube's general audience interface without oversight and fewer than 1 in 3 activate parental control on their devices.[304]Cumulatively, both

[299] Lina Jasmontaite and Paul De Hert, "The EU, Children under 13 years, and Parental Consent: a Human Rights Analysis of a new age based bright line for the protection of children on the internet" page 30 (2015) Vol. 5(1) International Data Privacy Law.
[300] BT/DEMOS, "Online harms: a snapshot of public opinion" (2020) available at https://demos.co.uk/wp-content/uploads/2020/10/Online-Harms-A-Snapshot-of-Public-Opinion-1.pdf (last accessed April 6, 2022).
[301] BT/DEMOS, "Online harms: a snapshot of public opinion" page 10 (2020) available at https://demos.co.uk/wp-content/uploads/2020/10/Online-Harms-A-Snapshot-of-Public-Opinion-1.pdf (last accessed April 6, 2022).
[302] These drawbacks include power imbalances that limit individual's autonomy over their data, shaping of design and functionalities to advance business interests rather than protect individual's control over data, complex data processing practices that make consent ill informed, lack of viable alternatives and effective choice.
Also see, Rahul Matthan, "There's a Better Way to Protect the Online Privacy of Kids" (2021) available at https://www.livemint.com/opinion/columns/theres-a-better-way-to-protect-the-online-privacy-of-kids-11615306723478.html (last accessed April 6, 2022).
[303] Macenaite and Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps" Vol. 26 (2) Information and Communications Technology Law (2017).
[304] United Nations Special Rapporteur for Privacy, "Artificial Intelligence and Privacy, and Children's Privacy" Human Rights Council page 12 (2021) available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement (last accessed April 6, 2022).

these measures have a significant impact on informational privacy of both children and adults, freedom of speech and express and online anonymity.[305]

Parental consent is also out of touch with the reality of digital practices of children. Surveys have concluded that a majority of children access the internet without the supervision of their parents. In France, a survey conducted by CNIL showed that 82 percent of children aged 10 to 14 and 95 percent of children aged 15 to 17 go on the internet regularly without their parents.[306] Further, parents severely underestimate the frequency with which their children access the internet without supervision. This underestimation increases with increase in children's age.[307]

Lastly, the drawback of relying excessively on age verification and parental consent mechanisms is that it leads to mitigation of the responsibility of companies, in a manner that does not violate their best interests and rights.

(b) Child rights by design

To remedy this, UNICEF's Good Governance of Children's data Project proposes a "children's rights by design" standard (CRbD) should be incorporated in the products and services offered by digital providers to children.[308] One of the first documents that outlined this approach to provide a framework for information and communication technology providers is the ITU / UNICEF Guidelines for Industry on Child Online Protection. This is now incorporated in the approach of data protection regulators in various jurisdictions. The foremost, in this regard, has been the UK ICO which came out with the Age Appropriate Design Code. This was followed by the Irish Data Protection Commissioner's public consultation named "Fundamentals for a Child Oriented Approach to Data Processing". These consultations culminated in the laying down of 12 principles for data processing of children. Quite a few of these principles

[305] M Macenaite and Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps" Vol. 26 (2) Information and Communications Technology Law (2017).
[306] CNIL, "Digital Rights of Minors: the CNIL Publishes the Results of the Survey and the Public Consultation" (2021) available at https://www.cnil.fr/fr/droits-numeriques-des-mineurs-la-cnil-publie-les-resultats-du-sondage-et-de-la-consultation-publique (accessed April 6, 2022).
[307] It needs to be noted that the underestimation on parents' part was not as stark when it comes to children conducting online transactions. The gap between reality and parents' perception is lesser for online purchases made by children below 15 years of age.
See, CNIL, "Digital Rights of Minors: the CNIL Publishes the Results of the Survey and the Public Consultation" (2021) available at https://www.cnil.fr/fr/droits-numeriques-des-mineurs-la-cnil-publie-les-resultats-du-sondage-et-de-la-consultation-publique (accessed April 6, 2022).
[308] This line of thought has also gained currency in the academic circles. Hoofnagle claims that the real benefit of COPPA was not that it provided for parental consent but that it placed limitation on retention of personal data. Similarly, Montgomery argues that practices such as behavioral advertising, geolocation targeting, tracking across platforms should not be allowed even with parental consent. As early as 2011, Thierer had argued that ensuring regulatory enforcement against unfair and deceptive practices is more useful than expanding parental consent and age verification measures.
See, Chris J. Hoofnagle, "Federal Trade Commission Privacy Law and Policy" Cambridge University Press (2016) ('(t)he real privacy protection in COPPA comes from its non-consent-related provisions, such as limits on data collection, use and retention'). Kathryn C Montgomery and Jeff Chester, "Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework" 1(4) European Data Protection Law Review (2015); Adam D Thierer, 'Kids, Privacy, Free Speech & the Internet: Finding the Right Balance' (2011) available at http://ssrn.com/abstract=1909261 (last accessed April 6, 2022).

recommended the bettering of data processing designs specific to children's needs. Similarly, the French DPA also after holding extensive consultations on the issue, came out with 8 principles to be followed by data controllers for children's data processing that advocate for better design of these principles. The CNIL undertakes specific case studies of applications and highlights the different ways in which those applications are compliant with the GDPR.[309]

Apart from the GDPR, similar concerns have been raised in the US. Following the publication of the Age Appropriate Design Code by the UK ICO, three senators of the US wrote letters to online providers of children's products / services such as Activision, Walt Disney, Microsoft, Nintendo, Sony Corporation of America and Warner Bros. Entertainment, inquiring whether they proposed to carry out the changes in their data processing of children's personal data to comply with the UK's Age Appropriate Design Code. Further, they asked whether these changes will be implemented for users in the United States, and if so, then whether these changes will be reflected on a public facing website or in terms of service.[310]

The development of this approach can also be evidenced in the FTC's enforcement of the COPPA Rule in the US. In 2013, the COPPA underwent a significant amendment, whereby it expanded the scope of "personal information" to include "persistent identifiers" that can be used to identify users over time and across websites.[311] This was aimed towards preventing profiling of minor users. In one of its biggest enforcement actions against Youtube, the FTC imposed a fine of USD 170 million.[312] Youtube's settlement with FTC springboarded many changes to the design features of the platform. This included restricting several features on Youtube Kids including attention retaining features such as autoplay on home, comments, personalised advertising, notification bell, save to playlist and save to watch later, playback in the miniplayer; unsafe exposure features including live chat or live chat donations and commerce supporting features such as merchandise and ticketing and the donate button.[313] These kinds of design feature modifications are significantly different from earlier enforcement actions that focused mainly on requiring parental consent and providing parents with privacy notices.

---

[309] CNIL, "Case Studies" available at https://design.cnil.fr/en/case-studies/ (last accessed April 6, 2022).
[310] Lori Trahan, Kathy Castor and Edward J. Markley's Letters to Online Service Providers are available at https://trahan.house.gov/uploadedfiles/final_game_letters_-_combined.pdf (last accessed April 6, 2022).
[311] FTC, "Revised Children's Online Privacy Protection Rule Goes into Effect Today" (2013) available at https://www.ftc.gov/news-events/news/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect-today (last accessed April 6, 2022).
[312] FTC, "Google and Youtube will Pay Record $170 million for Alleged Violations of Children's Privacy Law" (2019) available at https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law (last accessed April 6, 2022).
[313] Youtube, "An Update on Kids and Data Protection on Youtube" (2019) available on https://blog.youtube/news-and-events/an-update-on-kids/ (last accessed April 6, 2022); Youtube Team, "Better Protecting Kids' Privacy on Youtube" 2020 available at https://blog.youtube/news-and-events/better-protecting-kids-privacy-on-YouTube/ (last accessed April 6, 2022).
Chris Hoffman, "Why Youtube Videos "Made for Kids have Restricted Features" 2020 available at https://www.howtogeek.com/545240/why-youtube-videos-made-for-kids-have-restricted-features/ (last accessed April 6, 2022).

Hartrung proposes that the CRbD can be incorporated at three stages of the product design. The first is at the stage of corporate decisions that are taken for the product, the second is concerned at the stage of designing of the product or service and the third is at the stage of functioning of the product.[314]

- **Governance principles**

Data controllers who own and manage the product have a duty to incorporate the "best interests" of the child in the policy decisions that are made regarding the product that processes their personal data. This obligation would be discharged by adhering to the following principles:

- Giving primacy to the "best interests" of the child in case there is a conflict between the best interests of the child and the commercial considerations of the data controller.[315]
- Adopting a well rounded interdisciplinary perspective on achieving these "best interests" which include children's opinion (article 12, UNCRC) and consultation with specialists such as psychologists, health care specialists, privacy experts etc.
- Universal adoption of standards across different jurisdictions such that the best policies and technologies available for children's rights are made available instead of jurisdictions only where such standards are mandated by law.
- Building in accountability measures to show that the data controller is following through on its own published terms, policies and community standards.
- Conducting data protection impact assessments before deployment of the product / service. This would include consultation with children and parents, assessment on the standards of necessity and proportionality of data processing, identification and assessment of risks and assessment of risk mitigation strategies.[316]

- **Design principles**

[314] Pedro Hartung, "The Children's Rights-by-Design Standard for Data Use by Tech Companies" Issue Brief No. 5 Good Governance of Children's Data Project (UNICEF) Page 7 (2020) available at https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf (last accessed April 6, 2022).
[315] UNICEF and ITU, "Guidelines for Industry on Child Online Protection" (2015) page 12 available at https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf (accessed April 6, 2022).
[316]Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 57 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022); UNICEF and ITU, "Guidelines for Industry on Child Online Protection" (2015) page 12 available at https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf (accessed April 6, 2022).

At the stage of development of the product, the product or service should customise generic data principles in a manner that the corresponding rights can be exercised by children in an effective manner. Further, the user experience should also be such that advances the "best interests" of the children. This is a standard that is higher than that provided under a typical notice and consent frameworks designed for adults. These design features include:

- ***High privacy default settings***

A principle that is common across data regulators is that when it comes to children, the default setting of the product or service should be privacy enhancing.[317] This is important because children may not always be aware of the privacy options that they have and would accept whatever the default settings are. A high privacy default setting would result in the following consequences for some common features of online products or services:

a. Data minimisation - A data controller should not process more personal data than is required to provide its core service. There should also be a reduction in the level of granularity of the data collected to avoid specificity and accuracy to limit the scope for profiling.[318] Moreover, the personal data should only be collected when the child is knowingly using an element of that service and the collection should stop once they are no longer using the service.[319] Further, data sharing with third parties and data retention should be extremely limited.[320]
b. Audience control - It would also allow the minor to exercise audience control such that their particulars should be shared with a limited audience by default and not an indefinite number of users of the online service.[321]

[317] UNICEF and ITU, "Guidelines for Industry on Child Online Protection" (2015) page 13 available at https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf (accessed April 6, 2022). Also see, CNIL, "Digital Rights of Children" (2021) available at https://www.cnil.fr/en/recommendation-8-provide-specific-safeguards-protect-interests-child (accessed April 6, 2022).
[318] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 60 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
[319] UK ICO, "Age Appopriate Design: A Code of Practice for Online Services" (2020) 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/12-profiling/ (accessed April 6, 2022).
[320] Recommendation 8 of the CNIL states that personal data of children should not be reused or passed on to third parties for commercial or advertising purposes unless it is being done so in the best interests of the child. See, CNIL, "Digital Rights of Children" (2021) available at https://www.cnil.fr/en/recommendation-8-provide-specific-safeguards-protect-interests-child (accessed April 6, 2022).
[321] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 60 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).

c. Profiling - Any features of the service, apart from core features, which require additional processing of data should be switched off by default.[322]
d. Device level processing - There should be an option, where possible, to process the child's personal data on the user device instead of transferring the data to the cloud by default.[323]
e. Maintenance of user specific privacy settings on the device - In case there are several users of a device, it is required that the privacy settings should be user specific so that children can benefit from enhanced default privacy settings.[324]
f. Collection of sensitive personal data - Sensitive personal data such as biometric data of children should not be collected.[325]

This principle should be incorporated in software updates such that the original privacy choices of the minor user are retained.

The Irish Data Protection Authority further recommends that the data controller through design should encourage privacy preserving behaviours. This would include push / just in time notifications to notify the child that there are more privacy protecting measures available than the action the child has chosen to undertake or on the consequences the choice made by the minor may have on their data protection.[326]

- ***Geolocation data***

The use of geolocation data is a cause for specific concern because it can lead to the child being exposed to physical harms such as abduction, trafficking and physical, mental and sexual abuse.[327] Apart from default high privacy settings for geolocation data, there are other considerations that need to be taken. First, the level of granularity

[322] UK ICO, "Age Appopriate Design: A Code of Practice for Online Services" (2020) 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/12-profiling/ (accessed April 6, 2022).
[323] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 60 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
[324] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 61 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
[325] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 61 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
[326] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 60 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
[327] UK ICO, "Age Appopriate Design: A Code of Practice for Online Services" (2020) 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/ (accessed April 6, 2022).

of geolocation that is required for the specific purpose needs to be considered. As far as possible, the level of accuracy should be reduced.[328] Further, the controls in relation to geolocation should be clearly specified and the child should be given periodic prompts to turn off the location sharing once the purpose for processing has been completed or automatically switch it off.[329] The design should be such that location tracking is not left on by mistake.[330]

- ***Children's control over their data***

Children should have easy access to online tools that allow them to exercise their data processing rights. This includes the right of access, rectification, erasure, objection to data processing, data portability and rights against automated decision making and profiling. The UK ICO recommends that some of the ways to make the tools more accessible are:

a. Making the tool prominent by having clearly and easily identifiable icons
b. Locating the tools in a manner that are easy to find
c. Making the tools age appropriate such that they are designed as per the ability of particular user age groups.
d. Mechanisms to make communication and tracking of the complaint with the data controller easier.

Another important facet for increasing control over data is to increase user choice.[331] This would mean that children are given more granular choice over the parts of the service they wish to use and collect data specific to those choices. Services should not be "bundled in" such that to access a service that requires a particular data set, the child would also have to provide other sets of data for services they do not wish to use. There should be a choice based mechanism on whether they wish to use their data for additional features of the service.[332]

---

[328] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 60 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).

[329] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 60 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).

[330] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/10-geolocation/

[331] DPA

[332] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/8-data-minimisation/

- ***Profiling***

Given the vast amounts of data that is processed, profiling is largely 'invisible' and it is difficult for children to understand how their personal data is being used and what are its consequences. While some profiling may be benign or be required for regulatory purposes (such as identifying whether the user is of age or is a vulnerable user and may require additional assistance) or for commercial reasons such as maximising user engagement and increasing attention retention on the platform. There are differing views on the profiling by the data regulators. The Irish DPC states that profiling is not allowed unless it can be shown to be in the best interests of the child.[333] The UK ICO clarifies that profiling is not banned, but that it should take place in a safe and fair manner. This is also adopted by the French CNIL.[334] Profiling should be subject to a privacy setting. Such profiling would include modification of design in the following ways:

- If a core service can be delivered without profiling, then a privacy setting should be provided for any additional features of the service that would require additional processing, ideally by default.
- There should be a privacy setting, by default, for behavioural advertising that are used to fund the service but do form part of the core service that a child wants to access. "Behavioural advertising" that is used for funding is not likely to come within the "legitimate interests" of the data controller, and would require an "opt in" mechanism for valid consent.
- There should be increased user choice as to what kind of purposes they want to submit their data for profiling for. Catch all phrases such "providing personalised services", "enhancing user experience" or "improving service delivery" should not be used.

Further, age appropriate prompts can be designed if the data controller has reason to believe that given the age of the child and the nature of profiling, the risk of processing is high, for adult supervision to be sought while consenting to the processing. If on the basis of such profiling, the data controller recommends content, it has to ensure that these recommendations are age appropriate. This is because the data controller has a higher responsibility since it is his processing that has led to such content

[333] Also see, OECD, "OECD Guidelines for Digital Service Providers" (2021) available at https://www.oecd.org/mcm/OECD%20Guidelines%20for%20Digital%20Service%20Providers.pdf (accessed April 6, 2022)
[334] https://www.cnil.fr/en/recommendation-8-provide-specific-safeguards-protect-interests-child

recommendations as opposed to when the child has proactively sought age inappropriate content.

More pernicious outcomes of persistent identifiers is that they could facilitate non authorised and malicious contact. Therefore, it is important to maintain safety standards when profiling takes place.[335]

- ***Nudge techniques***

Nudge techniques are design features that encourage users to opt for certain choices that the data controller would want them to make. These techniques include highlighting one option over the other through the use of colours;[336] employing more clicks to reach one option than another; slowing down the process for exercising one option over the other;[337] using pop ups that encourage acceptance of more intrusive privacy settings[338] and thinly veiled advertising strategies such as non-transparent influencer marketing and product placement.[339]

For children, nudge techniques should not be used to lead them to make decisions that hoodwink them into opting for reduced privacy protections. In fact, positive nudging should be used to encourage privacy enhancing options for children, support their health and well being by making it easier to take breaks or quit a platform (providing for pause and save buttons). The UK ICO provides a break up of different age ranges and recommendations to provide guidance as to what would be considered an appropriate nudge for the specific age range.

- ***Transparency***

In 2018, in a study conducted by the BBC assessing the language used in the Terms and Conditions of Use and privacy policies of 16 frequently used applications by young

[335] Pedro Hartung, "The Children's Rights-by-Design Standard for Data Use by Tech Companies" Issue Brief No. 5 Good Governance of Children's Data Project (UNICEF) Page 7 (2020) available at https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf (last accessed April 6, 2022).
[336] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 28 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
[337] UK ICO, "Age Appopriate Design: A Code of Practice for Online Services" (2020) 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/ (accessed April 6, 2022).
[338] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 28 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
[339] Pedro Hartung, "The Children's Rights-by-Design Standard for Data Use by Tech Companies" Issue Brief No. 5 Good Governance of Children's Data Project (UNICEF) Page 7 (2020) available at https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf (last accessed April 6, 2022).

people, it was found that the reading level required to understand was that of a university student.[340] Provisioning of information in a manner that is accessible to children has been advocated by multiple authorities.[341] The Guidelines on Rights of the Child by the Council of Europe require that children should be provided privacy related information in an easily accessible, meaningful, child friendly and age appropriate manner.[342]

The data controller should provide information in an accessible, layered and child friendly and age appropriate manner.[343] This would include measures such as translating privacy policies into different languages, constant and easy access to privacy policies by displaying them at a prominent place and just in time notices.[344] The understanding of the privacy policies can be assisted through audio visual cues such as graphic representation, gamified or interactive content, icons and symbols that aid children's understanding, prompts telling children to take help from adults and explanation of the consequences of change from the default high privacy settings.[345] The use of these aides by the data controller should be modified depending on the age of the user. The Irish DPC further recommends that children and young people should have an opportunity to directly ask organisations questions they have about their data through instant chat, dedicated email addresses or privacy dashboards.[346]

In a case involving a data controller which conducted health tests for students, the Danish DPA held that it was not sufficient that the data controller had hosted its privacy policy in different ways such as physical copies, digital versions, communication

---

[340] CNIL, "Submission to the UNSRP on the Subject of Privacy Rights of Minors" page 4 (2020).
[341] OECD, "OECD Guidelines for Digital Service Providers" (2021) available at https://www.oecd.org/mcm/OECD%20Guidelines%20for%20Digital%20Service%20Providers.pdf (last accessed April 6, 2022). Also see, UNICEF and ITU, "Guidelines for Industry on Child Online Protection" (2015) page 9 available at https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf (accessed April 6, 2022).
[342] Council of Europe, "Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment" European Union (2018) page 17 available at https://rm.coe.int/guidelines-to-%20respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881albid (last accessed April 6, 2022).
CETS 223 – Automatic Processing of Personal Data (Amending Protocol),
[343] Datatilsynet Order number 2021-431-0142 Para 3.1 available at https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/tilsyn-med-iagttagelse-af-oplysningspligten-ved-hurtigtest-i-grundskolen- (last accessed April 6, 2022).
[344] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 29 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
[345] UK ICO, "Age Appopriate Design: A Code of Practice for Online Services" (2020) 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/ (accessed April 6, 2022).
See, Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 28 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
[346] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 29 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).

through schools and relevant municipalities and text messages to registered mobile numbers. It was also the responsibility of the data controller that schools are taking effective steps to disseminate he privacy policy to parents.[347]

- ***Parental controls***

Parental controls should be designed in a manner that respects the privacy of the child. One way to do this is to ensure that children are aware that they are being tracked or monitored by their parents.[348] They should have age appropriate information about how this works and could affect their privacy.[349] This would include providing audio or video materials to inform the child that their parents are being told what they do online to keep them safe and icons that provide a clear and obvious sign when tracking has been activated. As children grow, this can be supplemented with resources for parents to explain to their children their right to privacy.[350] Additionally, consent fatigue on the part of parents / guardians should also be kept in mind. This means that privacy tools such as parental dashboards should provide parents with a more accessible overview of the children's activity and relevant settings for their privacy.[351] This dashboard should also allow parents to intervene and modify in a secure manner their child's privacy settings especially where sensitive information such as location, biometrics or device sensors are involved.[352]

- ***Revalidating consent on attaining majority***

When an individual who has used the product / service as a child attains majority, they should be allowed an opportunity to re-consent to their data processing. This would be

[347] 3.2 https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/tilsyn-med-iagttagelse-af-oplysningspligten-ved-hurtigtest-i-grundskolen-

[348] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 61 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).

[349] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 7 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf
Also see, UNICEF and ITU, "Guidelines for Industry on Child Online Protection" (2015) page 13 available at https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf (accessed April 6, 2022).

[350] UK ICO, "Age Appopriate Design: A Code of Practice for Online Services" (2020) 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/ (accessed April 6, 2022).

[351] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 61 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).

[352] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 61 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (last accessed April 6, 2022).

more privacy and choice enhancing rather than automatically migrating the details to a new account with privacy protections for adults. In the Indian context, this has been recommended by the JPC on the PDP Bill, 2019.[353]

At this time of renewal of consent, the individual should be apprised of the modified protections that would be made applicable as per the adult status of the account. This would include new purposes for which data can be processed, changes in retention, data sharing and storage policies and deactivation of parental consent.[354]

- ***Continual monitoring of functioning of the product***

After the product / service has been deployed, there needs to be continuous monitoring of its compliance with privacy measures for children. This would include conducting data audits, resolving privacy complaints expeditiously[355] and conducting consultations and data protection impact assessments when modifying existing design features.

A study of the approach of various regulators along with the advocacy of these principles by framework documents goes on to show that data protection for children cannot be the responsibility of parents alone. The design of services and products matter significantly in the achievement of best interests of the child.

[353] Joint Parliamentary Committee on the PDP Bill, 2019, "Report of the Joint Committee on the Personal Data Protection Bill, 2019" Lok Sabha Page 31 (2019) available at http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 (last accessed April 6, 2022).
[354] Office of the Data Protection Commissioner, "Children Front and Centre: Fundamentals for a Child Oriented Approach to Data Processing (Draft Version for Public Consultation)" page 61 (2021) available at https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf (accessed April 6, 2022).
[355] UNICEF and ITU, "Guidelines for Industry on Child Online Protection" (2015) page 12 available at https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf (accessed April 6, 2022).

VI. *Roadmap for the government and the DPA*

An assessment of the provisions of India along with the experience of data protection regulations for children in other jurisdictions, has provided sufficient context to gauge next steps for India's proposed DPA. The JPC has recommended that the provisions of the PDP Bill, 2019 be given full effect to within two years of its enactment.[356] Given that it is expected that it will be passed before the end of this year (2022), the government and the regulator have their work cut out for them. As seen in the previous sections, solutions to children's privacy are not easy to come by. Jurisdictions such as the US (which have had a children privacy law for almost two decades now) and the EU (which has been engaging in this issue since 2009)[357] are yet to come up with fool proof ways of protecting child privacy. More importantly, India cannot just look to these jurisdictions and transplant their solutions, given its experience with the digital environment and privacy are remarkably different from those in these jurisdictions.

As per the PDP Bill, 2019, there are four ways in which the regulatory approach to the issue of children's personal data can be developed. These are divided between the government and the regulator:

a. Rules made under the Act – Clause 16(3)(d) gives the central government the power to prescribe rules for factors that may be considered while designing the age verification.[358]
b. Regulations made under the Act – Clause 16(2) and (3) give the Authority the power to specify the manner in which parental consent will be obtained and age verification mechanisms will be designed respectively.[359] Additionally, clause 16(4) allows the Authority to classify by regulations
c. Codes of Practice – Clause 50(6)(h) gives Authority the power to specify codes of practice to promote good practices of data protection and facilitate compliance with the obligations of Act in relation to regulation of personal data of children.[360]
d. Power to undertake research – Under clause 49, the Authority has the power to undertake research in the field of data protection.[361]

[356] Joint Parliamentary Committee on the PDP Bill, 2019, "Report of the Joint Committee on the Personal Data Protection Bill, 2019" Lok Sabha Page 28 (2019) available at http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 (last accessed April 6, 2022).
[357] Article 29 Data Protection Working Party, "Working Document 1/2008 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools) (2008) available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf (accessed April 6, 2022).
[358] Clause 16, Personal Data Protection Bill, 2018.
[359] Clause 16, Personal Data Protection Bill, 2018.
[360] Clause 50, Personal Data Protection Bill, 2018.
[361] Clause 49, Personal Data Protection Bill, 2018.

Considering the powers and the mandate of the Authority and the government, the areas on which the regulatory approach should focus on for children's data protection can be categorised into two. The first would include those areas which the PDP Bill, 2019 requires the government and regulator to formulate rules and regulations on. These are the first two issues in the list below. The issues for the second category have been culled keeping in mind the experiences of other jurisdictions. Deliberation of a regulatory approach on these would help the Authority to formulate a more effective data protection regime for children.

1. ***Age verification and parental consent mechanisms***

Developing credible age verification mechanisms are still a work in progress.[362] Self verification mechanisms, for example by asking the user to provide their date of birth or by way of self declaration, can be easily circumvented. Other ways include peer based mechanisms along with self verification. These methods can be circumvented by creating multiple profiles.[363] In developing reliable alternatives to these methods there is a need to keep certain design principles in mind.

- ***Ease of access.*** Age verification mechanisms should be designed keeping in mind ease of access. This means that age verification mechanisms should not result in exclusion of young people in accessing online services, simply because of the way in which they require age to be proved. For example, if an age verification mechanism requires the parent or guardian to make a nominal payment to the data controller via a bank transaction, an appropriate alternate method of verification should be provided to ensure that there is no undue discriminatory treatment to person who do not have a bank account.[364]

- ***Data minimisation.*** Second, age verification in itself leads to processing of more personal data. The design of age verification mechanisms needs to balance the requirements of providing for reliable proof of age with that of data minimisation. That this balance may not always be maintained is illustrated by a decision of the German Federal Court of Justice. In 2007, a matter came up before the Court on age verification mechanisms required for accessing pornographic websites. The age verification mechanism in question required entering national ID or passport number / name, address and credit card or bank account information and paying a minor amount was considered insufficient. It

[362] Jim Waterson, "UK Drops Plans for Online Pornography Age Verification System" (2019) available at https://www.theguardian.com/culture/2019/oct/16/uk-drops-plans-for-online-pornography-age-verification-system (accessed April 6, 2022). In 2019, UK abandoned its proposed nation wide age verification mechanism to access online pornography in the face of privacy concerns and demonstrations that the age verification mechanism could be easily sidestepped. These concerns remained despite considerable investment of time and money in developing these products.
[363] Macenaite and Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps" Vol. 26 (2) Information and Communications Technology Law (2017).
[364] European Data Protection Board, "Guidelines 05/2020 on Consent under Regulation 2016/679" (2020) Page 28 available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (accessed April 6, 2022).

was observed that these are not effective entry barriers because children could easily duplicate these details. The court suggested alternative verification mechanisms which included identification with a USB stick and a pin code for every login, webcam or biometric features recognition or online identification in accordance with the German Money Laundering Act (via PostIdent).[365] A case can be made that these kinds of requirements to prove age were possibly prescribed because of the risk of harm in question. However, it in fact points out to an additional concern that needs to be factored - that of parental privacy. The DPA should be mindful of the kinds of parental information it can asked to be collected to verify a parent's identity for parental consent.[366]

One of the ways to minimise data collection is that instead of requiring the exact age of the child to be verified, it could be sufficient to ascertain whether the data subject belongs to the age group that requires parental consent. Other ways include use of attribute based schemes instead of verifying the fully identify of the person, cross check only particular attributes to allow access to the internet.[367] In India, with the data protection law still developing, stakeholders have voiced their concern for guidance on how the data processed for age verification should be used or disposed.[368]

- ***Proportionality.*** The concern for increased data processing is compounded when age verification is required to be conducted for all kinds of data processing irrespective of the risk. Therefore, the third principle that is required to be followed is that these age verification mechanisms should be proportional to the actual risk that the resultant data processing may pose. As such, the standard to be followed for these should be risk and context specific.[369] This view is also subscribed to by the European Data Protection Board guidelines on consent. It provides that in low risk cases, verification of parental responsibility may be carried out via email, while in cases of high risk, more proof may be asked for. This principle is also important for the industry.[370] The French Data Protection Authority has made a case for imbibing the principle of "proportionality" to verify the age in relation to the "intended purposes, public targeted, data processed, technologies available and the level of risk associated with the processing."[371] As per a survey of the CNIL on children privacy, digital companies favoured a risk based

[365] BGH, Oct. 18, 2007, docket no. I ZR 102/05. This information is based on the English translation of the press release of the judgement, available here http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=41423&linked=pm The judgement is German is available here http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=43444&linked=urt&Blank=1&file=dokument.pdf
[366] Lina Jasmontaite and Paul De Hert, "The EU, Children under 13 years, and Parental Consent: a Human Rights Analysis of a new age based bright line for the protection of children on the internet" page 29 (2015) Vol. 5(1) International Data Privacy Law.
[367] Macenaite and Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps" Vol. 26 (2) Information and Communications Technology Law (2017).
[368] Prasid Banerjee, "Minor's Privacy Rights need a Graded Approach" (2021) available at https://www.livemint.com/technology/tech-news/minors-privacy-rights-need-a-graded-approach-experts-11614962672828.html last accessed April 6, 2022).
[369] Macenaite and Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps" Vol. 26 (2) Information and Communications Technology Law (2017).
[370] Nash et al., "Effective Age Verification Techniques: Lessons to be Learnt from the Online Gambling Industry" (2015) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2658038 (last accessed April 6, 2022).
[371] CNIL, "Submission to the UNSRP on the Subject of Privacy Rights of Minors" page 4 (2020).

approach for designing age verification and parental consent mechanisms. They advocated that "the level of protection remains proportionate to the risks". This is because a significant rate of abandonment was observed when age gating solutions such as entering credit card number or provisioning of an identity document was incorporated in their user interface.[372] This consideration is done away with if the recommendation of the JPC on doing away with the concept of guardian data fiduciaries is done away with in the PDP Bill, 2019.

- ***Development of certified methods.*** Fourth, there is a lack of age assurance standards, tools and industry certification schemes, thereby creating uncertainty for data controllers on the standards they should comply with to avoid liability. An important facet in vetting ways to verify age would be take inputs from the industry. The FTC in the US has cooperated continuously with the industry to establish a number of acceptable methods for attaining parental consent. It also allows the industry to submit new mechanisms for approval to the FTC. This encourages development of new consent verification that are effective and also acceptable to the industry.[373] For example, in 2013, the FTC based on an industry representation allowed for the use of knowledge based authentication. This verification method is based on asking questions that cannot be answered simply by having access to the wallet of person (such as credit card details). The adoption of a co-regulatory model in the US allows the industry to propose implementable and effective solutions which can then be approved by the regulator. The Indian DPA could use Codes of Conduct and use market driven tools for the enforcement of its provisions. This co-regulatory model / Codes of Conduct should, however, be cognisant of not creating entry barriers for newer players and start-ups.

2. Classification of data fiduciaries as guardian data fiduciaries

The DPA has to classify data fiduciaries as guardian data fiduciaries depending on whether they operate commercial websites / services "directed at children" or process large volumes of personal data of children. In light of the JPC recommendations, it is still unclear whether this concept will be carried in the final formulation of law. In case the concept does not survive, it will be useful to require "guardian data fiduciaries" to comply with the obligations of significant data fiduciaries considering the "risk of harm by processing by the data fiduciary".[374] As a significant data fiduciary, these data fiduciaries will be required to conduct data protection impact assessments.[375] As seen

[372]CNIL, "Digital Rights of Minors: the CNIL Publishes the Results of the Survey and the Public Consultation" (2021) available at https://www.cnil.fr/fr/droits-numeriques-des-mineurs-la-cnil-publie-les-resultats-du-sondage-et-de-la-consultation-publique (last accessed April 6, 2022).
[373] Macenaite and Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps" Vol. 26 (2) Information and Communications Technology Law (2017).
[374] Section 26(1)(d), Personal Data Protection Bill, 2019.
[375] Clause 27, Personal Data Protection Bill, 2019.

in the previous section, data protection regulators are increasingly favouring the need for data fiduciaries to conduct data protection impact assessment so that they can assess the risk and accordingly modify design features and data processing practices. Additional obligations of significant data fiduciaries such as maintenance of records, conducting data audits and appointing a data protection officer may be made applicable on erstwhile guardian data fiduciaries, if so notified by the DPA.[376]

3. *Identifying guardians that can provide consent*

The PDP Bill, 2019 does well to provide the necessary flexibility of requiring consent from a parent or a guardian. Verification of guardians becomes tricky in case where an individual other than a parent may be the one providing consent. Unlike parents, where there may be some form of official documentation, in other cases where the child is temporarily in the custody of another individual, there may be difficulties in proving that the concerned individual is the requisite person for giving consent.[377] The Irish Data Protection Act, 2018 allows grandparent, uncle, aunt, brother or sister to give consent on behalf of the minor.[378] In the US, schools may act on parents' behalf in an educational context in cases where personal data is collected for learning purposes, but not for commercial purposes.[379] Given that if the age of 18 is retained, parental consent will be required for almost 472 children,[380] it would be useful for the DPA to pre-empt regulatory confusion arising from these basic issues.

4. *Input children's understanding of privacy in policy making and privacy decisions*

The conception of privacy is not homogenous and differs widely across contexts. This understanding is reflected in the practices of many regulators which have conducted extensive surveys with children as participants. Section 123 of the Data Protection Act, 2018 (UK), in fact, mandates that while designing a code on age appropriate design for children, children should be consulted by the UK ICO.[381] Similarly, when France conducted its consultation on children's data protection, it conducted an extensive survey of 1000 parents and 500 children to understand their use of the digital space.[382] One of the recommendations of the Council of Europe for regulators while establishing

[376] Clauses 28, 29 and 30, Personal Data Protection Bill, 2019.
[377] Facebook, "Submission to the UN Special Rapporteur for Privacy, A Better Understanding of Privacy: Children's Right to Privacy" (2020).
[378] Article 2A, Data Protection Act, 1988 (Ireland).
[379] FTC, "A Guide for Business and Parents and Small Entity Compliance Guide" available at https://www.ftc.gov/tips-advice/businesscenter/guidance/complying-coppa-frequently-asked-questions> (last accessed April 6, 2022).
[380] Census of India, 2011.
[381] Section 123(3)(a), Data Protection Act, 2018 (UK).
[382] CNIL, "Digital Rights of Minors: the CNIL Publishes the Results of the Survey and the Public Consultation" (2021) available at https://www.cnil.fr/fr/droits-numeriques-des-mineurs-la-cnil-publie-les-resultats-du-sondage-et-de-la-consultation-publique (accessed April 6, 2022).

or reviewing a national data protection framework is to ensure child participation in the design or review process.[383]

It would be sub-optimal to rely on the experiences of only other children while designing an effective informational privacy framework for children in India. Just as regulators are increasingly imbibing the practice of stakeholder consultation to better inform their regulatory practices, there is a need to reach out to children to understand their conception and concerns about privacy.[384] Moreover, under article 12 of the CRC, India is obligated to give due weight to the views of children, in all matters affecting them, in accordance with the age and maturity of the child.[385] Even after the consultation, there should be ways for children to express their views regarding day to day data processing operations.[386]

5. Children with disabilities

While the PDP Bill, 2019 itself does not make a reference to children with disabilities, there is a need to reflect on how access should be shaped for children with disabilities. A Council of Europe Report that examined the interaction of children with disabilities with the digital environment concluded that children with disabilities experience a triple barrier in the enjoyment of their digital rights. First, they shoulder the generic burden of not being heard and taken seriously as children, second, their disability is almost always associated with diminished capacities and competence in decision making in the digital space and third, guardians of children with disabilities tend to be more protective of them than other children.[387] As such children with disabilities tend to enjoy less autonomy than other children.

Moreover, interactions of children with disabilities with digital media can in some instances be more privacy invasive. For example, children with hearing impairments may have to switch on their video while communicating online in sign language. In this regard, there is a need for the DPA to deliberate on specific privacy related concerns

---

[383] Livingstone, Lievens and Carr, "Handbook for Policy Makers on the Rights of the Child in the Digital Environment" European Union (2018) available at https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8 (accessed April 6, 2022).
Also see, UNICEF, "The Case for Better Governance of Children's Data: A Manifesto" (2021) page 65 available at https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf (accessed April 6, 2022).
[384] See, Stoilova, Livingstone and Nandagiri, "Children's Data and Privacy Online: Growing up in a Digital Age. Research Findings." (2019) available at lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf for one of the most comprehensive surveys undertaken on children's privacy understanding and their views of privacy related harms.
[385] Article 12, United Nations Committee on the Rights of the Child.
[386] J Lina Jasmontaite and Paul De Hert, "The EU, Children under 13 years, and Parental Consent: a Human Rights Analysis of a new age based bright line for the protection of children on the internet" page 29 (2015) Vol. 5(1) International Data Privacy Law.
[387] Page 16, L. Landy and others, "Two clicks forward and one click back: Report on children with disabilities in the digital environment" (October 2019), available at https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f (accessed April 6, 2022). Also see, Office of Communications, "Children and Parents: Media Use and Attitudes Report 2022" (2022) available at https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2022 (accessed April 6, 2022).

arising for children with disabilities and to balance it with needs for autonomous development.

6. Prioritise privacy enhancing measures around certain data sets

Certain data sets such as those of health and education present greater risk to children. The emergence of digitalised learning in recent years has led to exponential amounts of personal data of children being processed. As per Annual Status on Education Report, 2020 more than a third of all school going children were pursuing education through digital means.[388] This trend is also noted by the White Paper on Data Protection. It observes that as schooling services are increasingly being digitised, there is a need on guidance to manage the manner in which this information is being stored, processed and transferred to the cloud service provider.[389] Consent in an educational setting is of a different nature because the refusal or withdrawal of consent, might lead to denial of educational services, which are important. Second, online education technologies are based on complex data processing, which hinder informed consent. Therefore, there is a degree of power imbalance between edtech companies and children, even when they are assisted by their parents.

It has been proposed that the data processing carried out by these data controllers should be limited to 'the remit of a public task carried out by schools'. This would mean advertising, for example, is not a compatible purpose to children's personal data processing, and certainly not one that would override the best interest of the child in an educational setting. It has been observed that a contract based model would be insufficient in this context, as processing only on the basis of consent would give illusory control over personal data.[390] In India, since the pandemic, there have been report of schools partnering with private e-learning platforms. This admixture of unequal bargaining power with commercial interests increase the scope of abuse. In that context, the DPA must focus on adopting a specific approach to the regulation of data.

Similarly, health data sets include sensitive personal information such as biometric data of an individual. Given the ubiquitous scope of its collection (wearables, mobile applications) and the kinds of significant decisions that can be taken on automated processing of these data sets, it is important to incorporate heightened privacy measures in their governance.

---

[388] ASER Centre, "Anuual Status of Education Report (Rural) 2020 Wave I" (2021) available at http://img.asercentre.org/docs/ASER%202021/ASER%202020%20wave%201%20-%20v2/aser2020wave1report_feb1.pdf (last accessed April 6, 2022).

[389] Committee of Experts, "White Paper of the Committee of Experts on a Data Protection Framework for India" Ministry of Electronics and Information Technology Page 87 (2017) available at https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf (last accessed April 6, 2022).

[390] Council of Europe, "Contribution prepared by the Secretariat of the Council of Europe on the subject of the right to privacy of children, in response to the consultation carried out by the UN Special Rapporteur on the right to privacy (UNSRP)" Page 4 (2020).

7. ***Balance privacy and access to information***

The DPA should ensure that compliance with the requirements of age verification should not lead data fiduciaries to "lock out" children from a meaningful user experience. Internet has immense potential in terms of the various participatory rights it allows children to exercise. Keeping that in mind, DPA should continuously monitor, possibly through crowd sourcing, to ensure that these practices are not resorted to. There is a risk that denigration of user experience for children can drive them "underground" i.e. they may be incentivised to lie about their age to receive a more wholesome experience on the internet. India is at an increased risk of this given that ***all*** data fiduciaries are required to have in place age verification mechanisms to some extent. This would allow even "general audience" websites to easily filter children and disadvantage them. Instead of limiting access to reduce risk of liability, data fiduciaries should be required to incorporate stronger data protection measures for children's personal data.

8. ***Guidance to parents on data sharing***

"Sharenting" has emerged one of the major threats to the informational privacy of children. The entire regulatory architecture is premised on age verification and parental consent with the assumption that parents will always align their actions with the privacy of their children. However, as has been discussed earlier, sharenting itself can endanger the informational privacy of children long before they develop a consciousness of their privacy. The South Australia Commissioner for Children and Young People has developed a fact sheet for parents to communicate the factors that should be weighed while sharing children's personal and the way to do so in a safe manner.[391] Given the centrality of parents / guardians to data protection for children, it is critical that the DPA not ignore this issue.

9. ***Development of a best practices code with extensive consultation***

One of the main takeaways from this paper has been that the emphasis for responsible behaviour needs to be shifted from the parents to the data fiduciaries. However, this shift in responsibility also entails considerable regulatory uncertainty for the data fiduciaries. As has been seen, till now the only regulatory material data fiduciaries can rely on for the kind of design specifications for their platforms and data processing comes mostly in the form of a "best practices" guide from three or four data protection regulators. The experience for other regulators has shown that this is a time intensive exercise given the extensive stakeholder consultations these involve. One of DPA's

[391] South Australia Commissioner for Children and Young People, "Sharenting" available at https://www.ccyp.com.au/wp-content/uploads/2019/02/CCYP_2018.3.13_sharenting_infographic_final.pdf (last accessed April 6, 2022).

first order of business should be to initiate this exercise. Through this exercise it will get a better sense of the regulatory components that should be provided for in the regulations, codes of practice and guidance notes.

10. Continuous monitoring to ensure children in India have same protections as elsewhere

It is clear that children in different countries receive differential protection by the same data controllers. In the Global South, children and families often do not have access or have delayed access to safer technologies that may have been incorporated in the online experiences for children from developed countries.[392] A data fiduciary may inculcate privacy enhancing measures when the data protection regulator of a particular jurisdiction may rule against privacy threatening practices of a data fiduciaries. The DPA in India should follow up on such developments and ensure that the enhanced protections are also incorporated in personal data processing of Indian children.

[392] Pedro Hartung, "The Children's Rights-by-Design Standard for Data Use by Tech Companies" Issue Brief No. 5 Good Governance of Children's Data Project (UNICEF) Page 5 (2020) available at https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf (last accessed April 6, 2022).

V. Conclusion

This paper has aimed to understand the discourse around children's informational privacy in India. It has attempted to evaluate the proposed Indian framework as per both the international principle based understanding of the scope and application of the right to privacy as also the existing regulatory frameworks in comparable jurisdictions. While some jurisdictions like the US have dedicated privacy laws for children, most other jurisdictions are trying to retrofit it into their existing frameworks for privacy for adults. India falls in neither of these countries. It is uniquely positioned in a situation where it can formulate its framework without the legislative baggage of existing regulations. In this situation, it must critically analyse its proposed framework.

A common refrain against up and coming regulatory frameworks is that they ape the COPPA Rule in different aspects such as age of digital consent, rights available to minors and the centrality of age verification and parental consent in ensuring privacy of minors.[393] India should be cautious of this pitfall. No doubt several concerns have been raised with the proposed age of digital consent in India, yet it would not be fruitful to reduce it to 13 *only* under the influence of other jurisdictions. The understanding and exercise of the right to privacy is extremely contextual. It is hardly ideal to transplant notions and solutions from a jurisdiction India. An analysis of the frameworks in other jurisdictions in so far as it can provide with indicative lessons from the experiences in those jurisdictions. However, discretion should be advised in trying to emulate those frameworks. What is required is to imbibe an indigenous understanding of the right to privacy in the Indian framework. This can be done only through conducting extensive stakeholder consultations and surveys to know how children in India conceptualise their privacy. Regulations and codes of practice should respect this understanding. Had this approach been previously imbibed, it is possible that data protection regimes would have already moved forward from considering age verification and parental consent mechanisms as the be all and end all to ensure children's privacy. Simultaneously, a data protection framework for children should also be enabling. The aim of a data protection regulation aimed towards children should be to create conditions that permit children to develop capabilities to engage with the digital environment in an independent manner.

In this context, the role of supporting paraphernalia apart from legal interventions also needs to be recognised. A number of countries have undertaken vigorous information campaigns to promote awareness of privacy and data protection and how these rights

[393] Milda Macenaite and Eleni Kosta, "Consent for Processing Children's personal data in the EU: Following in US footsteps?", 26(2) Information & Communications Technology Law Journal (2017) available at http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096, (last accessed April 6, 2022).

can be exercised among children.[394] The data protection law in Spain, in fact, statutorily provides that the education system will skill students to responsibly consume and critically engage with digital media in a way that protects their privacy and personal data.[395]

The PDP Bill, 2019 as also the Joint Parliamentary Committee Report on the PDP Bill, 2019 have their heart in the right place in proposing ways they believe would ensure greater protection for children. However, there is a need to allow for scope for their empowerment. Going forward, once the final formulation of the data protection law is known, a balancing of protection and empowerment should inform the approach of the DPA as well.

[394] National Authority for Data Protection and Freedom of Information, "Key to the World of the Net" as submission by Hungarian National Authority for Data Protection and Freedom of Information to the UN Special Rapporteur for Privacy, Page 42 2016 available at https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/privacy-child/NHRI-Ombusman-Commissions/5-Hungary-DPA-I.pdf (last accessed April 6, 2022) provides an illustrative list of such material being disseminated in other jurisdictions.
[395] Article 84.2, Protection of Personal Data and Guarantee of Digital Rights, 2018 (Spain).

www.vidhilegalpolicy.in
Vidhi Centre for Legal Policy
A-232, Ratan Lal Sahdev Marg,
Block A, Defence Colony
New Delhi 110024
011-43102767/43831699
vclp@vidhilegalpolicy.in