REGULATION OF BEHAVIOURAL MONITORING AND TARGETED ADVERTISEMENTS DIRECTED AT CHILDREN

Ensuring Personalisation Benefits Children

CUTS International 1983-2023

#2506

Regulation of Behavioural Monitoring and Targeted Advertisements Directed at Children

Ensuring Personalisation Benefits Children

REGULATION OF BEHAVIOURAL MONITORING AND TARGETED ADVERTISEMENTS DIRECTED AT CHILDREN

ENSURING PERSONALISATION BENEFITS CHILDREN

Published by

CUTS International
D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts1@cuts.org, Web site: www.cuts-international.org

Citation: CUTS International. (2025). *Regulation Of Behavioural Monitoring and Targeted Advertisements Directed at Children: Ensuring Personalisation Benefits Children.*

Cover Image Credit*: Knot9*

CONTENTS

Dr. Sasmit Patra
MEMBER OF PARLIAMENT
RAJYA SABHA

Foreword

22nd March, 2025

Regulation of Behaviour Monitoring and Targeted Advertisements

This report presents timely and critical insights into the role of personalization in children's digital lives. It brings together perspectives from multiple stakeholders and proposes framework that prioritize both safety and inclusivity for children. The report highlights both the benefits of well-implemented behavioural monitoring and the potential risks of overreach. It advocates for risk-based, age-appropriate safeguards that balance protection, access, and innovation, for example, allowing content filtering or assistive technologies with privacy controls, while restricting profiling for commercial advertising. The report highlights key considerations such as data minimization, privacy-by-design, and parental involvement, offering solutions to ensure child safety without undermining digital inclusion.

Importantly, the study recommends refining the definition of 'child' into age brackets, young children and teenagers, allowing for tailored protections. It also suggests metrics like parental satisfaction and psychological safety to assess the appropriateness of behavioural monitoring practices.

The CUTS team must be commended for their rigorous and thoughtful work. This report brings together diverse perspectives and proposes frameworks that prioritise both protection and inclusion. I trust it will contribute meaningfully to evidence-based policymaking and assist stakeholders in navigating complex trade-offs in protecting young users online. I hope it sparks deeper engagement across sectors to ensure every child in India can access the digital world safely, confidently, and equitably.

Dr. Sasmit Patra

C-104, Swarn Jayanti Sadan, Dr. B. D. Marg, New Delhi-110001, INDIA
Tel.: +91-11-23314809 | Email: sasmit.patra@sansad.nic.in

ACKNOWLEDGEMENTS

The report is the culmination of collaborative efforts from numerous individuals who contributed their insights, expertise, and support. The author extends his gratitude to Amol Kulkarni, Director (Research) at CUTS International, for his constant guidance, thought-provoking discussions, and leadership throughout this project.

The author extends his sincere thanks to Dr. Sasmit Patra, Member of Parliament, Rajya Sabha, and Member, Parliamentary Standing Committee on Communications and Information Technology, for kindly writing the foreword and lending valuable support to this initiative.

Special thanks are also due to the digital startups, civil society organisations, law firms, and academics who generously shared their time and valuable perspectives, enriching our understanding of the landscape.

The report has also benefited from the contributions of Shivangi Tyagi (former consultant, CUTS International), along with support of Sohom Banerjee, Aakarsh Bhargav, Sobhan Guha, and Pratyush Banerjee. The author also extends appreciation to Nishchay Rao (Intern at CUTS International) for his valuable contributions to this report.

The Publications Team at CUTS International-Madhuri Vasnani, Rajkumar Trivedi, Mukesh Tyagi and Shivendra Shekhawat-deserve special recognition for their exceptional effort in bringing this report to fruition.

The author acknowledges the contributions of other individuals who, while not named here, played crucial roles in this project's success.

Any errors or omissions that remain are solely author's responsibility.

Krishaank Jugiani
Senior Research Associate

EXECUTIVE SUMMARY

The internet has become an integral part of children's lives, playing a crucial role in their education, social interactions, and access to information. The growth of personalised internet, enabled by behavioural monitoring and targeted advertising, has significantly shaped children's online engagement, tailoring content to their needs and interests. It offers opportunities for enhanced learning, provides tailored health and well-being resources, and fosters inclusive and safe online communities. It helps enhance the relevance of content considering diverse linguistic, cultural, and socioeconomic backgrounds.

Further, personalisation ensures free content availability, which is crucial for maintaining digital rights, especially for children from economically constrained backgrounds. It also fosters inclusivity and accessibility, particularly in diverse countries like India, by addressing varying linguistic, cultural, and socioeconomic needs. It aids children with disabilities through tools like voice interactions and eye-tracking and helps shield them from harmful content while promoting positive behaviours like financial literacy and public health awareness. Additionally, personalisation aids in empowering young creators by allowing them to engage meaningfully with their audience, and leverage the potential of the digital economy.

When done wrong though, personalisation carries significant risks. Excessive collection of sensitive personal data increases the risk of data breaches and privacy violations, while manipulative advertising practices can exploit children's evolving critical reasoning skills. It can promote excessive screen time, leading to adverse physical and mental health outcomes. Unregulated behavioural monitoring can inadvertently stereotype children based on their online activities, reinforcing biases and limiting their exposure to diverse viewpoints. Without proper standards and safeguards, risks like exposure to inappropriate content, commercial targeting of children, and privacy violations can emerge.

This report has delved into the complex interplay between personalisation, behavioural monitoring, and targeted advertising in children's digital lives, outlining the benefits and risks. The study employed a mixed-methods approach combining secondary research with primary stakeholder feedback. Secondary research involved a detailed review of literature on existing regulatory frameworks, platform policies, and the implications of personalisation for children. Primary research consisted of in-depth interactions with and feedback from more than 100 stakeholders, including representatives from platforms, start-ups, policy influencers, experts, child rights

groups, civil society, consumer groups and young internet users between 17-20 years old.

During the discussion, young users shared their experiences of internet use, offering insight into their preferences. Responses highlighted the varied ways children use the internet for learning, entertainment, and health, corroborated by stakeholder feedback. These insights form the basis for actionable recommendations, ensuring the balance of personalisation benefits with robust safeguards. It aims to provide insights for policymakers and industry to navigate trade-offs in determining how data fiduciaries can conduct behavioural monitoring and targeted advertising for children, the purposes and conditions for such practices, and the age thresholds above which these activities can be permitted.

The report identifies key benefits, risks, and recommendations across various key sectors:

- **Education**: Personalisation in education offers enhanced learning opportunities, improved student engagement, helps in the prediction of student performance, and provides tailored support for children with disabilities. However, tracking children without adequate safeguards raises privacy and consent concerns and may exacerbate inequalities in access to digital education. Recommendations include implementing graded exemptions for behavioural monitoring based on age, limiting data collection to service delivery, and ensuring robust data security measures.
- **Health and Well-being**: Personalised health services allow for early detection of mental health issues, timely interventions, and improved access to sensitive information on topics like sexual health. Yet, concerns due to inadequate measures such as reduced self-regulation, internet addiction due to overuse, exposure to inaccurate health information, vulnerability to harmful content, and data security must be addressed. Transparent disclosures, age-appropriate exemptions, and digital literacy programmes are critical to mitigating these risks.
- **Safe Spaces for Marginalised Communities**: Behavioural monitoring supports community building and connection among marginalised groups, such as LGBTQIA+ youth and children in abusive situations by suggesting relevant content and spaces. However, in the absence of proper safeguards, risks like harassment, misinformation, and misuse of platforms can be challenging. Allowing behavioural monitoring for credible platforms, along with strict safeguards and robust data security standards, can create safer digital environments.
- **Age Estimation Services**: Accurate age estimation enables the delivery of age-appropriate content and features, enhancing safety and parental control. Nonetheless, concerns due to inadequately protected personalisation, like privacy risks associated with large-scale data collection, and the potential for

reinforcing stereotypes and discriminating against children based on their online behaviour must be addressed. Testing age-estimation technologies in regulatory sandboxes and ensuring transparency in data processing can mitigate these concerns.

- **Social Media**: Personalised social media platforms help users to express themselves, build community, and monetise opportunities from their talent. However, proactive measures are needed with essential security frameworks to address risks such as data misuse, manipulation through targeted advertising, addiction, and negative psychological effects with concerns about self-image issues, peer pressure and filter bubbles. Promoting algorithmic transparency, media literacy, and mental health resources can help children navigate social media responsibly.
- **Gaming**: Behavioural monitoring in gaming ensures a fair play environment and detects predatory behaviour but raises concerns about addiction, commercial exploitation and data misuse without appropriate precautions. Responsible gaming practices, parental control tools, and regulations on in-app purchases are recommended to safeguard children's interests.
- **Music and Podcasts**: Personalised recommendations in music and podcasts enrich user experiences but inadequate personalisation may narrow exposure and pose privacy risks. Age-appropriate content filtering and ethical data processing are essential to maintaining a balanced digital ecosystem.

A complete prohibition on behaviour monitoring and targeted advertisements, as proposed under section 9(3) of the Digital Personal Data Protection Act (DPDP Act) could lead to children losing out on the benefits of personalised internet. While the recently released draft Digital Personal Data Protection Rules propose exemptions to entities such as healthcare professionals, educational institutions, and crèches, these exemptions remain narrow in scope. They overlook scenarios where data processing could benefit children, such as content on awareness issues and those aligned with their interests and preferences.

Without personalisation, children could experience irrelevant content, reducing their ability to engage meaningfully online and also limiting innovative services to them. It can also expose them to inappropriate content, such as material promoting self-harm, violence, or misinformation, and face an overwhelming flow of irrelevant or harmful material, posing risks to their online safety and diminishing their digital experience.

A depersonalised internet experience would also resemble traditional media, lacking the tailored experiences that digital platforms offer. The relevant content may go behind a paywall, leading to reduced opportunities and investment in innovation, increased security risks and children migrating to unregulated platforms, increasing cyber risks. The economic model of the internet could also undergo significant shifts, leading to subscription-based services, potentially excluding children from financially

disadvantaged backgrounds and deepening digital inequities. Policymakers must, therefore, adopt a nuanced approach to balance personalisation benefits with strong safeguards to prevent negative impacts.

A core recommendation is implementing age-appropriate frameworks that cater to the varying developmental needs of children and teenagers. Younger children under eight often struggle to discern commercial content, requiring robust protections and parental oversight to safeguard against targeted advertising and inappropriate material. In contrast, older children and teenagers (ages 13–17) have a more nuanced understanding of online interactions and the trade-offs between personalisation and privacy. Consequently, younger children (below eight) need strong protection from targeted advertising and inappropriate content through parental oversight. Tweens (ages 9–12) and Teenagers (ages 13–17), on the other hand, should be proportionately empowered to make informed choices, with clear disclosures on data use and privacy settings.

Thus, transparency and agency around behaviour monitoring and targeted advertisements become vital. Platforms must provide age-appropriate explanations of data collection and usage, enabling children and guardians to make informed decisions. Teenagers should be taught how personalisation algorithms work and how their choices influence the content they see. Platforms should offer tools for children and parents to control data-sharing preferences and opt out of unnecessary monitoring. Exemptions under the DPDP Act must consider age differences, ensuring tweens and teenagers are provided tools for transparency, algorithmic control, and accessible, age-appropriate information.

A risk-based framework is necessary to assess behavioural monitoring and targeted advertising practices. Policymakers should differentiate between beneficial and exploitative practices, allowing exceptions for services that benefit children. Purpose-specific data policies can limit monitoring to ethically sound uses. Platforms should also conduct regular Data Protection Impact Assessments (DPIAs) to identify and mitigate risks and also ensure that personalisation technologies are inclusive and equitable. They should prioritise accessibility features, such as multilingual support and tools for differently-abled users. Platforms must safeguard against misuse, including impersonation, trolling, and data exploitation, especially for marginalised groups.

Purpose distinction is essential for determining the ethical scope of behavioural monitoring. Monitoring for safety and well-being purposes, such as detecting cyberbullying, grooming, or mental health risks, should be clearly defined as permissible. However, high-risk automated processing, such as profiling children for targeted advertising, must be strictly prohibited. Platforms must demonstrate evidence of benefit versus harm, showing that data collection is necessary and proportionate for fulfilling the intended purpose.

Privacy by design and default must be central to all platforms catering to children. Platforms must build privacy settings into the architecture of the product and implement high-privacy settings by default. They should also limit personal data collection to essential needs and require active consent for personalisation from children or parents/guardians. Measures like data anonymisation and shorter retention periods should be adopted to further protect sensitive information while enabling ethical personalisation.

Digital literacy for parents and children is also crucial for ensuring safe online environments for children. Parents should have tools to guide children's online interactions while respecting their privacy. For teenagers, digital literacy programmes are essential to build awareness about risks, privacy rights, and responsible technology use. Digital literacy programmes for teenagers must go beyond theoretical knowledge, equipping them to navigate personalisation algorithms practically and safely, in collaboration with schools, civil society, and industry. Policymakers should encourage collaboration between platforms and schools to integrate digital literacy into curricula, preparing children for the digital world.

Regulatory sandboxes are valuable for testing personalisation technologies in controlled environments. Platforms can test age-estimation, algorithmic transparency, and data minimisation practices before implementation at scale. Policymakers should use these outcomes to create robust, evidence-based regulations that prioritise children's safety and well-being. Policymakers must craft frameworks to nudge platforms toward safer consumer experiences, offering clear metrics for permissible tracking, including privacy protection, psychological impacts, and parental satisfaction.

The findings highlight the need for a balanced approach to regulating behavioural monitoring and targeted advertising, to ensure personalisation benefits children. Policymakers should adopt an evidence-based approach that ensures transparency, accountability, and inclusivity, fostering a safe and ethical digital ecosystem, while envisaging scenarios to allow behaviour monitoring and targeted advertisements, as provided under sections 9(4) and 9(5) of the DPDP Act. It is also crucial to explore more exemptions under the Fourth Schedule of the DPDP Rules, which are use-case specific. Such exemptions could be differentiated by age groups, aligned with principles of safe, ethical, and responsible data processing, and guided by a risk-based framework.

International examples emphasise the importance of both protecting children and empowering them to make informed online choices, offering valuable lessons for India. This approach will enable children to benefit from technology in a safe, enriching environment that supports their growth and development while ensuring their rights are protected.

1. INTRODUCTION

Children's data under the Digital Personal Data Protection Act

The Government of India recently enacted the Digital Personal Data Protection Act, 2023 (hereinafter referred to as "the Act" or "DPDP Act").[1] The Act seeks to regulate the way companies process[2] an individual's digital personal data[3], including that of children.[4]

Specifically, Section 9 of the Act deals with the processing of children's personal data. Section 9(1) requires data fiduciaries[5] to obtain verifiable consent from the parent of a child before processing any personal data of such child. Section 9(2) provides that a data fiduciary shall not undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child. Consequently, sections 9(1) and 9(2) intend to provide agency to users and guard against harmful data processing in the case of children.

Section 9(3) goes a step further and provides that a data fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children. While the Act provides illustrations and explanations to clarify its intent and scope for several provisions, no such attempt has been made for terms like 'tracking', 'behaviour monitoring' or 'targeted advertising'. This has led to varied interpretations about such undefined terms. For instance, it has been pointed out that since purpose of the Act is to protect digital personal data, advertisements not based on processing of such data of users (including children), but based on context of their search queries, website visits, are outside the purview of the Act.[6]

---

1 The Digital Personal Data Protection Act, 2023, available at: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

2 As per DPDP Act, processing in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction

3 Section 2(t) of the Digital Personal Data Protection Act, 2023 defines 'personal data' to mean any data about an individual who is identifiable by or in relation to such data.

4 As per the DPDP Act, child means an individual who has not completed the age of eighteen years.

5 As per the DPDP Act, data fiduciary means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

6 https://www.socialsamosa.com/experts-speak/how-india-dpdp-act-could-change-digital-campaigns-8606658 and https://www.financialexpress.com/business/brandwagon-adtech-and-data-privacy-balancing-compliance-and-innovation-3673787/

Section 9(4) of the Act provides that the provisions of sections 9(1) and 9(3) shall not be applicable to the processing of personal data of a child by such classes of data fiduciaries or for such purposes, and subject to such conditions, as may be prescribed[7] by rules made under the Act. Consequently, the Act envisages that tracking or behaviour monitoring of children and targeted advertisements directed at children can be permitted by specific classes of data fiduciaries, for specific purposes, or under specific conditions. Section 40 of the Act empowers the Central Government to make rules by notification[8] and subject to the condition of previous publication. The Government is yet to issue rules.

In addition, as per section 9(5) of the Act, the Central Government may, if satisfied that a data fiduciary has ensured that its processing of personal data of children is done in a manner that is verifiably safe, notify for such processing by such data fiduciary the age above which that data fiduciary shall be exempt from the applicability of all or any of the obligations under sections 9(1) and 9(3) in respect of processing by that data fiduciary as the notification may specify. In other words, if a data fiduciary processes the personal data of children in a verifiably safe manner, it can be allowed to undertake tracking or behavioural monitoring or targeted advertising of children above a certain age. However, the term 'verifiably safe' has not been defined or explained under the Act.

On January 03 2025, the Ministry of Electronics and Information Technology (MeitY) released the Draft Digital Personal Data Protection Rules, 2025 ("draft Rules" or "the Rules") for public consultations. Rule 11, read with the Fourth Schedule of the Rules, proposes specific instances where certain data fiduciaries are exempted from Section 9(3) of the Act. The exemptions under Part A of the Fourth Schedule allow

- clinical establishments, mental health establishments, and healthcare professionals, including allied healthcare professionals, to process data for providing health services to protect a child's health;
- educational institutions to process data for educational purposes and the child's safety; and
- crèches, day-care centres, and related transportation services to process data for ensuring children's safety and tracking their locations during transit.

Moreover, exemptions under Part B of the schedule exempt activities such as fulfilling legal duties, providing benefits or subsidies, creating user accounts for email communication, ensuring that information detrimental to a child's well-being is inaccessible to them, and verifying that the Data Principal is not a child. The exemptions granted to fiduciaries for the latter three use cases represent a positive step toward fostering a safe and supportive online environment for children. However, there are concerns around the lack of précised guidelines in the Schedule. Despite

7 As per the DPDP Act, prescribed means prescribed by rules made under the Act.

8 As per the DPDP Act, notification means a notification published in the Official Gazette.

potential concerns about the interpretation of the Rules, an approach that prioritises children's access to the internet while leveraging personalisation to their benefit should be adopted.

There seems to be a tension between different provisions of section 9 of the Act. Section 9(2) sets out a broad principle-based vision that processing of children's data must be in their interest, and section 9(1) provides for a procedural safeguard in the form of verifiable parental consent. Section 9(3) appears to take a step back and prohibits behaviour monitoring and targeted advertisements, which are dependent on the processing of children's data and could be used to advance their interests when done right. Recognising the potential inconsistency, sections 9(4) and 9(5) allow envisaging scenarios wherein behaviour monitoring and targeted advertisements for children could be allowed.

Need to strike a balance: Ensuring personalisation for children's welfare

Children should be able to leverage the potential of the internet to gain the knowledge they seek, interact with friends, further their interests, and acquire skills they desire, in an accessible, safe and secure manner, away from predators, harmful and irrelevant content. Personalisation, when appropriately implemented, can support this by referring them content and connections to suit their liking.

The internet also provides a powerful medium for children where they can express their creativity, connect with their peers, form communities based on common interests, and even empower their entrepreneurial spirit by becoming content creators. Many of these functionalities are possible because of personalisation.

Behaviour monitoring is the key to offering such a personalised experience, without which children might be inundated with loads of content, much of which may not be relevant to them, and some of it might also be harmful. They may not be able to reach out to like-minded others sans personalisation. Moreover, certain types of behavioural monitoring may actually serve protective functions, such as detecting cyberbullying or identifying predatory behaviour.

Inappropriate personalisation for children has been linked with concerns like exposure to unsuitable content and misinformation, fraudulent actors and predators, promotion of age-restricted products, adverse impact on child's physical and mental health,[9] developmental delays[10], and targeted advertisements and service features that

9 https://www.indiatoday.in/health/story/higher-screen-time-linked-to-increase-in-myopia-in-children-study-2559171-2024-06-27

10 https://www.researchgate.net/publication/353028391_Prevalence_of_excessive_screen_time_and_its_association_with_developmental_delay_in_children_aged_5_years_A_population-based_cross-sectional_study_in_India

generate revenue at children's expense. [11] Growing concerns have emerged about problematic applications of behavioural monitoring and targeted advertisements directed at children, and the misuse of their data. Additionally, children's privacy and safety, particularly regarding the monitoring of their online behaviour, remain pressing concerns.

It should be possible to address these concerns and minimise such risks without taking away the benefit of personalisation from children. This is the balance which children's data protection focused legal frameworks, like section 9 of the DPDP Act, must pursue. To this end, it would be essential to direct the purpose and use of behaviour monitoring to protective and enabling ends and not exploitative ones, and accordingly determine the type and scope of data collection, management, and ensuring transparency of these processes for parents and children.

Unreasonable restrictions on personalisation could potentially have a detrimental impact on innovation leading to the deterioration of services, curtailment of safety options and hindering of valuable product features offered by digital platforms to children.[12] Hence, a nuanced approach to regulating behaviour monitoring and targeted advertisements directed at children would be essential.

How is consumer behaviour monitoring done on the internet?

Tracking an individual's preferences online is done through many techniques, one example of which is analysing web browser level cookies.[13] These are small files that websites store in their visitors' devices, with an aim to remember some information about the user when they visit the website again.[14] Cookies can be temporary or permanent – temporary cookies or session cookies disappear when the browser is closed, while the website stores permanent cookies.[15] Tracking devices via cookies serve many functions – like obviating the need to re-enter passwords and usernames, remembering 'wishlists' and 'shopping carts,' and other preferences.[16]

[11] Profiling for content delivery and service personalisation, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/best-interests-framework/profiling-for-content-delivery/, Ghosh, Arnab, Game Over: An Analysis of How Video Game Loot Boxes and Advertisements Target Children with Potential Solutions (March 14, 2023). Available at SSRN: https://ssrn.com/abstract=4387884 or http://dx.doi.org/10.2139/ssrn.4387884

[12] Quach, S., Thaichon, P., Martin, K.D. *et al.* Digital technologies: tensions in privacy and data. *J. of the Acad. Mark. Sci.* 50, 1299–1323 (2022). https://doi.org/10.1007/s11747-022-00845-y

[13] Ignacio N. Cofone, *The Way the Cookie Crumbles: Online Tracking Meets Behavioural Economics,* International Journal of Law & Information Technology (2016), pp. 1-25, doi: 10.1093/ijlit/eaw013

[14] Ibid.

[15] Ibid.

[16] Ibid.

In a larger sense, regulating the internet for children also means considering their rights online and the role that the internet plays in their offline lives.[17] It has been argued that children's positive rights (enabling rights, like the right to freedom and expression) must also be balanced with negative rights (protective rights, like the right to privacy and the right to be protected from harmful information).[18] The balance requires careful consideration of ethical, technological, and legal factors.

About the study

The study aims to better understand the role of personalisation in the digital lives of children. We undertake an in-depth use case specific analysis to examine the benefits and risks emerging from behaviour monitoring and targeted advertisements directed at children. We will also analyse the exemptions proposed under the draft Rules to assess whether such exemptions are sufficient or should be broadened to ensure a more holistic and personalised experience for children in a safe and secure manner.

Since behavioural monitoring differs with scenario, an overarching discussion of the technology may be unable to capture the nuances that a use-case-based assessment might illustrate. Through a mixed methods approach of integrating primary and secondary research, we aim to present different use cases of internet for children, highlighting the benefits of behaviour monitoring done right, and the risks of it going overboard.

We hope this exercise will aid in providing insights and evidence to support policymakers in navigating complex trade-offs for determining classes of data fiduciaries who can be permitted to undertake behaviour monitoring and targeted advertisements directed at children, purposes for which behaviour monitoring and targeted advertisements could be allowed to be directed at children, conditions subject to which behaviour monitoring and targeted advertisements could be permitted to be directed at children, and age of children above which data fiduciaries can be permitted to undertake behaviour monitoring and targeted advertisements towards children.

Chapter 2 discusses the role of personalisation in enabling digital access for children. Chapter 3 conducts a thorough use-case analysis of behaviour monitoring across key sectors, and related benefits and risks. Chapter 4 explores the impact of a complete ban on behavioural monitoring and tracking and targeted advertisements. Chapter 5 discusses the developmental differences among children, and the requirement of an age-appropriate framework for personalisation, while Chapter 6 concludes with recommendations for policymakers and an optimal way forward.

---

[17] Sonia Livingstone, *Regulating the Internet in the Interests of Children: Emerging European and International Approaches* in The Handbook of Global Media and Communication Policy, Mansell et al (eds.), Apr. 08, 2011, doi.org/10.1002/9781444395433.ch31

[18] Ibid at page 510.

Approach and methodology

This report utilises a mixed methods approach of combining primary and secondary research, to better understand the contours of personalisation for children on the internet, related benefits and risks, safeguards and conditions with which it could potentially be allowed to benefit children.

The secondary research involved desk research and literature review of research reports, articles, papers, impact assessments, existing and emerging regulatory frameworks, and personalisation policies of prominent platforms, among other literature. The primary research involved obtaining written and oral feedback from more than 100 stakeholders, including, industry, start-ups, online app developers, academia, think tanks, experts, child rights groups, civil society organisations, young users (aged 17-20 years[19]), media, policy influencers, former senior bureaucrats, among others.

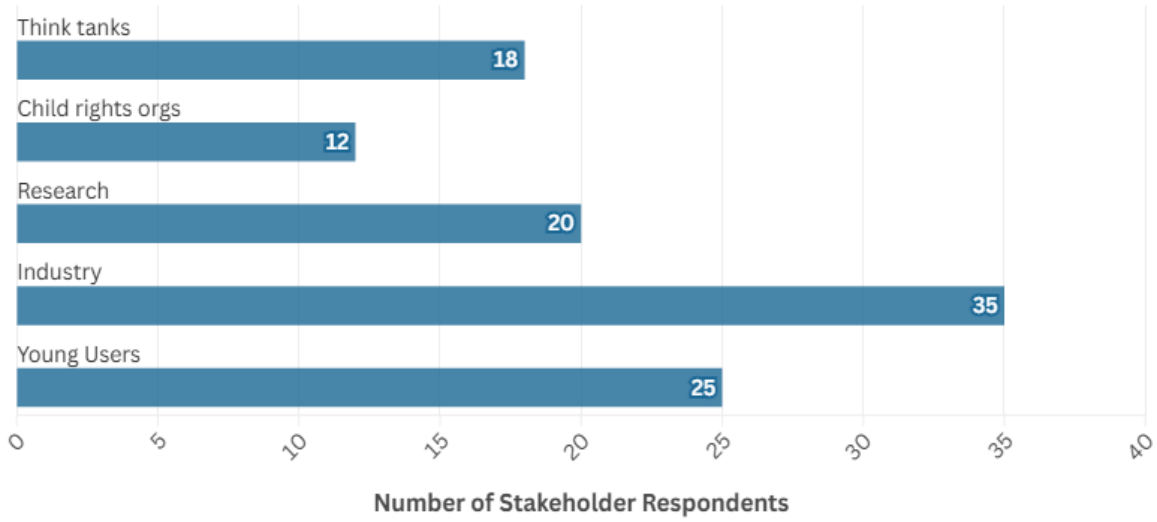
The feedback from stakeholders related to use cases over internet for children, the scope of behavioural monitoring and targeted advertisements, their benefits and risks, practices to ensure a safe and productive online experience for children, and potential mechanisms to regulate behavioural monitoring and targeted advertisements appropriately. These discussions provided an overview of issues to consider when implementing policies aimed at children that regulate tracking, behavioural monitoring, and targeted advertising.

In addition, interacting with children helped us better understand the nature of their engagement with the internet, including using it for self-consumption as well as commercial purposes.

In aggregate, we received responses from around 110 stakeholders, which helped us obtain a comprehensive evidence-based view on the subject, ensure appropriate analysis, and suggest actionable recommendations. Both quantitative as well as qualitative responses were received from the stakeholders in form of their feedback.

[19] It was felt that young users belonging to this age-group may be in a position to provide first hand perspectives of internet usage by children. Internet users below this age group were not contacted directly owing to practical and ethical considerations.

Respondent categories for the study (n=110 respondents)



2. PERSONALISATION AND DIGITAL ACCESS

Role of personalisation in internet access

Around the world, the internet is becoming an indispensable tool for children and teenagers (aged 13-17 years), offering a gateway to learn, connect, and participate in the digital economy's vast resources and opportunities. They tend to use edtech platforms to study online, social media to be closer to their peers, follow videos/posts that interest them, and game online.[20] A study conducted on internet usage by young people within the age group of 13 to 20 years in India[21] revealed the internet usage among respondents, with it emerging as the first-choice media usage for young people. According to the study, children use internet for entertainment, information searches, homework, browsing news and current events, seeking health-related information, and for engaging in online shopping.

The use cases among children from this study corroborate those with the feedback we received from young users, as shown in the figure below.

Purpose of internet usage by children (n = 135 responses for 25 respondents)

At present, much of content and opportunities on the internet in India is outside of the paywall, which allows children across social and economic backgrounds to access it, without financial implications. This includes access to content across sectors, including education, entertainment, health, music, and skilling, among others. Access

[20] OfCom, *Children and Parents: Media Use and Attitudes Report,* Apr. 19, 2024, https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-media-use-and-attitudes-2024/childrens-media-literacy-report-2024.pdf?v=368229

[21] Nain, Harikishni & Chaudhary, Monica. (2022). *Internet Usage by Young Kids in India,* FWU Journal of Social Sciences, Fall 2022, Vol.16, No.3, 120-131 DOI: http://doi.org/10.51709/19951272/Fall2022/9

to technology and the internet can provide children with a range of skills that could benefit them in the world they are growing up into.[22] If leveraged in the right way and universally accessible, digital technology can be a game changer for children being left behind – whether because of poverty, race, ethnicity, gender, disability, displacement or geographic isolation – connecting them to a world of opportunity and providing them with the skills they need to succeed in a digital world.[23]

Advertising plays a crucial role in ensuring this content remains accessible to all, regardless of financial constraints. Platforms also collaborate with experts in child development, and digital learning to enhance their offerings and refine guidelines for quality content tailored to children and teenagers, and create a child friendly and safe environment on internet.[24] Personalisation, therefore, not only helps platforms generate profit but also aims to enhance the value children, as consumers, get from the online experience.[25] Absent personalisation, platforms may feel the need to shift to user-chargeable service models wherein those who are in a position to pay more get access to more content in a safer environment. This would be counter intuitive as those who are unable to pay are in a greater need to access resources, skills and content available on the internet, with the objective of bridging the economic divide.[26]

Key benefits to children of personalisation done right

The internet and its services meet the diverse needs and interests of children by leveraging personalisation to make the digital space truly enriching, relevant and meaningful, while helping children navigate the huge volume of user generated content that is available for consumption online. Personalised advertising, based on the contexts like location and age groups and not micro targeting based on personal information, can allow teenagers to carefully examine the services they may want to engage with, and not get lost in the myriad of services.

By offering content that is relevant and tailored to their interests, such as personalised content recommendations, users are more likely to remain on a website and interact meaningfully, increasing the chances of conversion, return visits and long-term loyalty. Personalised recommended content ensures that users are presented with recommendations that align closely with their interests. Without such personalisation, children and teenagers are likely to be suggested only the most popular content, missing out on content that aligns better with their interests but might otherwise

22 https://www.theguardian.com/sustainable-business/2015/dec/24/is-technology-in-the-classroom-good-for-children

23 https://www.unicef.org/media/48601/file

24 https://blog.youtube/inside-youtube/youtubes-principled-approach-children-teenagers/

25 https://www.sciencedirect.com/science/article/abs/pii/S1094996809000322

26 For instance, Snapchat states on its website: "Advertisers pay a lot more to show ads to people who are more likely to be interested in them. It is not possible for us to keep Snapchat a fun, safe, and innovative online space, without charge, unless we show personalized ads." https://values.snap.com/privacy/ads-privacy

remain undiscovered.[27] By serving personalised content, businesses can ensure that their customers are presented with content that are most relevant to them, at the right time.[28]

Personalisation also unravels the opportunity to support inclusive education of children, differently abled people and other minority groups. It can provide multiple means of presenting, representing and expressing learning and help learners overcome barriers they would otherwise experience to participate in the curriculum. It also has the potential to increase enjoyment and motivation.[29] Fast and affordable internet access is likely to be this generation's greatest leveller.[30]

This is also significant given India's vast linguistic, cultural, and socioeconomic diversity, where a standardised internet experience may not be sufficient to meet the varied needs of users. Personalisation allows platforms to suggest regional music, folklore, and traditional art to children, enabling children and teenagers to engage with content that resonates with their cultural backgrounds. Interactive formats that feature age-appropriate regional stories, music, and festivals make cultural learning both accessible and enjoyable, fostering a deep appreciation for their heritage among the youth.[31] As revealed in our stakeholder consultations, such innovations and opportunities to access content in different mediums and languages preferred by young users are possible through revenue generated by platforms by enabling personalised content and advertisements.

Experts also underscored the usefulness of behaviour monitoring to improve accessibility and effectiveness of varied internet use cases for children. These may include cases such as applying for scholarships or educational opportunities. Moreover, children, particularly those not digitally or functionally literate in mainstream languages like English or Hindi, rely on voice interactions with their devices, which is facilitated through behavioural monitoring.

A personalised approach that tailors content, resources, and interactions to each user's preferences, leveraging the internet as a more inclusive, engaging space, can really be valuable for users. Further, by providing regional language options and seamless multilingual support, digital platforms can ensure that young learners not only access

---

27 https://static.googleusercontent.com/media/publicpolicy.google/en//resources/youth-legislative-framework.pdf

28 https://www.forbes.com/councils/forbestechcouncil/2023/04/11/the-internet-of-you-how-web-personalization-is-shaping-the-future/

29 https://unesdoc.unesco.org/ark:/48223/pf0000373655

30 https://blogs.lse.ac.uk/internationaldevelopment/2022/11/29/internet-access-as-a-tool-for-boosting-economic-and-social-equality/

31 Xia Y, Shin S-Y, Kim J-C. Cross-Cultural Intelligent Language Learning System (CILS): Leveraging AI to Facilitate Language Learning Strategies in Cross-Cultural Communication. Applied Sciences. 2024; 14(13):5651. https://doi.org/10.3390/app14135651

but also fully understand quality educational content in both English and their mother tongue.[32] This can be especially beneficial for youth in rural areas, where high quality access, comprehension and retention can improve significantly when learning occurs in familiar languages and also promotes multiculturalism.

Furthermore, since 'accessibility' requirements may vary with users, behavioural monitoring can serve as a useful tool in determining the specific level of accessibility required by each user. Some users, for instance, may benefit from eye-tracking technologies, while others may benefit from audio captioning.[33] It also provides support for differently abled children through accessible digital tools.[34] Emerging features like virtual reality experience can allow them to build their understanding and get acquainted with immersive technologies.

Behaviour monitoring also serves as evidence for future innovation on accessibility by recording accessibility gains via monitoring actual user behaviour, and identifying areas for improvement. Tracking user authentication data, such as usernames and passwords, ensures that only authorised users have access to their accounts, keeping their personal data safe.[35] Studies have also highlighted how behavioural monitoring enables effective access to technologies for individuals with special needs and those with limited education. These interventions can be customised to suit varying levels of physical abilities, technological skills, and social environments, ensuring they are accessible and effective for diverse users.[36]

Right personalisation can help children actively participate in the creator economy

Scholars have also highlighted that several international approaches to regulating children's internet usage are driven by an emphasis on children being a vulnerable group, grouping them with other marginal communities like "persons with disabilities,

---

32 Ibid

33 Bunyi et al, *Accessibility and Digital Mental Health, Considerations for More Accessibly and Equitable Mental Health Apps,* Front Digit Health. 2021; 3: 742196, Sept. 29, 2021. doi: 10.3389/fdgth.2021.742196

34 Behavioural monitoring can enhance the digital experiences of differently-abled children and those from multilingual or limited literacy backgrounds by tracking interactions such as voice commands, emotion recognition technologies, customisable text-to-speech options to create personalised, safer, and more user-friendly environment without barriers. See, Aarambh India, *Understanding the Internet of Children & Young People in India: The Ideal Internet Report 2019 – 2020*, https://aarambhindia.org/understanding-the-internet-of-children-young-people-in-india-the-ideal-internet-report-2019-2020/#:~:text=Usage-,1.,2; Garcia-Garcia, Jose & Penichet, Victor & Lozano, María & Fernando, Anil. (2021). Using emotion recognition technologies to teach children with autism spectrum disorder how to identify and express emotions. Universal Access in the Information Society. 21. 10.1007/s10209-021-00818-y.

35 https://edly.io/blog/digital-identity-verification-in-edtech/

36 Alberto Monge Roffarello and Luigi De Russis. 2023. *Achieving Digital Wellbeing Through Digital Self-control Tools: A Systematic Review and Meta-analysis*. ACM Trans. Comput.-Hum. Interact. 30, 4, Article 53 (September 2023), 20-23. https://doi.org/10.1145/3571810

older persons, indigenous people, refugees and internationally displaced people, migrants, and remote and rural communities."[37]

However, the widespread use of the internet for learning, socialising, and entertainment highlights the active role of children and teenagers as digital participants, and not just as consumers but increasingly as content creators[38] too. Today's children, as digital natives, are increasingly putting out content on social media, with the support of their parents or guardians, often referred to as "kidfluencers". Children, therefore, are no longer confined to passive consumption of pre-set content but play an active role as agents in the digital economy. For young entrepreneurs and creators, algorithms suggest their content to relevant audiences, helping them build digital businesses or personal brands.[39]

The approach of viewing children *only* as a vulnerable group with no agency of their own does not adequately capture their role as agents and participants in the digital economy and as creators of online content.[40] They are also active creators and contributors to social media, monetising what they post, therefore benefiting from, and being consumers as well as contributors to the creative digital economy. The Indian Government has also recognised the potential of young talent in this area, constituting national creator awards in several diverse fields.[41]

Key risks of personalisation gone wrong

Personalisation goes wrong when it is done without necessary principles, safeguards, standards, and oversight. It can direct inappropriate content to children, such as content related to self-harm, health and current affairs related misinformation, and violent or abusive material, among others.[42] In some cases, it can also lead to showing age-restricted products to children.[43]

---

37 Byrne, Jasmina; Burton, Patrick (2017). *Children as Internet users: how can evidence better inform policy debate?. Journal of Cyber Policy, 2(1), 39–52.* doi:10.1080/23738871.2017.1291

38 Term taken from Pew Research Centre Study on Teen Content Creators and Consumers, Nov. 2, 2005, https://www.pewresearch.org/internet/2005/11/02/part-1-teens-as-content-creators/#:~:text=More%20than%20half%20of%20online,might%20be%20called%20Content%20Creators

39 https://startuptimes.net/meet-the-13-year-old-entrepreneur-who-is-teaching-kids-how-to-code

40 See page 42, Ibid.

41 PM Presents First Ever National Creators Award in 20 Categories, *Times of India,* Mar. 8, 2024, https://www.indiatoday.in/india/story/pm-modi-national-creators-award-20-categories-for-excellence-jaya-kishori-drew-hicks-social-influencers-2512170-2024-03-08

42 Khalaf A M, Alubied A A, Khalaf A M, et al. (August 05, 2023) The Impact of Social Media on the Mental Health of Adolescents and Young Adults: A Systematic Review. Cureus 15(8): e42990. doi:10.7759/cureus.42990

43 Z. Moti et al., "Targeted and Troublesome: Tracking and Advertising on Children's Websites," 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2024, pp. 1517-1535, doi: 10.1109/SP54263.2024.00118.

Use of on-by-default settings, without adequate transparency or safeguards can also lead to targeted advertisements and service features that generate revenue at children's expense (for example loot boxes or in-game purchases), promote excessive screen time, could lock children in, and lead to unauthorised transactions. [44]

Personalisation can involve the collection of personal data, which needs to be handled with care. The absence of adequate protections could lead to data breaches and privacy violations. During our consultations, stakeholders highlighted concerns with inadequate security standards deployed by some accessibility-focused service providers, often relying merely on consent for data collection and sharing, which is unlikely to be effective as the target customer base requires accessibility support.

Personalisation allegedly leads to increased and excessive screen time, due to children getting addicted to the personalised content, which has been associated with a higher risk of myopia in children and adolescents.[45] Excessive screen time has also been associated with developmental delays in young children.[46]

The UK's Information Commissioner's Office framework recommends using personalisation to deliver appropriate content to children while also cautioning against its inaccurate application.

Benefits of personalisation done right and risks of personalisation gone wrong[47]

Rights of children	Benefits of personalisation done right	Risks of personalisation gone wrong
The inherent right to life and survival. Their physical and emotional development should not be impeded.	Promotes positive health behaviours and online safety tools	Exposes children to unsuitable content (for example age-inappropriate products, self-harm or inaccurate health information)

[44] Ghosh, Arnab, Game Over: An Analysis of How Video Game Loot Boxes and Advertisements Target Children with Potential Solutions (March 14, 2023). Available at SSRN: https://ssrn.com/abstract=4387884 or http://dx.doi.org/10.2139/ssrn.4387884

[45] https://www.theguardian.com/society/2025/feb/21/every-hour-children-spend-on-screens-raises-chance-of-myopia-study-finds

[46] https://www.researchgate.net/publication/353028391_Prevalence_of_excessive_screen_time_and_its_association_with_developmental_delay_in_children_aged_5_years_A_population-based_cross-sectional_study_in_India

[47] Profiling for content delivery and service personalisation, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/best-interests-framework/profiling-for-content-delivery/ Personalisation goes wrong when it is done without necessary principles, safeguards, standards, and oversight, prioritising commercial gains over children's well-being and exposing them to content that may not be in their best interests.

Rights of children	Benefits of personalisation done right	Risks of personalisation gone wrong
Right to information from a diversity of digital media sources, and in particular those that promote their social well-being and general health.	Results in targeting news information in the best interests of the child	Exposes children to information not in their best interests (for example misinformation)
Right to be protected from all forms of physical or mental violence, abuse, maltreatment or exploitation.	Provides access to safe and child-appropriate content	Exposes children to violent or abusive content
Right to the highest attainable standards of health, and access to health care information and services online.	Promotes public health messaging and advice	Exposes children to inaccurate health information.
Children have a right to be protected from economic exploitation of all forms.	Targets content that promotes financial literacy, skilling and safe online behaviour.	Target adverts and service features that generate revenue for children (for example loot boxes or in-game purchases), using on-by-default settings, without adequate transparency or safeguards. Leads to fraudulent or misrepresented products.
Children have a right to be protected from the illicit use of drugs and age-restricted substances	Promotes information that protects children from drug abuse.	Target age-restricted products to children (for example alcohol)

Key measures taken by platforms to ensure personalisation benefits children

During our stakeholder consultations, some platforms highlighted different measures they undertake to ensure that personalisation happens in the best interests of children.

Personalisation of content and ads can potentially be based on data provided by users about themselves, their interests, and inferences about their interests based on their online activities. However, for personalised ads, some platforms do not use inferences about children's gender cohort, their interests, or their friends' interests, to personalise

the ads for such children.[48] This may be a useful way to ensure minors are not able to access irrelevant or inappropriate ads while still benefiting from personalised organic content such as recommendations.

Similarly, some platforms do not use advertisements based on information collected by them about users' activity on the websites and platforms of their advertisers and partners.[49] Refraining from using activity based advertisements can help users monitor and navigate online behaviour and make conscious decisions about online transactions rather than being driven purely by advertisements. Moreover, for some platforms, advertisements are only based on user types and not on micro details about user behaviour.[50]

For children, some platforms prohibit ad personalisation altogether. They treat personal information from anyone viewing content designed for children as if it belongs to a child, regardless of the viewer's actual age. Furthermore, these platforms do not permit the use of third-party trackers in advertisements displayed on content created for children. While advertising is allowed to support creators of high-quality kids' content, strict guidelines are in place to limit the types of products and services advertised. For instance, ads for dating apps, food and beverages, and those containing violent or graphic content are restricted.[51] Further, they also allow parents or legal guardians to choose supervised accounts and the right experience for their children, while taking into account that the developmental needs of children differ from those of teenagers, appropriately reflecting this in their practices.[52] Such an approach to ensure alignment between the age-appropriateness of content and ads permissible on such content can also help create a safe online experience for children.

It will be useful to encourage platforms to craft and disclose their unique strategies around content and advertisements directed at children. Transparent and upfront disclosures can help children and their parents make informed decisions about platforms and content which children should access. This can foster innovation among

---

48 Snap publicly available disclosures state that: "If you are located in the EU or UK and are under 18 we do not use inferences about your gender cohort, interests or friends' interests to personalize the ads you see." See, Snapchat Ads Transparency | Snapchat Privacy. Similarly, "If you are located in the EU or UK and are under 18, we do not use information collected by Snap from your activity on the websites and platforms of our advertisers and partners (i.e., "Activity-Based Ads") to determine which ads to show you. Similarly, we may also limit the use of this information to certain age ranges in other jurisdictions to comply with local laws." See, https://values.snap.com/privacy/ads-privacy

49 https://values.snap.com/privacy/ads-privacy

50 Snap discloses that "We don't share everything about you with advertisers. We only allow advertisers to specify what type of user should see their ads and measure whether their ads are successful…We also hold our advertisers to certain standards. We expect them to be honest about their products, services, and content, to be kind to our diverse community, and to not compromise your privacy." See https://values.snap.com/privacy/ads-privacy

51 https://blog.google/products/ads-commerce/our-strict-privacy-standards-around-made-for-kids-content/

52 https://blog.youtube/inside-youtube/youtubes-principled-approach-children-teenagers/

platforms and a competitive environment with the best interests of the child at its core.[53] It would also be beneficial to encourage platforms that handle children's data to conduct regular data protection impact assessments and audits. These assessments could focus on ensuring that the processing of children's personal data does not violate their rights or compromise their safety, privacy, and well-being.

Personalisation of content can also enable a safer online experience as it can help content creators and advertisers to avoid targeting to specific cohorts which are not relevant for their products, and also comply with legal frameworks. For instance, in several countries, advertisements for alcohol are not shown to minors.[54]

Internet access and use are being increasingly associated with the positive wellbeing of users, including young users. Consequently, regulation impacting access to internet by children should rely on data and not be guided by anecdotes.[55] Considering the varied uses of the internet by children for beneficial purposes and the role of personalisation in enabling such benefits, a blanket approach to prohibit behaviour monitoring and targeted advertisements, may not be advisable. It would be pertinent to better understand different use cases and purposes of the internet for children, services offered/developed, risks involved, and available mechanisms to foster a safe online experience.[56] The assumption that all behavioural monitoring is detrimental to children can be an incorrect premise for policy making and can lead to the exclusion of children from gaining the benefits of these services. This analysis can help policymakers develop exemptions under sections 9(4) and 9(5) and also the Fourth Schedule of the DPDP Act and the rules respectively.

53 https://static.googleusercontent.com/media/publicpolicy.google/en//resources/youth-legislative-framework.pdf

54 As per Snap's publicly available policies: "Advertisers might want to market certain products to certain age groups that may be more receptive to a particular ad or avoid groups for which an ad is not relevant or appropriate. For example, if you are under 21 in the U.S. we won't show you ads for alcohol." Similarly, "If you are located in the EU or UK and are under 18 we do not use inferences about your gender cohort, interests or friends' interests to personalize the ads you see." See, https://values.snap.com/privacy/ads-privacy

55 https://www.bbc.com/news/articles/c89z2v0pjl3o

56 https://childrescuecoalition.org/educations/safeguarding-children-online-the-importance-of-monitoring-internet-and-social-media-usage/

Key Takeaways at a Glance
Personalisation on the internet enhances children's experiences by tailoring content to their individual needs and interests, supporting meaningful engagement in education, entertainment, and social interaction. It ensures free content availability, which is crucial for maintaining digital rights, especially for children in economically underprivileged situations. Personalisation also fosters inclusivity and accessibility, particularly in diverse countries like India, by addressing varying linguistic, cultural, and socioeconomic needs. It aids children with disabilities through tools like voice interactions and eye-tracking and helps shield them from harmful content while promoting positive behaviours like financial literacy and public health awareness. However, personalisation's benefits hinge on the responsible management of children data. Without proper standards and safeguards, risks like exposure to inappropriate content, excessive screen time, commercial targeting of children, and privacy violations can emerge. Achieving a balanced approach is critical- one that leverages personalisation's advantages while safeguarding children's privacy, rights, and safety in the digital ecosystem.

3. Understanding Personalisation Across Use Cases

In this chapter, we will discuss specific use cases of the internet for children, how personalisation through behavioural monitoring happens in each case, potential benefits and risks to children in each case, and measures that can be put in place to ensure that behaviour monitoring benefits children.

Education

One of the critical areas where personalisation enhances digital access is in enhancing children's learning capabilities. It facilitates self-regulated online learning that enables children to set goals, follow individualised learning paths, and access materials tailored to their preferences and enhance learning outcomes.[57]

Further, by deploying educational data mining techniques, online activity tracking extracts knowledge from large amounts of student-generated content to predict student performance, identify at-risk students, and improve instructional design.[58] Some examples of online tracking methods on education platforms include:[59]

- **Learning Analytics Platforms**: systems that collect and analyse data from online assessments, quizzes, and surveys in order to provide insights into the learning outcomes, patterns, preferences and challenges of students and teachers.
- **Screen recording and monitoring software:** applications that capture and record the screen activity of students and teachers during online classes with the objective of verifying identity, attendance, and participation. These can also detect cheating and plagiarism attempts during online exams.

These tools can enhance the educational environment and should be retained, as they contribute to the positive development of students while ensuring fairness and accountability.

---

57 Thanyaluck Ingkavara, Patcharin Panjaburee, Niwat Srisawasdi, Suthiporn Sajjapanroj, The use of a personalized learning approach to implementing self-regulated online learning, Computers and Education: Artificial Intelligence, Volume 3, 2022, 100086, ISSN 2666-920X, https://doi.org/10.1016/j.caeai.2022.100086.

58 Yaw Boateng Ampadu, *Online Activity Tracking in Educational Institutions,* Online Identity – An Essential Guide, Rohit Raja and Amit Kumar Dewangan, Eds., Apr. 10, 2024, DOI: 10.5772/intechopen.1003084 [Ampadu]

59 Id at page 2.

The online education space has evolved tremendously through the use of online tracking software, which provides more individualised instructions, higher student engagement, enhanced teacher effectiveness, and prediction of student performances.[60] The data collected from tracking individual student progress can also be aggregated to give larger insights into curriculum and policy improvements.[61] Being able to monitor each student's learning process can give teachers and schools insights into where each student is falling short and what they could do to increase attentiveness (whether it's through changes to teaching styles, and curriculums, or incorporating more community-building and hands-on exercises).

Personalisation of learning

During our conversations, a stakeholder shared the use of tracking in promoting "accelerated learning" which focuses on motivating students with grade-level work rather than rushing through the curriculum. It involves timely, targeted support ("just-in-time" interventions) to address specific gaps in learning. For instance, instead of revisiting entire missed units, personalisation can help teachers prioritise essential skills required for upcoming grade-level content and provide tailored support to reinforce key concepts. This approach allows students to continue learning the current grade material while receiving on-demand assistance as needed.

Innovative personalised learning can help children grasp new topics and deepen their understanding with a conversational learning companion that adapts to their unique curiosity and learning goals. It can help navigate complex concepts with an interactive guide and make connections to enhance their understanding through learning aids.[62]

60 Ampadu at page 3-6.

61 Id at page 6.

62

While tracking student behaviour can definitely ensure greater engagement, such mechanisms give rise to certain risks. These risks can vary depending on the tracking technology deployed by the organisation. These include:[63]

- Social Media Monitoring: observing and analysing students' engagements and behaviours on social media platforms, with the objective of gaining an in-depth comprehension of their non-academic social interactions and activities.
- Mobile device tracking: monitoring students' usage patterns, app utilisation and location data.
- Significant concerns regarding the privacy of minors, especially when utilised without appropriate consent mechanisms.[64]

Considering that use of behaviour monitoring in education is contingent on collection of sensitive data of children, service providers need to ensure they deploy extremely efficient data security practices. This is particularly important considering India's low level of digital literacy and some prominent EdTech platforms allegedly engaging in predatory practices by profiling children for commercial purposes.[65] Additionally, these technologies are limited by the socio-economic context in which they are employed.[66] In a country where students do not possess the same level of access to technology, these technologies can further amplify the digital divide experienced by students.[67] Excessive use of technology in education has also been linked with ignorance of emotional and social skills in learners, which are important for success in work and life.[68]

Under Part A of the Fourth Schedule of the Draft DPDP Rules, educational institutions are exempted from the prohibition on behaviour monitoring and tracking as long as the data processing is solely for fulfilling educational purposes and ensuring the safety of children. While in the right spirit, these exemptions must be carefully implemented. As discussed, while tracking enhances learning, it raises risks, including mobile device tracking, profiling, and privacy concerns, especially when appropriate safeguards are lacking.

---

63 Ampadu at page 3-4.

64 Page 8, Ampadu.

65 '*Worst Decision of My Life'*: Byju's accused of driving parents into debt with predatory practices, Scroll, Dec. 17, 2022, https://scroll.in/article/1039797/worst-decision-of-my-life-byjus-accused-of-driving-parents-into-debt-with-predatory-practices

66 Page 7, Ampadu.

67 Id.

68 https://www.theguardian.com/sustainable-business/2015/dec/24/is-technology-in-the-classroom-good-for-children

Potential way forward regarding personalisation in education sector

Considering the potential benefits and risks of behaviour monitoring and tracking on children in the education sector, while a blanket prohibition is certainly not desirable, a blanket exemption may also not be entirely suitable. Children below a certain age may be unable to actively discern which technology on an edtech platform (or even which edtech platform) is trustworthy. At the same time, teenagers (aged 13-17 years) may be able to confidently navigate risks, distinguish safe from risky platforms, and understand the purposes of data processing. Thus, children's age can serve as a benchmark to design graded exemptions from behaviour monitoring. When designing the exemption to behavioural monitoring and tracking within the education sector, policymakers should also consider factors like:

- safeguards to ensure that data is only collected and processed to ensure the delivery of the promised service; and
- safeguards to ensure adequate data security.

Health and well-being

Teenagers often have more difficulty accessing health, particularly mental health, services for sensitive matters, causing them to live in a state of relative health 'information poverty,' compared to adults.[69] They are often interested in finding information about health topics like exercise/diet, sexual health, and alcohol/drug misuse.[70] Since the advent of the internet, it has long served as a source of health information in addition to the traditional sources accessed by teenagers (like parents, peers, friends, mass media, and books).[71] Stakeholders during consultations for the study revealed that these issues are becoming of increasing importance in India as well, and our inferences for the Indian urban youth are limited by the absence of detailed studies on related issues conducted in the Indian context.[72]

Studies have reported that teenagers mention the ability to access health information previously denied to them is crucial.[73] This also results in empowering them with information when they visit a medical professional,[74] although this phenomenon could

[69] Gray et al., *Health Information Seeking behaviour in adolescence: the place of the internet*, Social Science & Medicine 60 (2005) 1467-1478. [Gray]

[70] Gray at 1468.

[71] Id.

[72] Thakan, S., Mehta, A., & Singh, L., *eHealth – information-seeking behaviour among school going adolescents through internet, International Journal Of Community Medicine And Public Health*, *9*(6), 2570–2573 (2002) https://doi.org/10.18203/2394-6040.ijcmph20221536.

[73] Page 1471, Gray.

[74] Id.

also be observed in adults. Compared to traditional media, the benefit of the internet is the personalisation of information, a feature that makes the internet much more salient as a resource.[75]

For instance, personalised nutrition advice intervention through digital-based technologies leads to a healthier diet, resulting in improved overall well-being with the benefits of convenience, sustainability, and cost-effectiveness.[76] On the other hand, personalised speech therapy can help children overcome early developmental challenges, such as communication and behaviour development.[77]

Personalised tools also empower young people by providing confidential access to essential health information on topics like sexual health and mental well-being. Programmes like health-tracking apps illustrate how digital tools can promote healthier behaviours through targeted, real-time support. Such platforms engage users emotionally and rationally, fostering self-awareness and encouraging positive change. Additionally, social media and digital communication help young people maintain connections across various communities, offering a constant support network.[78]

Personalisation in health

A stakeholder pointed out that personalised mental health support offers distinct advantages and is significantly more effective, avoiding generic support, which may not meet users' specific needs. They highlighted that behavioural monitoring plays a crucial role in this support. For instance, if a teenager mentions feeling unhappy at home or experiencing bullying at school, these data points can be captured to provide personalised meditation suggestions. If their emotional indicators, such as levels of anger or sadness, exceed a certain threshold, then they can facilitate expert intervention. They also emphasised that the data remains highly protected and is not used in any other manner except when a high score is detected, and even then the response is limited to offering the user the option to chat with a mental health professional.

75 Id.

76 Celis-Morales, Carlos & Livingstone, Katherine & Marsaux, Cyril & Macready, Anna & Fallaize, Rosalind & O Donovan, Clare & Woolhead, Clara & Forster, Hannah & Walsh, Marianne & Navas-Carretero, Santiago & San-Cristobal, Rodrigo & Tsirigoti, Lydia & Lambrinou, Christina-Paulina & Mavrogianni, Christina & Moschonis, George & Kolossa, Silvia & Hallmann, Jacqueline & Godlewska, Magdalena & Surwiłło, Agnieszka & Mathers, John. (2016). Effect of personalized nutrition on health-related behaviour change: evidence from the Food4Me European randomized controlled trial. International Journal of Epidemiology. 46. Dyw186. doi: 10.1093/ije/dyw186.

77 https://www.butterflylearnings.com/

78 https://innovativepublichealth.org/blog/benefits-of-technology/

With the recent increase in awareness of mental health-related issues, several campaigns have been launched on social media platforms to reach users struggling with mental health issues.[79] One such example is the #HereForYou campaign launched on Instagram and Snapchat to help users find support online and offline for preventing and recovering from mental illnesses.[80] In more recent years, Bournvita's #GetTheMessage campaign was launched to draw attention to children's mental health and well-being.[81] Scholars have recognised the importance of matching the right content to the right user as a way of amplifying these campaigns – highlighting the importance of behavioural tracking and personalisation on these platforms.[82] Moreover, teenagers have not only consumed and benefitted from such content, they have actively utilised the internet to create apps that would reach other children battling mental health issues, while giving them a platform to voice their concerns, often anonymously.[83]

However, behavioural tracking may act as a double-edged sword, with posing as risks in several cases.[84] Some of the experts we consulted during the study highlighted the negative impacts of behavioural tracking/monitoring and targeted advertisements on children's mental health. For instance, they highlighted that personalisation of content can lead to a decrease in self-regulation at the individual level and a decrease in in-person social interactions. As per studies and expert interviews, there have been concerns that increased screen time may lead to internet addiction in young people.[85] Similarly, they also pointed out that personalised and targeted ads may encourage an increase in promoting impulsive buying behaviour in children, which can negatively impact their decision-making and autonomy. Moreover, the prevalence of considerable misinformation on the internet about mental health and well-being could harm teenagers, if relied on without due care.

---

79 Saha et al, *A Computational Study of Mental Health Awareness Campaigns on Social Media,* TBM 2019;9:1197-1207, doi: 10.1093/tbm/ibz028 [Saha]

80 Saha at 1198.

81 Cadbury Bournvita Highlights kids' emotional well-being through digital campaign, ETBrandEquity.com, Oct. 11, 2021, https://brandequity.economictimes.indiatimes.com/news/advertising/cadbury-bournvita-highlights-kids-emotional-well-being-through-digital-campaign/86930429

82 Saha at 1204.

83 Indian teen builds app to help peers address mental health issues, overcome bullying, South China Morning Post, Nov. 7, 2023, https://www.scmp.com/yp/discover/lifestyle/features/article/3240489/indian-teen-builds-app-help-peers-address-mental-health-issues-overcome-bullying; 17 Year Old Launches Mental Health App Targeted at Teenagers, CXOToday News Desk, Oct. 4, 2022

84 See generally, Bozzola E, Spina G, Agostiniani R, Barni S, Russo R, Scarpato E, Di Mauro A, Di Stefano AV, Caruso C, Corsello G, Staiano A. The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks. Int J Environ Res Public Health. 2022 Aug 12;19(16):9960. doi: 10.3390/ijerph19169960. PMID: 36011593; PMCID: PMC9407706.

85 A. Orben, *Teenagers, Screens and Social Media: A Narrative review of reviews and key studies*, Social Psychiatry and Psychiatric Epidemiology, 55(4) (2020), pp. 407-414

Notably, digital service providers are implementing interventions that modify behavioural monitoring activities in a way which supports digital well-being by offering tools for digital self-control, which can be beneficial for children. These tools, such as timers and lock-out mechanisms, help children manage their technology use by enabling self-regulation. Experts highlighted how children use digital wellness tools to track and manage their screen time. They are generally aware of how to monitor their usage, and this becomes particularly important as they approach their exams, allowing them to balance study time with other activities effectively. The use of digital phenotypes[86], which are created using digital trace data, can help in capturing the breadth of each individual's behaviours, thereby enabling adolescent wellbeing.[87]

Can children regulate their own screen time?

Researchers have been creating versions of applications for young children to help them manage their internet consumption and screen time. Several others have also been working with preschoolers and parents, where both parent and child work together to create a "device-based playtime together." Experts found that parental involvement during the planning state reduced the need for later parental intervention by 93 percent.[88] Researchers think that communication between parents and children about technology can actually be empowering.

Though strict parental controls may seem like the solution, many such solutions seem to a teenager (aged 13-17 years) like their parent sitting and watching them while they use the internet. While this may work for a tween (children between 9-12 years), it certainly does not work with teenagers. Excessive parental control over teenagers' lives could be counterproductive as well – parental control settings could restrict teens from accessing important things like information about their sexuality.

The trade-off for the policymaker lies in allowing these spaces to flourish while establishing proper guardrails to ensure the privacy and security of data is protected. As experts point out, bad things happen online as they do offline – policymakers must focus on programmes that would make for greater parent-child cooperation and digital literacy to ensure children are not helpless in the face of trouble.

86 Digital phenotypes are real-time measurement of user data from their personal digital devices, used to assess behaviours and psychological states, revealing a close link between digital phenotypes and users' well-being. Digital Phenotyping, Available at: https://www.hsph.harvard.edu/onnela-lab/research/

87 Mubashir Sultan, Christin Scholz, Wouter van den Bos, *Leaving traces behind: Using social media digital trace data to study adolescent wellbeing,* Computers in Human Behavior Reports, Volume 10, 2023, 100281, ISSN 2451-9588, https://doi.org/10.1016/j.chbr.2023.100281.

88 https://faculty.washington.edu/alexisr/PlanAndPlay.pdf

The Fourth Schedule of the Draft DPDP Rules suggest exemptions to healthcare institutions, including clinical establishments, mental health professionals, educational institutions, and crèches to process data for providing health and crèches & related services for monitoring safety and tracking locations during transit. While in the right spirit, these exemptions must be carefully implemented. It is essential to balance the potential benefits of these exemptions with the need for robust privacy protections to safeguard children from the adverse effects of unregulated behavioural monitoring.

A balanced approach to way forward: Several experts highlighted the need for behavioural monitoring in the areas of mental health and well-being. Teenagers might particularly benefit from platforms that monitor behaviour to detect signs of depression, anxiety, or other mental health issues. Such monitoring could facilitate timely interventions or recourse provision.[89] However, ethical implications and the boundaries of such monitoring were also pointed out as well as the need for clear guidelines. These may include maintaining confidentiality, privacy, and autonomy of the individual, beneficence/non-maleficence, and legal considerations such as mandated reporting.[90]

The balance between the benefits and risks arising from behavioural monitoring in the area of "health-related information", is clearly a difficult one to strike. The needs of children from different age groups must weigh heavily as a factor for policymakers as they proceed. While children younger than eight years may not use online health related services, for tweens (9-12 years) and teenagers (13-17 years), this functionality can be crucial to their mental and physical well-being. Consequently, behaviour monitoring and tracking to detect signs of depression, anxiety, or other mental health issues, must be allowed with adequate transparency and disclosures. This could be enabled through leveraging the possibility of purpose specific exemptions under section 9(4) of the Act.

In addition, teenagers (aged 13-17 years) could be provided greater freedom, agency, and autonomy to benefit from online health and wellness services, after ensuring that the specific service providers indulge in verifiably safe processing. Policymakers can ensure this by obtaining self-certification from service providers on some pre-specified indicators of data minimisation, purpose limitation, processing, sharing, and security, and conducting continuous monitoring.

89 Aledavood, T., Torous, J., Triana Hoyos, A.M. *et al.* Smartphone-Based Tracking of Sleep in Depression, Anxiety, and Psychotic Disorders. *Curr Psychiatry Rep* 21, 49 (2019). https://doi.org/10.1007/s11920-019-1043-y

90 Sussman, Nicole & Dejong, Sandra. (2018). Ethical Considerations for Mental Health Clinicians Working with Adolescents in the Digital Age. Current Psychiatry Reports. 20. 10.1007/s11920-018-0974-z

Safe spaces for marginalised communities

Tracking or behavioural monitoring can also serve as a "matching tool" to connect people with similar interests. For some communities, this might be more important than for others. Stakeholders under the study discussed the importance of accessing information by marginalised groups and other vulnerable populations like women in distress, LGBTQIA+ youth, children in abusive homes, etc. These views were corroborated by studies like the Report from OfCom UK, which showed that many 11-18 year-olds identifying as LGBTQIA+ found safe spaces for community online as opposed to offline.[91] The sense of 'community' also prevailed in other teenagers aged 13-17 who suffered from chronic health issues, with many stating that they sought support online, as per a recent study by OfCom UK.[92]

In addition, some experts pointed out that behavioural monitoring is beneficial for children who have experienced trauma or are in vulnerable situations, such as those affected by gender or sexual violence. This monitoring is crucial for developing care plans that address their educational, social, and health needs. Behavioural monitoring is often useful here, both for ensuring that resources reach the target populations and connecting users with similar experiences.

Personalisation on the internet also offers young people tailored, meaningful digital experiences that address their unique needs and support positive engagement. For marginalised youth, such as LGBTQ+ teens, personalised digital experiences can provide meaningful support. Through personalisation, platforms are able to recommend content, groups, and discussions that align with users' interests, helping youth connect with supportive networks. For these youth, online spaces offer vital communities for support and shared experiences, mitigating isolation they may encounter in their daily lives.[93]

However, despite the internet being their 'safe space,' it is not considered completely safe. Several stakeholders indicated that persons from marginalised communities encountered hate comments, misinformation, and trolls as they struggled to find themselves and their community. There have also been instances of impersonation, misuse, and abuse of such platforms, which apparently offer safe spaces for marginalised communities, including children.

---

91 OfCom, *Children and Parents: Media Use and Attitudes Report,* Apr. 19, 2024, https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-media-use-and-attitudes-2024/childrens-media-literacy-report-2024.pdf?v=368229. See page 18.

92 OfCom, *Children and Parents: Media Use and Attitudes Report,* Apr. 19, 2024, See page 26.

93 https://innovativepublichealth.org/blog/benefits-of-technology/

Can the internet offer a safe space for marginalised communities?

Children begin experiencing curiosity about their sexuality as early as ages 12-13 but often do not have a place to turn to. India has many stories, like that of Roshni from Jamshedpur, who, after learning about queerness on the internet, became comfortable with her sexual identity. The information she found online helped her become more herself. On the other extreme, though, a 16-year-old makeup artist, Pranshu Yadav, was trolled mercilessly for wearing a saree online. Pranshu eventually died of suicide.[94] Several people from the LGBTQIA+ community have reported that social media helped them discover their true identities, meet similar people, form a sense of community, and gather relevant information. This has been true for Dalit and Adivasi queer people as well, who are perhaps more susceptible to dangers and trolls – both offline and online.

Given the importance of ensuring the welfare of children belonging to marginalised communities and the insufficiency of offline safe spaces available for them, particularly teenagers, it is vital to ensure that genuine online platforms that offer such spaces are preserved, with adequate safeguards, due diligence, and accountability standards to prevent misuse. During our consultations, many stakeholders also mentioned that any misuse cases must be dealt with by putting additional safeguards. Overall, a need to take a balanced approach was pointed out, with experts agreeing that there were some necessary use cases.

Beneficial monitoring to support young marginalised communities

Behaviour monitoring can become beneficial monitoring for young marginalised users if credible dedicated platforms focus on using such monitoring to match people belonging to marginalised communities. They must assure to have in place adequate safeguards to prevent impersonators and online predators from accessing their platforms, have robust safety and security standards to prevent misuse of data, and should not process the data for any purpose other than matching. The safeguards such platforms put in place could be periodically tested, along with their data usage and sharing models. Such a balanced approach, which can uphold the well-being of children, could be operationalised through the possibility of exemptions carved into sections 9(4) and 9(5) of the Act.

[94] https://www.hindustantimes.com/htcity/cinema/16yearold-queer-child-pranshu-dies-by-suicide-due-to-bullying-did-we-fail-as-a-society-mental-health-expert-opines-101701172202794.html

Age-estimation services

Indian households typically have multiple users, including children, who share devices and online services. Consequently, it can become challenging to distinguish which member of a household is using a device or online service at any given moment. Behavioural biometrics, such as screen touching and keystroke dynamics, can be used to identify the nature of the device's or services' user at a given moment, including if the user is likely to be a child or not. A child's age can be further deduced through various behavioural indicators, such as search queries related to school subjects. These age estimation techniques through behavioural monitoring can effectively classify users without explicitly collecting verifiable age data, such as government IDs, providing a less intrusive means of identification. Several stakeholders during our discussions mentioned that some prominent platforms use such techniques to estimate user age and direct appropriate content to them.

These behavioural biometrics aiming to detect age are usually designed to tailor technology interfaces towards children (e.g., widget layout) and to improve parental control options.[95] Furthermore, it has been pointed out that the use of geolocation technology for monitoring children's movements (especially young children) offers parents a convenient means of ensuring their safety and managing household logistics. This technology provides peace of mind by allowing parents to check their children's whereabouts without direct communication, contributing to a sense of security.[96]

However, the use of behavioural monitoring for age estimation has also been critiqued as being flawed by design, since it requires large amounts of sensitive data to work.[97] Criticism of the technology has also pointed to the fact that age estimation techniques may cause further harm by stereotyping children into what is "normal" behaviour versus what is not, as compared to adults.[98]

---

95 Finnegan et al. Systematic Reviews (2024) *The utility of behavioral biometrics in user authentication and demographic characteristic detection: a scoping review* 13:61 https://doi.org/10.1186/s13643-024-02451-1; CUTS International, *Global Technological Developments in Age Verification and Age Estimation,* Briefing Paper, bp-global-technological-developments-in-age-verification-and-age-estimation.pdf (cuts-ccier.org)

96 Mavoa, Coghlan, and Nansen (2023): *It's About Safety Not Snooping* https://doi.org/10.24908/ss.v21i1.15719

97 See page 21, European Digital Rights, *Online Age Verification and Children's Rights,* October 4, 2023, https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf

98 Ibid

Moreover, during our stakeholder consultations, it was also pointed out that the effectiveness of these age appropriation methods through behavioural monitoring is questionable in countries like India. These methods might be effective in more digitally advanced contexts, but given India's digital divide, limited awareness, and potentially high cost of these technologies, they may require significant adaptation for implementation. The effectiveness of these age appropriation methods will also vary based on the volume and nature of usage data. Furthermore, the availability of historical data plays an important role in developing reliable age estimates.

Despite the issues described above, it is crucial that India not shut itself off from the possibility of deploying these age-estimation technologies, provided appropriate safeguards are in place. This has been indicated in Part B of the Fourth Schedule, which exempts data fiduciaries from the prohibitions for age verification, aligning with the parental consent provisions and due diligence requirements under Rule 10. These requirements mandate data fiduciaries to obtain verifiable parental consent before processing a child's personal data and conduct due diligence, such as verifying the identity and age of the parent providing the consent. It may be possible to test the effectiveness and risks of such technologies in a safe and controlled environment by taking the regulatory sandbox approach. Those solutions that pass the regulatory sandbox test could be permitted, particularly for teenagers (aged 13-17 years), and subject to them adopting adequate safeguards and not misusing data. Fiduciaries may also be encouraged to conduct regular data protection impact assessments and audits and ensure that such solutions do not violate children's privacy while prioritising their safety and well-being.

Social media

Like the rest of the internet, social media feeds are personalised for each individual user.[99] This is done through algorithms that filter and prioritise content based on each users' data. Customisation using personal data and individual specific insights makes the platform experience more relevant since individuals are shown content that they may be interested in. Feeds are customised through algorithms that consider a user's "demographics, online habits and preferences, activities of friends and connections, and a number of other factors."[100]

[99] Ragnhild Eg et al, *A Scoping Review of personalized user experiences on Social Media: The Interplay between Algorithms and Human Factors,* Computers in Human Behaviour Reports, Vol. 9 (Mar. 2023), doi: 10.1016/j.chbr.2022.100253

[100] Ibid.

It is the personalisation of social media that makes these platforms relevant and compelling to users.[101] Some experts have also referred to it as an "evolutionary process" where popular content is prioritised, and content that receives less attention is relegated to the backend.[102] Personalisation is so native to online spaces like social media that many young users may be unable to imagine the internet without it.

Routine social media use is positively related to "mental health, self-related health, social well-being, and resilience."[103] Studies have found that teenagers said social media made them feel more connected to their friends' lives it is like having a support network.[104] Findings from interaction with young users by CUTS also show that they use the internet in areas enhanced by personalisation.

Additionally, personalisation also enables 'discovery' – many young users do not automatically think of things to look for. Quoting a teenager from a study on algorithmic literacy, they do not simply "wake up and think about soccer, and therefore start looking for soccer" [for example]. They are also not opposed to scrolling through some content to find something that may pique their interest.[105] Young users also actively personalise the current affairs they'd like to see through active engagement with content, increasing their participation as citizens.[106] They take learning from social-media platforms as well, accessing educational content, awareness posts, and similar materials, often facilitated by personalisation that caters to their preferences.[107] A stakeholder during consultation pointed out that personalisation can provide young users access to free services, available on its platform, such as education and awareness resources.

---

101 G. Aydin, Role of personalization in shaping attitudes towards social media ads, International Journal of E-Business Research, 14 (3) (2018), pp. 54-76

102 L. Pangrazio, N. Selwyn, It's not like it's life or death or whatever": Young people's understandings of social media data, Social Media + Society, 4 (3) (2018), pp. 1-9

103 Bekalu MA, McCloud RF, Viswanath K. Association of social media use with social well-being, positive mental health, and self-rated health: disentangling routine use from emotional connection to use. *Health Educ Behav*. 2019;46(2_suppl):69–80. doi: 10.1177/1090198119863768.

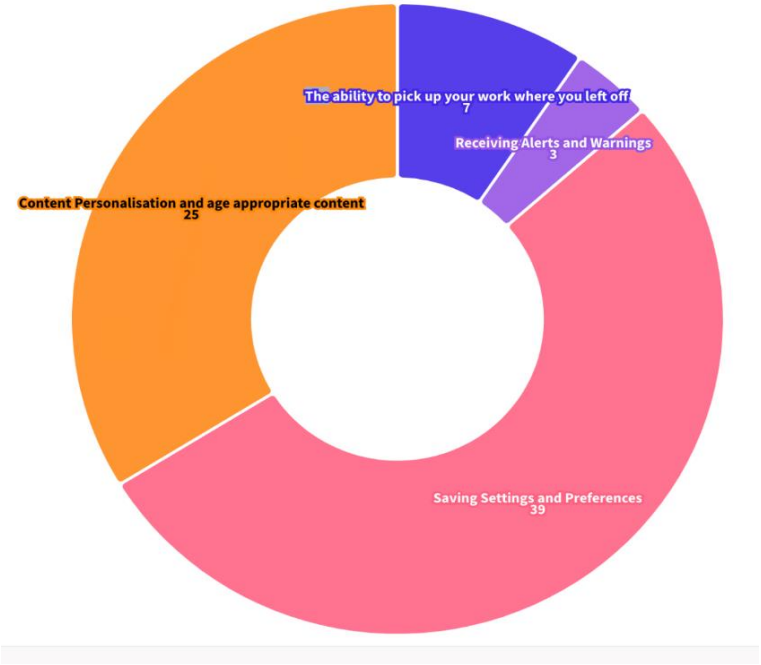
104 Anderson M, Jiang J. Teens' Social Media Habits and Experiences. Pew Research Center. Available from: https://www.pewresearch.org/internet/2018/11/28/teens-social-media-habits-and-experiences/.

105 Swart, J. (2021). Experiencing algorithms: How Young People Understand, Feel About, and Engage With Algorithmic News Selection on Social Media. Social Media + Society, 7(2). https://doi.org/10.1177/20563051211008828

106 Ibid

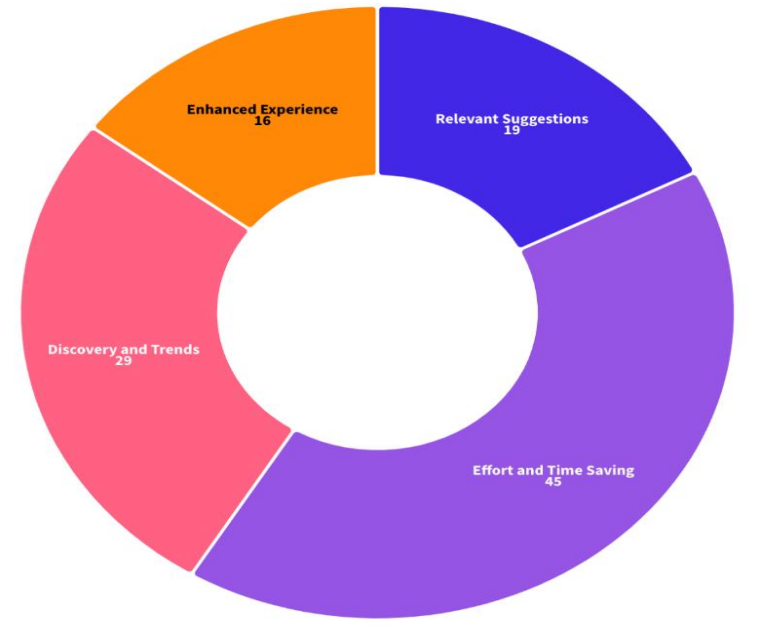
107 https://csic.georgetown.edu/magazine/social-media-reshaping-todays-education-system/

Young users' perspectives on the usefulness of behaviour monitoring (n = 74 responses for 25 respondents)



Young users also thought targeted advertisements provided significant benefits to them by saving their time and effort and increasing the chances of finding products that they may like or are up to the latest trends.

Young Users on the usefulness of targeted advertising (n=109 responses for 25 respondents)



In our interactions, experts and civil society organisations also thought that content optimisation and personalisation were some of the most significant benefits of behavioural monitoring for children. This was being enabled by remembering preferences like styles and formats like colour themes, saving progress in work, games, and other activities, and functionalities like marking emails read, and distinguishing them from unread emails.

Our findings point to an intrinsic value in receiving content that is tailor-made according to one's preferences - humour ('memes'), creativity (hobbies-related content), current affairs, or even simply a trending dance reel endorsing the latest makeup product.

Personalisation supports innovation and entrepreneurship

Behavioural monitoring also supports innovation by facilitating the design and usage of new features and functionalities by young users on the internet. By monitoring how young users engage with current features, platforms can identify areas for improvement or supply entirely new features that can enhance the user experience. In our stakeholder consultations, experts also highlighted the importance of behavioural monitoring for young content creators, as it recommends their content to the right audience. This becomes particularly important as India's content creation economy continues to grow.[108]

Young people today are also emerging as prolific creators, actively shaping online spaces. For example, children today are emerging as content creators in several areas, such as Do-It-Yourself (DIY) projects, showcasing their talents like dance, skits, music, and visual arts. In this way, platforms enable tweens (children between 9-12 years) and teenagers (children between 13-17 years) to express themselves, build communities, with the support of their parents or guardians.[109] Keeping in with the creative and entrepreneurial spirit, teens are also building apps to help their fellow teenagers get mental health help.[110] The Ofcom report of the UK also highlighted that children felt like creating their own content was a popular way of expressing their creativity online.[111] 54 percent of the parents surveyed by OfCom also felt like being online

[108] Majority of Gen Zs consider themselves as content creators: YouTube report - Economic Times

[109] Journal of Content, Community & Communication, Vol. 20 Year 10, June, 2024 [ISSN: 2395-7514 (Print)], DOI: 10.31620/JCCC.06.24/06; Leading YouTube channels by child content creators across India as of February 2022, by subscribers

[110] See supra note 87

[111] OfCom, *Children and Parents: Media Use and Attitudes Report,* Apr. 19, 2024, https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-media-use-and-attitudes-2024/childrens-media-literacy-report-2024.pdf?v=368229. See page 19.

helped their child develop creative skills.[112] This may be true for a large part of India as well.

However, research also points to the negative implications of excessive personalisation and the opacity of algorithms on social media.[113] While personalisation achieves a highly customised feed, researchers point out that this may, in fact, be a part of the problem. By limiting the kind of content that a user interacts with, excessive personalisation can influence preferences, opinions, and worldviews.[114] This is particularly concerning for children, whose opinions and views are easily malleable. This is tied to how opaque these algorithms are. Studies have pointed out the general unawareness about how these algorithms work, pointing out that many people are unaware that certain content is absolutely absent from their feeds.[115] However, people may be more aware of these patterns now.[116]

There are also concerns about social media normalising young people's relationships with harmful products. For example, some experts believe that harmful products that can be pushed on children using invasive behavioural monitoring and individual tracking techniques can include products aimed to mislead younger people, like weight loss products and other misleading products that could harm their health. Ironically, this perhaps highlights a need to not prohibit targeted advertising entirely, but to use tracking and behavioural monitoring appropriately to ensure young users are only shown age-appropriate ads.

In our interactions, young users also thought that privacy breaches were one of the biggest risks of behavioural monitoring for children, followed by feelings of manipulation, pressure, and exploitation. Young users also underscored their annoyance when 'content was shown to them repeatedly even when they did not look for it.' Research has also linked social media use to depressive symptoms among young women.[117]

---

112 See page 18, OfCom report

113 Ragnhild Eg et al, *A Scoping Review of personalized user experiences on Social Media: The Interplay between Algorithms and Human Factors,* Computers in Human Behaviour Reports, Vol. 9 (Mar. 2023), doi: 10.1016/j.chbr.2022.100253

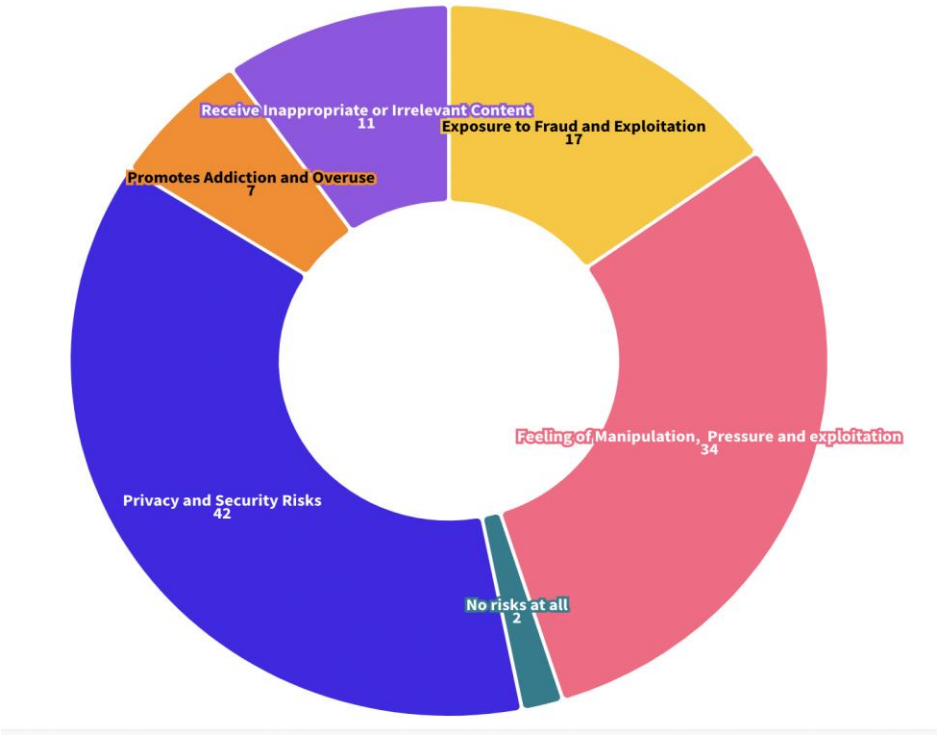
114 Ibid.

115 Eslami et al, *"I always assumed that I wasn't really that close to [her]": Reasoning about Invisible Algorithms in News Feeds*, CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems Pages 153 – 162, https://doi.org/10.1145/2702123.2702556

116 J.H. Schmidt et al, *How do intermediaries shape news-related media repertoires and practices? Findings from a qualitative study,* International Journal of Communication, 13 (2019), pp. 853-873

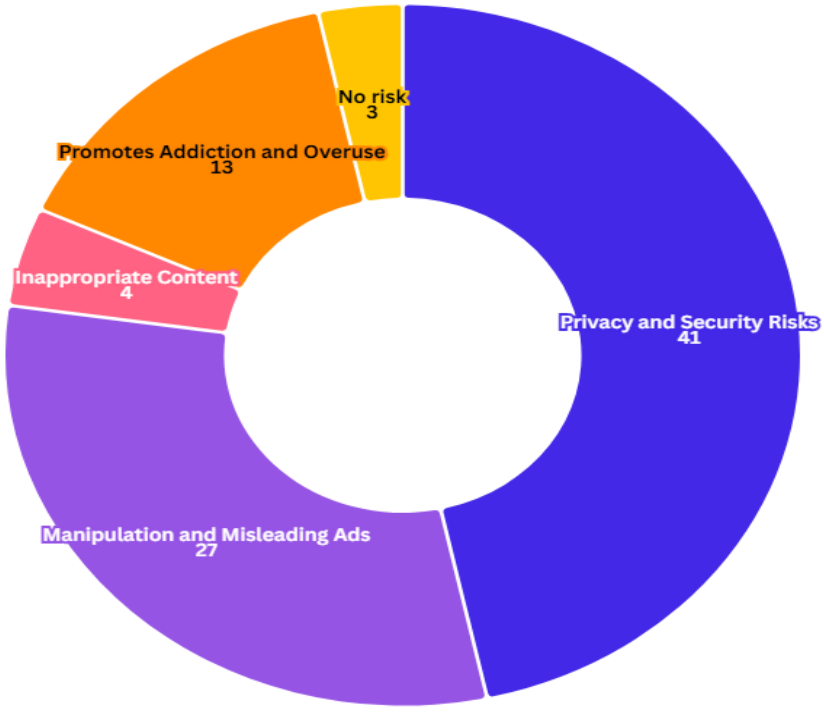
117 https://www.bbc.com/news/articles/c89z2v0pjl3o

Young users' perspectives on risks of tracking or behavioural monitoring (n=113 responses for 25 respondents)



Similarly, privacy and security risks, and manipulation and misleading ads, with respect to targeted advertisement were reported as top risks by children of behaviour monitoring as seen below.

Young users' perspectives on risks of targeted advertisements (n=88 responses for 25 respondents)



Some of the stakeholders that we consulted mentioned that the level of personalisation and addiction made possible by behavioural monitoring and targeted advertising creates an environment where the agency of the brain to make rational decisions is compromised. Some pointed out the heightened concerns amongst parents and guardians on increasing consumerism among children. Organisations like WHO and UNICEF also emphasise that children often lack critical reasoning skills, making them more vulnerable to manipulation.[118] There are also several ethical concerns – the potential for exploitation and children's inability to fully grasp the implications of these practices. Research highlights that these practices influence children's attitudes and behaviours.[119]

An expert, on the other hand, admitted that children do, in fact, *want* personalisation on social media. Discussions on personalisation on social media give rise to conversations about the agency that users can exercise over the algorithms. Providing users effective agency over algorithms can potentially reduce the risks of excessive personalisation - information overload, excessive screen time, and so on.

Effective agency can be enabled through transparency about data collection and usage, related benefits and risks, and empowering users to make informed choices about these aspects can help shape their feed. Experts have pointed out that at present, their agency is restricted to some extent due to platform design, although users are not entirely powerless and have some agency over their choices.[120]

According to research, teenagers' confidence can be improved by explicit disclosures about how their actions impact the content they are shown. Platforms should be encouraged to "keep promises" – to have their algorithms reflect users' choices. This could help manage the feelings of reduced control and instate a sense of agency.[121] They can also be encouraged to conduct regular data protection impact assessments and audits to maintain transparency and accountability.

In India, these efforts would be needed at a larger scale and from user-friendly perspectives. Disclosures in vernacular languages, through pictorial, audio, and video

---

118 Tinhinane Medjkoune, Oana Goga, and Juliette Senechal. 2023. Marketing to Children Through Online Targeted Advertising: Targeting Mechanisms and Legal Aspects. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23), November 26–30, 2023, Copenhagen, Denmark. ACM, New York, NY, USA, 16 pages. https://doi.org/ 10.1145/3576915.3623172

119 Packer J, Croker H, Goddings AL, Boyland EJ, Stansfield C, Russell SJ, Viner RM. Advertising and Young People's Critical Reasoning Abilities: Systematic Review and Meta-analysis. Pediatrics. 2022 Dec 1;150(6):e2022057780. doi: 10.1542/peds.2022-057780

120 Swart, J. (2021). Experiencing algorithms: How Young People Understand, Feel About, and Engage With Algorithmic News Selection on Social Media. Social Media + Society, 7(2). https://doi.org/10.1177/20563051211008828

121 Page 8, Swart.

depictions, would ensure a greater understanding of how personalisation works on social media. Platforms could also engage with grassroots and consumer organisations that work with rural populations to ensure greater delivery and awareness of transparency practices. Effective transparency, greater agency and control, and assurances by platforms to use algorithms only for the purposes and in a manner authorised by users, particularly teenagers, could form the bedrock of designing exemptions under section 9(4) of the Act and allowing behaviour monitoring and targeted advertisements.

Potential way forward regarding personalisation on social media

Stakeholder consultations pointed out that teenagers (children aged 13-17 years) may be much more discerning of behaviour monitoring and targeted advertisements than children below this age group. Thus, the differences between children of different age groups, the agency and privacy preferences of children above a certain age, and the need to treat them as consumers as well as creators on the internet must be taken into account. Moreover, it was pointed out that teenagers (aged 13-17 years) may be less vulnerable to online content than children of lower age groups. Teenagers may be able to differentiate between harmful and beneficial content and engage with the content. However, the discernment level may also vary based on the platform involved. Some researchers argue that algorithms are understood through use.[122] For instance, a group of teenagers may be able to identify sponsored posts on social media, but not on search engines.

Consequently, treating all young users below 18 years alike may not be appropriate owing to their differential development levels and understanding (or lack thereof) of how personalisation works on social media, and it may be advisable to empower teenagers (aged 13-17 years) with more relevant information and tools to make informed decisions about the extent of personalisation on social media. Personalisation as a concept is a double-edged sword, with different utilities for different age groups. While children from 0-8 may not benefit from personalisation much, children above this age group could derive great value from the technology. This age-appropriate approach may be relevant to carve out exemptions under section 9(5) of the Act once the platforms assure verifiably safe data processing. They must put in place mechanisms to collect and process only such data required for providing services and as approved by teenagers.

[122] Page 3, Swart.

Gaming

Online gaming is also a prominent use case for young users. It has been pointed out that profiling player behaviour through in-game actions enables personalisation of gameplay, tailoring the experience to different player types and enhancing overall satisfaction. This personalisation allows players to receive automated feedback, customised guidance, and real-time game adjustments, all of which contribute to a more enjoyable experience.[123] Data mining techniques help identify variations between players, further supporting the customisation of gaming experiences.[124] Experts also highlighted that free-to-play games, which cater to a broad audience, particularly minors, often employ player analytics for features such as matchmaking[125] and engagement tracking.[126] These practices may fall under behavioural monitoring. Several gaming platforms have been taking steps to leverage the potential of behaviour monitoring. For instance, AI-driven player profiling detects behaviours like cheating, ensuring a fair and engaging environment.[127]

This does not mean that gaming is not susceptible to risks. Some risks related to gaming overuse include, trapping and cyberbullying by predators, exposure to inappropriate and violent content, addiction, leak or misuse of personal information compromising children's safety, impact on mental health and development of anxiety and social isolation, and physical health issues, among others.

---

123 C. Stephanidis et al. (Eds.): HCII 2020, LNCS 12425, pp. 631–643, 2020. https://doi.org/10.1007/978-3-030-60128-7_46

124 Ibid.

125 In online multiplayer games, matchmaking, enabled by algorithms, assign players to play with (in team) or against, based on factors like skill level and preferences to ensure balanced and competitive matches.
Huang, Yan and Jasin, Stefanus and Manchanda, Puneet, 'Level Up': Leveraging Skill and Engagement to Maximize Player Game-Play in Online Video Games (November 14, 2018).
SSRN: https://ssrn.com/abstract=2885082 or http://dx.doi.org/10.2139/ssrn.2885082

126 Engagement tracking monitors player behaviours such as playtime, login frequency, and in-game purchases to gauge their level of engagement. This data is used to enhance the gaming experience and also provide usage reminders to remind players to play responsibly.
Ferreira CP, González CSG, Adamatti DF. Player Engagement Analysis of a Business Simulation Game from Physiological, Psychological and Behavioral Perspectives: A Case Study. *Applied Sciences*. 2022; 12(19):10143. https://doi.org/10.3390/app121910143

127 A. Faraz, J. Mounsef, A. Raza and S. Willis, "*Child Safety and Protection in the Online Gaming Ecosystem,*" *in IEEE Access*, vol. 10, pp. 115895-115913, 2022, doi:0.1109/ACCESS.2022.3218415

Safe monitoring in gaming

Numerous tools have been developed by platforms to mitigate threats in online gaming against children, such as content filtering and parental controls, which help prevent contact with children and protect them from child predators. Various methods employing machine learning techniques have been created to detect predatory behaviour, offering potential solutions for detection and protection in these situations.[128] Additionally, detecting predatory behaviour on gaming chat platforms using AI tools is an emerging area made possible through behavioural monitoring.

A broad, blanket ban on behavioural monitoring and tracking of children's data could adversely affect online games by disabling their core features, thereby impacting the overall gaming experience. Personalisation also becomes necessary for giving kids a safe and secure online gaming environment, especially when it comes to predatory behaviour. A ban on all forms of behavioural monitoring might prevent the use of tools designed to protect children which could undermine efforts to safeguard minors online.

Consequently, a nuanced approach is necessary for allowing behaviour monitoring in the gaming industry. As indicated, specific behaviour monitoring solutions can foster safe environments for gamers. Retaining these benefits and allowing them under exemptions envisaged under sections 9(4) of the Act would be essential. In addition, gaming platforms should showcase how they are processing gamers' data, and put in place adequate safeguards to prevent access by third parties, breaches and leakage, to be able to obtain exemptions under section 9(5). This can be done by conducting regular data protection impact assessments and audits.

Music and Podcasts

Tracking or behavioural monitoring is also a practice in the music industry. It allows platforms to recommend familiar music. Spotify, for example, recommends songs based on various inputs. One of these inputs is a "sound profile," which is a combination of the songs users search for, like, and save to their playlists.[129] Curating pertinent information, including music and songs, by the service providers makes the service more relevant, which is one way that personalisation benefits the user. Consumers, including young users, value the delivery of relevant and interesting content effortlessly.[130] Use of music streaming platforms is popular among young

[128] Ibid.

[129] Understanding Recommendations on Spotify, Spotify, https://www.spotify.com/fr/safetyandprivacy/understanding-recommendations

[130] Armstrong CC, Odukoya EJ, Sundaramurthy K, Darrow SM. *Youth and Provider Perspectives on Behavior-Tracking Mobile Apps: Qualitative Analysis.* JMIR Ment Health. 2021 Apr 22;8(4):e24482. doi: 10.2196/24482.

users, particularly those under 18 years of age. Research has shown that young users value this personalisation for its ability to deliver pertinent and interesting content effortlessly, noting that they enjoyed how relevant content appeared without the need for active searching.[131] Personalisation on apps like Spotify, Apple Music, Saavn, etc. effectively obviates the need to actively search and download music. Additionally, these platforms also host several podcasts. These services provide 'discovery' functions and are nowadays instrumental in introducing young users to audio content (music and podcasts) that they may not come across without personalisation. Similar to other content, young users are avid consumers and creators of podcasts. Podcasts are often educational and can expose children to several new fields like literature, science, history, and sports as well as serving as a medium of creative expression.

Additionally, since audio podcasts do not have video, they also present a relatively anonymous way for children to express themselves and be safe online. Like any other content, discovering a relevant podcast (and broadcasting your own to others) relies heavily on behaviour monitoring and targeted advertisements. However, considering podcasts can be made by any individual, the same level of discernment is required while exploring them as is required for any other content to ensure that the young user is not being exposed to harmful ideas or misinformation, in audio format.

Young User's perspectives on entertainment-related Personalisation

According to young internet users in our discussions too, content personalisation based on interests, and receiving recommendations for products similar to the ones being searched, and were the most popular services unlocked by behavioural monitoring. They appreciated how personalisation helped them *"discover relevant gaming apps and music"*, and even products similar to those they had previously searched for, enhancing their overall online experience. Other popular services were remembering settings and preferences and the ability to pick up work where it was left.[132]

PMID: 33885364; PMCID: PMC8103306, Table 3 available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8103306/

131 Bell, A. R., Tennfjord, M. K., Tokovska, M., & Eg, R. (2022). *Exploring the role of social media literacy in adolescents' experiences with personalisation: A Norwegian qualitative study*. Journal of Adolescent & Adult Literacy, 00, 6. https://doi.org/10.1002/jaal.1273

132 Behavioural monitoring enables digital platforms to track and store user-specific configurations, language, theme, or notification settings across sessions, ensuring a personalised experience. It also enables users to resume activities seamlessly by monitoring and saving progress in their work, games, etc., enabling continuity without manually re-entering or resetting data when returning to a service.

Markus Zanker, Laurens Rook, Dietmar Jannach, Measuring the impact of online personalisation: Past, present and future, International Journal of Human-Computer Studies, Volume 131, 2019, Pages 160-168, ISSN 1071-5819, https://doi.org/10.1016/j.ijhcs.2019.06.006

A blanket prohibition on music platforms from undertaking behaviour monitoring and targeted advertisements may not be advisable, and that may deprive young users of the benefits and advantages they derive from such platforms. Consequently, personalisation to the extent beneficial for young users may be permitted under section 9(4) of the Act, while ensuring that the data is processed only in a manner which is necessary to provide such benefits, and is not misused, and is protected from cyber attackers.

Behaviour Monitoring Use Cases: Benefits, Risks, and Recommendations at a Glance

Use Case	Benefits	Risks	Recommendations
Education	Enhanced learning, higher student engagement, prediction of student performance, insights into curriculum and policy improvements, and personalised support for differently abled children.	Privacy and consent concerns due to tracking without appropriate safeguards, the potential to worsen existing inequalities in access to technology, and potential neglect of essential social and emotional skills.	• Implement graded exemptions for behavioural monitoring based on age. • Ensure data is collected and processed only for service delivery. • Implement robust data security measures.
Health & Well-being	Personalised health information, interventions, and support; access to sensitive information on topics like sexual health and mental well-being, early detection of mental health issues, timely intervention, and access to resources.	Potential decrease in self-regulation, reduced in-person social interactions, internet addiction, exposure to inaccurate health information and vulnerability to harmful content, and data security concerns with health data collection.	• Allow behaviour monitoring for mental health and well-being purposes with transparency and disclosures. • Implement age-appropriate exemptions. • Promote digital literacy on health information and critical evaluation skills. • Ensure robust data security and privacy measures for sensitive health data.

Use Case	Benefits	Risks	Recommendations
Safe spaces for marginalised communities	Community building**,** connecting individuals with similar interests, particularly for marginalised groups, access to online spaces for LGBTQIA+ youth, children in abusive situations, and other vulnerable situations.	Exposure to hate comments, harassment and abuse**,** misinformation, and trolls, Misuse of platforms through impersonation, exploitation, and abuse of safe spaces intended for vulnerable communities.	• Permit behavioural monitoring for credible dedicated platforms focused on providing services to marginalised communities. • Implement strict safeguards to prevent misuse, impersonation, and online predation. • Ensure robust safety and security standards and restrict data processing.
Age estimation services	Enables tailored age-appropriate content and features, improved options for parental monitoring and management of children's online activities, and facilitates safety & security through geolocation for monitoring children's movements and ensuring their safety.	The effectiveness of age estimation methods may be limited in certain contexts, privacy risks due to the collection of large amounts of sensitive data for age estimation, potential for reinforcing stereotypes and discriminating against children based on their online behaviour.	• Test age-estimation technologies in a controlled environment (e.g., regulatory sandbox). • Implement exemptions for verified age-estimation solutions with robust safeguards against data misuse and discrimination. • Promote transparency and user control over age-related data collection and processing.
Social media	Helps users discover relevant content and trends, personalised feeds; enhances connection with friends and communities,	Risk of data misuse, exploitation, and manipulation through targeted advertising, filter bubbles, limited exposure to diverse	• Empower users with transparency and control over personalisation algorithms.

Use Case	Benefits	Risks	Recommendations
	provides platforms for children to express themselves, build communities, and unlock opportunities to monetise their talents.	perspectives, potential influence on opinions and worldviews, negative psychological effects with concerns about addiction, self-image issues, and peer pressure.	• Implement age-appropriate safeguards against data misuse and manipulation. • Promote media literacy and critical thinking skills to navigate social media responsibly. • Address mental health concerns and provide support resources for online interactions.
Gaming	AI-driven player profiling detects cheating and ensures a fair environment, content filtering, and AI-powered detection of predatory behaviour, enhanced gameplay through matchmaking and engagement tracking for improved user experience.	Potential for excessive gaming and negative impacts on physical and mental health, concerns about the collection and use of player data for unintended purposes, and in-app purchases can lead to financial risks.	• Allow behaviour monitoring for safety and fairness purposes in gaming. • Implement robust safeguards against data misuse and addiction. • Promote responsible gaming practices and provide parental control tools. • Regulate in-app purchases and protect children from financial exploitation.
Music & Podcasts	Personalised recommendations help users discover new music and podcasts, algorithms curate content based on user preferences, and platforms for creating and accessing podcasts on various topics.	Risk of encountering harmful or age-inappropriate music and podcasts, concerns about the collection and use of listening data for unintended purposes, filter bubbles and potential narrowing of musical tastes.	• Allow personalisation while ensuring data is processed responsibly and not misused. • Implement age-appropriate content filtering.

4. Impact of complete prohibition on Personalisation

Challenges in frictionless access and discovery of relevant content

During consultations for the study, many stakeholders understood the risks of unregulated personalisation through behavioural monitoring and targeted advertising for children. At the same time, they acknowledged the benefits of personalisation done right. Stakeholders disagreed with the proposal of complete prohibition on personalisation, highlighting the role that behavioural monitoring plays in facilitating a positive holistic internet experience for young users.

Personalisation has many benefits, including fostering access, reducing discovery costs, allowing young users to shape their own spaces, express their creativity, and consume and create relevant and tailor-made content. A complete prohibition on behaviour monitoring and targeted advertisements may impede the capabilities of platforms to collect and process user data for personalisation, attract advertisers and content providers, and invest in providing a safe and personalised online experience to children.

In a recent study in India with respect to access to online content by children, the majority of children and parents surveyed believed that a lack of personalised content feed on the internet would negatively impact children's online experience. In this study, children were informed that social media and other platforms personalise content based on their online activities such as likes, search/browsing cookies, and history. If this changes, children would no longer see tailored content, and instead are likely to be shown all content chronologically. More than 50 percent of children thought this change would harm their experience.[133]

Similarly, as per the study, children's preferences with respect to targeted advertisements vary across age and gender. Not all categories of ads are equally preferred by all children. It was believed that lack of personalisation, which may arise from restrictions on the processing of children's data, could make the ads less useful.[134]

In another survey, it was revealed that key benefits of personalisation, as perceived by consumers were reduced irrelevant advertising, discovering new products, and online

[133] Singh, M., Nishant, Sachdeva, G., Tewari, A. (2024). *Balancing Consent & Customisation*. Youth Ki Awaaz, available at: https://www.youthkiawaaz.com/dpdpsurvey/

[134] Singh, M., Nishant, Sachdeva, G., Tewari, A. (2024). *Balancing Consent & Customisation*. Youth Ki Awaaz, available at: https://www.youthkiawaaz.com/dpdpsurvey/

search and shopping becoming faster and easier. All these benefits could go away, or search costs may escalate, if personalisation is prohibited. Going forward, most consumers are likely to prefer a world with fewer, but personalised advertisements.[135] In the absence of behaviour monitoring and targeted advertisements, users including children may have to encounter a deluge of relevant and irrelevant content and advertisements, wherein segregating the two may become quite time and resource intensive. Furthermore, parents would also lose the ability to set personalised restrictions and monitor their child's online activity effectively.

As discussed above, personalisation enhances children's learning by enabling tailored educational materials, self-regulated learning, and access to regional cultural content like music and folklore, fostering better outcomes and cultural appreciation. In this regard, stakeholders during our consultation emphasised that these benefits, supported by revenue from personalised content and ads, might disappear or become chargeable if personalisation is prohibited. Such a ban could also limit access to meaningful and affordable digital resources, disproportionately impacting marginalised children and reducing innovation in educational and cultural tools.

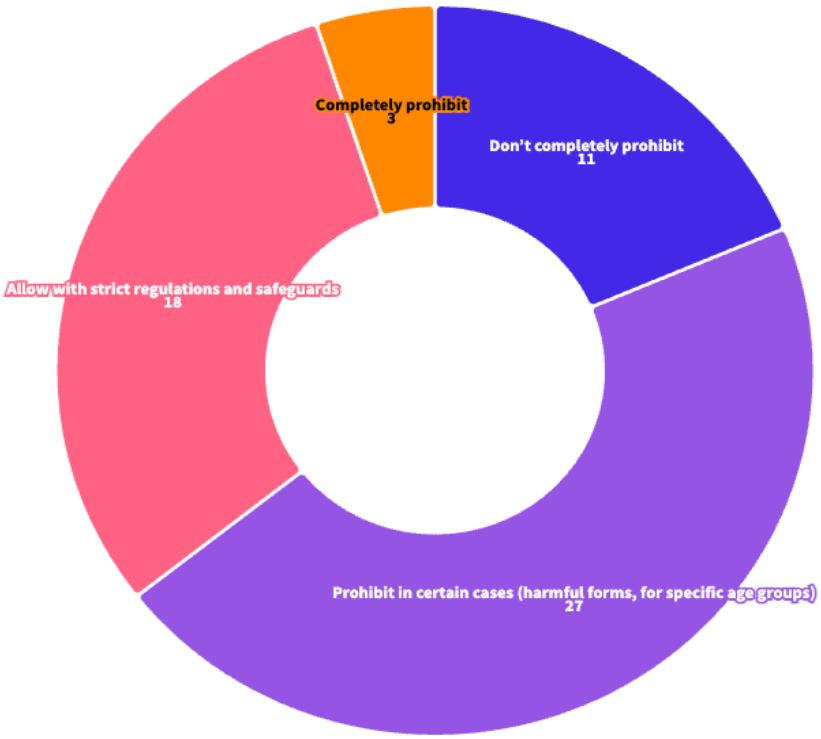
Experts on the impact of complete prohibition on tracking or behavioural monitoring (n=93 responses for 35 respondents)

[135] https://www.adlucent.com/resources/blog/71-of-consumers-prefer-personalized-ads/

Experts also agreed that a complete ban or prohibition would stifle access, and innovation, which may counterintuitively thwart efforts to enhance children's safety online. In addition, as per stakeholders, there would be a significant impact on services that rely on personalisation – that would include several platforms that children use for entertainment and social networking. For instance, imagine a world where Instagram does not show tailored content, but any and all sorts of content available on the internet that may or may not interest a user. In another example, one may also imagine a depersonalised Netflix displaying entertainment content that is not tailor-made, which would perhaps look similar to how cable television functioned in the early years.

In our consultations, some stakeholders advocated for a risk-based approach to prohibition, mentioning that practices of monitoring, tracking and advertising should be prohibited only if they lead to significant harm. This highlights the necessity of implementing suitable measures under section 9(4) and section 9(5) of the Act.

Experts on approaches to tracking or behavioural monitoring (n=59 responses for 35 respondents)

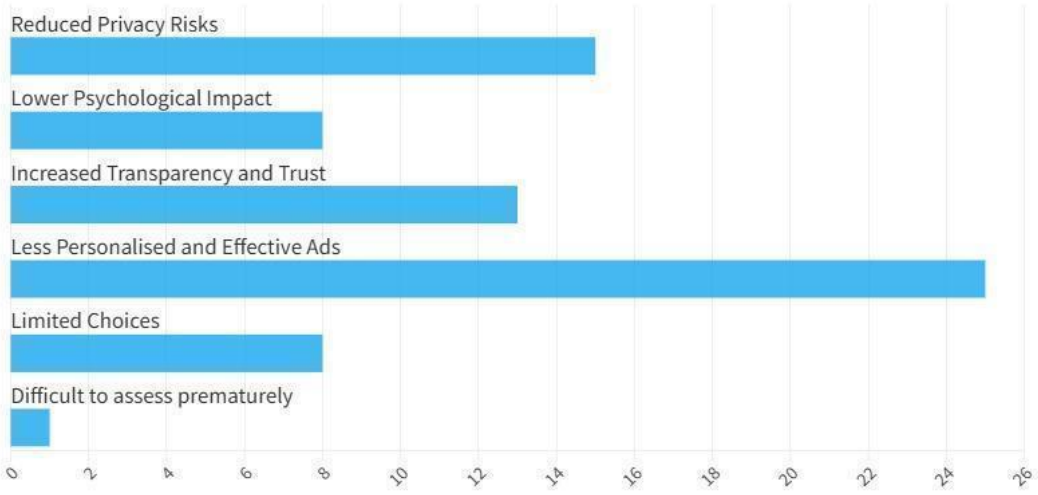


With respect to targeted advertisements, young users reacted positively and indicated that targeted advertisements helped save time by suggesting things they like and reducing efforts to find relevant information and/or products. This becomes particularly relevant for marginalised young users from backgrounds who might not have adequate resources to access the internet at their leisure. A few experts also pointed out that not all targeted advertising is harmful. For example, showing age-appropriate content can be beneficial and less intrusive than random ads, which may include inappropriate ad content. Cohort-based advertisements, which do not use cookies have therefore been suggested as a balanced possible way forward by experts, and other jurisdictions alike.[136]

Research has also pointed out that people across groups share concerns about their data privacy and show similar levels of acceptance regarding personalised digital services and the use of private data for personalisation. On average, personalised services are more acceptable than the collection of personal information or data. Without personalisation, platforms might find it difficult to provide customised services to users, including children.

Addressing such an 'acceptability gap' would require transparent personalisation that minimises the use of personal data, and respects people's preferences, should be easy to adjust.[137]

Experts on effects of Cohort ads (n=75 responses for 35 respondents)

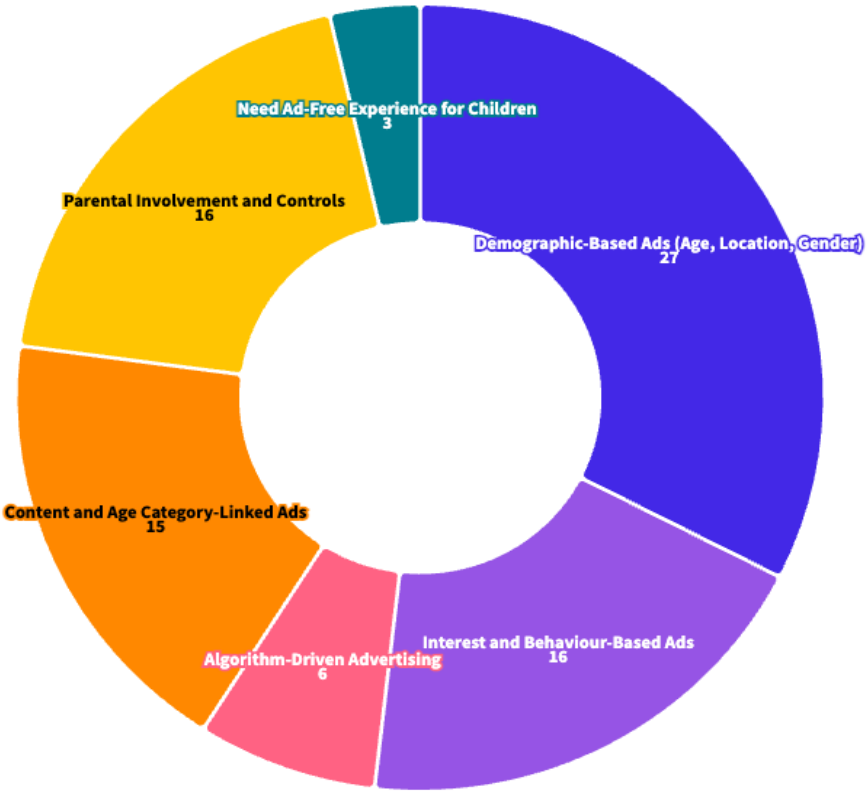


[136] CNIL, Alternative to Third-Party Cookies: What Consequences Regarding Consent?, November 23, 2021, https://www.cnil.fr/en/alternatives-third-party-cookies-what-consequences-regarding-consent

[137] https://www.nature.com/articles/s41599-021-00787-w

In addition, sufficient controls must be in place to ensure that children below a certain age do not see advertisements for inappropriate content. Experts mentioned that inappropriate content is not just limited to drugs and alcohol but can also include ads for harmful practices like misleading "detox" weight loss products, etc.

Experts on the ideal scope of advertising (n=83 responses for 35 respondents)



As discussed earlier, it is important to preserve children's agency, both in the form of safeguarding their 'positive' (enabling) rights and 'negative' (protective) rights. It is crucial to uphold their fundamental rights to access the internet, privacy, free expression, self-determination, and protection from exploitation.[138] It would not be prudent to regulate the internet on behalf of children solely based on how adults understand them. It would be important to let young users make informed decisions about their personal information and digital interactions. This is informed by the understanding that not all children are the same and that children of different age groups must be treated differently.

[138] United Nations Children's Fund (UNICEF), March 2017. Discussion Paper Series: Children's Rights and Business in a Digital World, Privacy, Protection of Personal Information and Reputation Rights, available at https://archive.crin.org/sites/default/files/unicef_crb_digital_world_series_privacy.pdf

Approaches by other jurisdictions

It is to be noted that several jurisdictions and international organisations, including the European Union, United Kingdom, UNICEF, and many others, have opted to regulate the use of personalisation through behaviour monitoring, only for the best interests of the child, and platforms claim to have appropriate measures in place to protect the child from any harmful effect.[139] While there are differences in specificity of the approaches, best practices include:[140]

- Personalisation options should be switched off by default, unless there is a compelling reason for it to be activated in the best interests of the child.
- Any personalisation must be accompanied by appropriate safeguards to protect the child from harm, such as exposure to harmful content.
- Privacy settings for behavioural advertising should always be offered.
- Services should differentiate between types of personalisation for different purposes, and provide clear information when personalisation is activated. Different types of personalisation should not be bundled into one consent notice or privacy setting.
- What happens to the child's personal data and any risks that may arise from it must be clearly explained. Age-appropriate prompts to seek assistance from an adult must also be provided. Personalisation should not be activated if children are uncertain or don't understand.
- Additionally, children's data should not be used for automated decision-making or advertising purposes unless it is in their best interests, wherein it could be used with appropriate measures to safeguard against psychological or physical harm.
- Children should be provided options to tailor how content is personalised. This could include content controls.
- If profiling is on, appropriate measures must be put in place to safeguard the child (in particular from inappropriate content). These could include contextual tagging, algorithmic risk assessments, transparent information on how content is recommended, robust reporting procedures, and elements of human moderation.
- Assurances must be obtained from, and due diligence must happen on, third-party platforms with whom children's data is shared. It is essential to ensure that such third parties are not using children's data in ways that are not in the children's best interests.[141]

---

139 5 Rights Foundation, *Approaches to children's data protection, A comparative international mapping,* available at: https://5rightsfoundation.com/wp-content/uploads/2024/08/Approaches-to-Childrens-Data-Protection-.pdf

140 5 Rights Foundation, *Approaches to children's data protection, A comparative international mapping,* available at: https://5rightsfoundation.com/wp-content/uploads/2024/08/Approaches-to-Childrens-Data-Protection-.pdf

141 ICO Children's code recommendations on profiling for content delivery and service personalisation. See, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-

It has been reported recently that the Australian Federal Government is considering a ban on social media for children under 16, which could make Australia the first country with such an age restriction. This is because social media is apparently taking kids away from real friends and real experiences. However, experts argue that this move could create unintended consequences, including isolating children, reducing access to essential support networks, and encouraging a shift toward riskier unregulated platforms.

Experts argue that the ban could result in several negative outcomes. Many young people - especially those from marginalised groups - rely on social media for support, advocacy, and connection. For instance, LGBTQIA+ youth, rural teens, and children with disabilities often use social platforms to connect with others who share similar experiences. A blanket ban could isolate these groups, depriving them of crucial social resources.[142] Similar concerns could arise if personalisation and behaviour monitoring are completely prohibited under the DPDP Act.

As indicated earlier, children increasingly gain knowledge about news from social media,[143] and it has become an important space for student activism, enabling teens to connect with others, learn about global issues, and organise for positive change. A ban on social media could isolate an already lonely generation, eroding their sense of personal and political agency and restricting their ability to develop essential skills for the future.[144] A prohibition could push children and teenagers toward less regulated, alternative platforms, operating outside the fringes of regulatory scrutiny, which could expose them to harmful content and serious risks.[145] Similar concerns may arise if personalisation is not permitted under the DPDP Act.

guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/best-interests-framework/profiling-for-content-delivery/

142 https://www.theeducatoronline.com/k12/news/social-media-ban-may-impact-vulnerable-youth--expert/286053

143 https://www.westernsydney.edu.au/newscentre/news_centre/more_news_stories/opinion_young_australians_increasingly_get_news_from_social_media,_but_many_dont_understand_algorithms

144 https://www.theguardian.com/commentisfree/2024/nov/14/australia-social-media-ban-anthony-albanese-government

145 https://au.reset.tech/uploads/ACRT-Open-letter-re-social-media-bans.pdf

Key Takeaways at a Glance
A complete prohibition on behavioural monitoring and targeted advertisements for children could have significant negative consequences on their online experience. Without personalisation, children could experience irrelevant content, reducing their ability to engage meaningfully online and also limit innovative service to them. It can also expose children to content not suited for their age, posing risks to their online safety. A depersonalised internet experience would also resemble traditional media, lacking the tailored experiences that digital platforms offer. It may also drive children towards less regulated, riskier platforms. A more balanced approach is needed, focusing on clear consent mechanisms and robust privacy protections for children. A risk-based framework that weighs the advantages and risks of personalisation is preferable to a blanket ban. Many jurisdictions have also adopted child-centric regulations with safeguards, and have not enforced outright prohibition.

5. The Draft Digital Personal Data Protection Rules, 2025

The Draft Digital Personal Data Protection Rules, 2025 released for public consultations by the Ministry of Electronics and Information Technology (MeitY) propose in Rule 11, along with the Fourth Schedule, specific instances where certain data fiduciaries are exempted from Section 9(3) of the Act.

Exemptions for Classes of Data Fiduciaries: Part A of the Fourth Schedule of the Draft Rules proposes exemptions for certain classes of data fiduciaries from specific restrictions.

- clinical establishments, mental health establishments, and healthcare professionals, including allied healthcare professionals, to process data for providing health services to protect a child's health;
- educational institutions to process data for educational purposes and the child's safety; and
- crèches, day-care centres, and related transportation services to process data for ensuring children's safety and tracking their locations during transit.

While these exemptions try to strike a balance between regulatory compliance and protecting children, there are concerns that these are too narrow, due to their limited applicability and potential to hinder beneficial use cases for children. The narrow scope of exemptions does not take into account scenarios where data processing could significantly benefit children, such as enabling personalised educational content or tailoring online experiences to enhance engagement and learning outcomes. Further, as discussed above, young users today often turn to social media platforms for learning, leveraging personalisation to access educational materials, awareness campaigns, and similar resources tailored to their interests and preferences. Similarly, other beneficial use cases of internet-based services such as offering safe services to marginalised young groups, enabling the discovery of new interests and ability to tailor their feed, cannot be neglected.

Thus, there may be merit in exploring more exemptions, which are use-case specific and inherently beneficial for young users. These exemptions could be guided by a risk-based framework, differentiated by age groups, and aligned with the principles of safe and responsible data processing.

Exemptions for Data Processing Activities: Part B of the Fourth Schedule suggests exemptions for specific data processing activities. These entities are exempted from

the prohibition on behavioural monitoring or tracking and targeted ads and can process children's data

1. If it is strictly necessary for the exercise of legal powers, duties, or functions aimed at benefiting the child under any Indian law.
2. If required for the provision of subsidies, benefits, certificates, licenses, or other legitimate services under Section 7(b) of the DPDP Act for the child's welfare.
3. For the creation of user accounts, such as email accounts to facilitate communication.
4. For protection of the child's well-being by preventing access to information likely to cause any detrimental effect on the child.
5. Age verification to confirm a data principal is not a child, is in line with the parental consent provisions and due diligence requirements under Rule 10.

These exemptions also require further clarification. Exemptions 3 and 5 could inadvertently result in continuous monitoring to determine whether the data principal is a child. As discussed earlier, this becomes particularly challenging in households where devices or accounts are shared, making it difficult to differentiate between a child and a parent. To address these concerns, including AI-based age estimation for exemption under Part A of the Schedule could be a potential solution.

Additionally, exemption 4, aimed at ensuring harmful information is not accessible to children lacks clarity regarding the definition of "detrimental" content, the mechanisms required, and the extent of monitoring necessary. The ambiguity raises concerns about who decides what constitutes harmful content, as perceptions may vary across children, parents, and platforms. It is also unclear whether the tracking permitted under this exemption will involve real-time behavioural monitoring and content filtering. This also raises further complexities, such as whether all content will be scrutinised and whether even borderline content, such as references to sensitive topics like terrorism or sexuality, will be restricted-even when intended for awareness purposes. Moreover, platforms may need to distinguish between the intent of such content, which could increase compliance costs for them. This may also inadvertently lead to continuous monitoring of children's online activity, profiling based on their interests, and potential overreach in content regulation. These concerns highlight the need for precise guidelines to address such ambiguities.

6. Necessity of an Age-Appropriate Framework for Personalisation

While discussing behaviour monitoring and targeted advertising with children, policymakers must recognise that all children may not perceive such personalisation similarly. Many stakeholders and comprehensive research have pointed out that children under 18 are not and must not be treated the same.

Studies have shown that children's perceptions of the internet and advertising, in general, are vastly different and that they can be categorised into distinct developmental stages. For instance, "children below age four or five cannot distinguish commercial from non-commercial content on television; before age seven or eight, they do not realise that the purpose of the commercial is to sell products."[146] This developmental stage is presented even more starkly on the internet, where there may not necessarily be any divide between commercial and non-commercial content.[147]

On the other hand, research suggests that teenagers (aged 13-17 years) are generally more capable of critical thinking, risk assessment, and understanding consequences than younger children. This developmental stage allows for a more nuanced understanding of online interactions. For instance, teenagers, aware that their feeds are personalised, show preferences towards personalised content. They are also able to discern the difference between an advertisement and regular content, highlighting the developmental differences between them and tweens (aged 9-12 years).[148] Moreover, teenagers are more likely to understand and manage online risks, such as privacy settings, cyberbullying, and inappropriate content. Children across age groups may not also have the same level of awareness or skills to protect themselves online.[149] In terms of "psychosocial maturity," studies suggest that it develops rapidly in adolescence/ teenage years.[150]

However, a higher developmental stage and capacity to appreciate nuance also brings risks for teenagers. It has been argued that teenagers face unique mental health

---

146 Patricia M. Greenfield (2004). *Developmental considerations for determining appropriate Internet use guidelines for children and adolescents. , 25(6), 751–762.* doi:10.1016/j.appdev.2004.09.008 [Greenfield]

147 Id at 753.

148 Sweeney, E., Lawlor, M.-A., & Brady, M. (2022). Teenagers' moral advertising literacy in an influencer marketing context. International Journal of Advertising: The Review of Marketing Communications, 41(1), 54–77. https://doi.org/10.1080/02650487.2021.1964227

149 https://www.simplypsychology.org/piaget.html

150 Costello et al, *Adolescents and Social Media: Privacy: Brain Development, and the Law,* J. Am. Acad. Psychiatry Law 44:313-21, 2016.

challenges associated with online interactions, including issues related to self-image and peer pressure, which are less prevalent among younger users.[151] While 16-year-olds can be capable of acting like adults, they are also susceptible to impulsive behaviours, social coercion, and online harm.[152] Such unique challenges might also nudge platforms to design services appropriate for teenage users, as distinct from users below their age groups. Therefore, it becomes important that teenagers (aged 13-17 years) are able to access personalised content, undertake healthy and safe online interactions and, access mental wellbeing and support services.

According to a recent OfCom study, children are also able to recognise that apps collect their data and use it to show them personalised content, and 46 percent agreed with the statement that they *"... [are] happy for apps to use the information they have collected about me to decide what to show me."*[153]

However, there exists confusion about the attitudes of children about apps collecting their data, particularly in the minds of teenagers (aged 13-17 years).[154] This is because, owing to their developmental differences, younger children (below 13 years of age) may not exhibit any major 'confusion' about their data being shared, especially since they do not fully comprehend the risks and benefits associated with personal data sharing and processing. Second, the 'confusion' among teenagers points to a certain level of discernment (safety, security, and autonomy considerations) within them regarding their personal information.

As opposed to unquestioningly sharing their data, the 'confusion' expressed by teenagers could be evidence that they are trying to make the trade-off between quality of service and protecting their personal data (even if they do not know clearly what to choose), and take an informed decision about data sharing, while taking into account access, privacy, and data protection related concerns. This also corroborates with the developmental theory - children under the age of 18 differ significantly in terms of their understanding of the internet, with teenagers showing a greater understanding of the trade-offs involved. Additionally, our discussions with young internet users corroborate this assertion to a large extent.

Regarding targeted advertising, developmental differences dictate how children perceive ads. Research indicates that children from the age of two to eight tend to 'buy into' the fantasies presented by advertisers (the perceptual stage), while children

---

151 https://www.pewresearch.org/internet/2018/09/27/teens-and-cyberbullying/

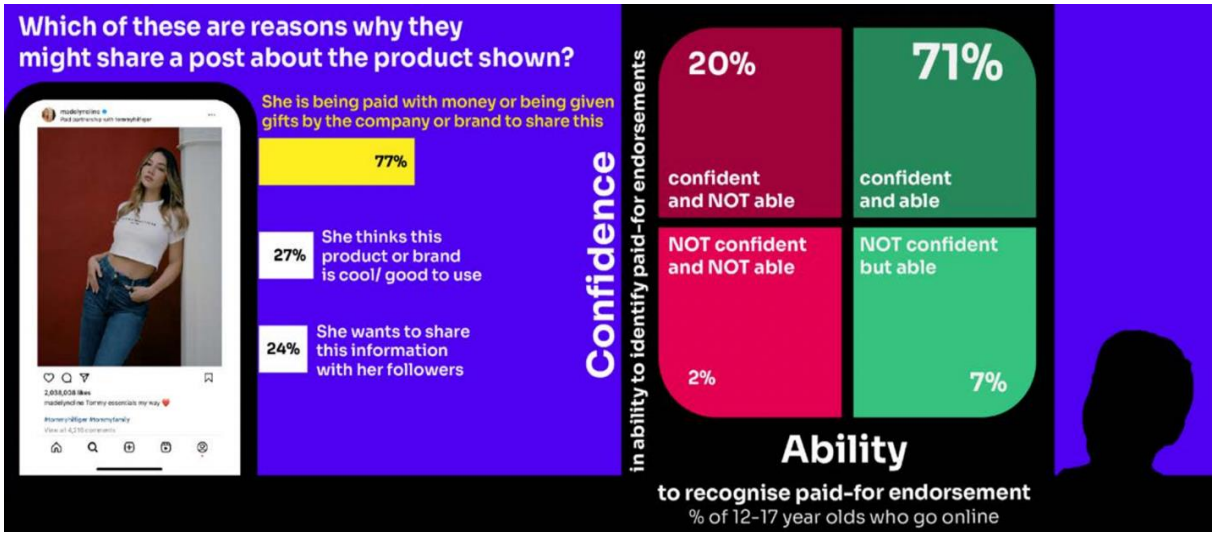
152 Costello et al, *Adolescents and Social Media: Privacy: Brain Development, and the Law,* J. Am. Acad. Psychiatry Law 44:313-21, 2016.

153 OfCom, *Children and Parents: Media Use and Attitudes Report,* Apr. 19, 2024, https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-media-use-and-attitudes-2024/childrens-media-literacy-report-2024.pdf?v=368229. See page 31.

154 Ibid.

between ages nine to twelve begin to understand the information given in a commercial (the analytical stage), and often grasp that advertisers intend to sell a product through a commercial.[155] Children aged thirteen and upward, however, are likely to understand advertisers' motives, to a large extent.[156] Consistent with this theory, the OfCom report stated that teenagers (aged 13-17 years) recognised influencer marketing.[157] Consequently, the standards that service providers may need to deploy to ensure the well-being of children, may differ with their age, and be influenced by development and maturity levels.

However, not all studies conducted outside India can be directly transplanted into the Indian context due to certain cultural, digital literacy, access and socioeconomic differences. In a study on the impact of television advertising conducted with tweens (aged 9-12 years) residing in New Delhi, they reported a lower level of discernment regarding advertising, with the majority of the sample not understanding the persuasive intent of the advertisement.[158] They were also more prone to falling for misinformation.[159] This appears to be consistent with the developmental differences between tweens and teenagers.



Source: OfCom, Children and Parents: Media Use and Attitudes Report, 2024

[155] Sandra L. Calvert, (2008). *Children as Consumers: Advertising and Marketing. The Future of Children, 18(1), 205–234.* doi:10.1353/foc.0.0001

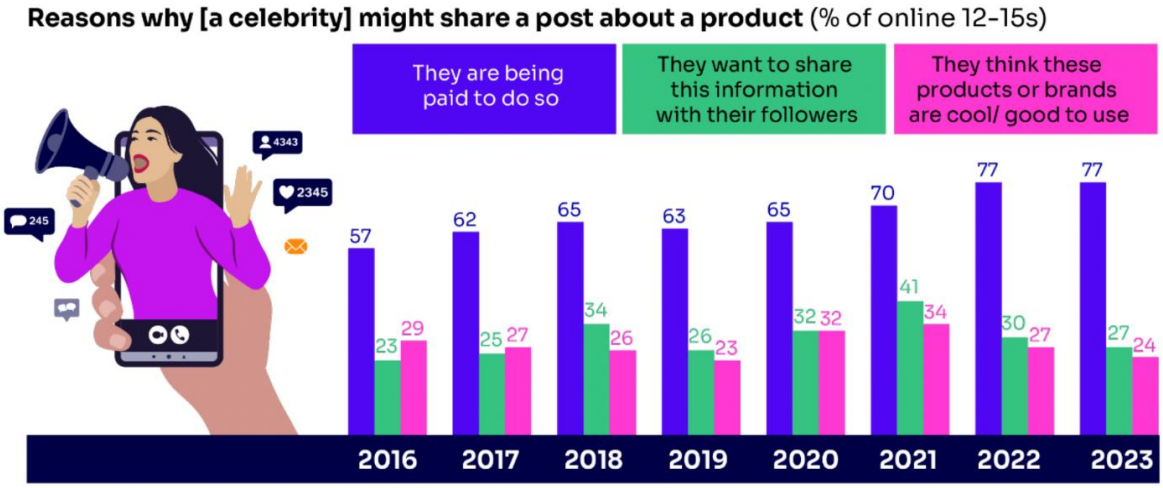
[156] See page 215, Sandra L. Calvert, (2008). *Children as Consumers: Advertising and Marketing. The Future of Children, 18(1), 205–234.* doi:10.1353/foc.0.0001

[157] See page 40, OfCom report.

[158] Kulveen Trehan (2018): Advertising literacy to empower the young media consumers in India: a critical exploration of the advertised mind, Media Asia, DOI: 10.1080/01296612.2018.1448522

[159] Ibid.

With the increasingly pervasive role the internet plays in our lives, awareness levels of teenagers aged 13-17 years have also increased over time. Developmental levels of children vary significantly over time. As children grow older, they tend to become more discerning consumers of the products they are advertised.[160] The figure below illustrates the trends from 2016 to 2023:



Note: question-wording changed slightly over the years, and the methodology changed in 2020 and 2021, so trend is indicative

Source: OfCom, Children and Parents: Media Use and Attitudes Report, 2024

Consequently, like the EU, India should consider children as active consumers and users of technology, not merely passive recipients.[161] The Better Internet for Kids (BIK+) strategy adopted in May 2022 by the European Union aims to ensure that children are "*protected, respected and empowered online in the new Digital Decade*".[162] The objectives include protecting children from harmful and illegal content, empowering them to protect themselves in situations of vulnerability, allowing their active participation and respecting them by giving them a say in their digital environment, with the aim to "foster innovative and creative digital spaces."[163] The EU has put this into practice by creating a 'leaflet' in a child-friendly format that helps children understand the core issues and how to contribute to solving them. This approach articulates the trade-offs while carefully acknowledging the benefits and risks of the internet – explaining the same to both adults and children.

[160] Ibid.

[161] See page 15, Lievens, Livingstone et al, *Children's Rights and Digital Technologies,* available at https://eprints.lse.ac.uk/84871/1/Children%27srightsanddigitaltech_revised_clean%20final.pdf. [Lievens]

[162] A European Strategy for a better internet for kids (BIK+), European Commission, https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids

[163] Ibid.

Key Features of Child-Friendly Leaflet from EU BIK+ Strategy

Source: Child Friendly Version of European Strategy for Better Internet for Kids[164]

For these reasons, it has been argued that it is probably unhelpful to treat young users of 13 and above similarly to children under 13 years of age.[165] This highlights a need to consider young users aged between 9-12 and 13-17 as separate segments instead of clubbing them under a broad umbrella called 'children,' a term that may best relate to those below 8 years of age.

Section 9(5) of the Act, which allows for the possibility of behaviour monitoring and targeted advertisements for children above a specified age, subject to the processing being done in a verifiably safe manner, also appears to be acknowledging the developmental differences among internet users below 18 years of age, and need to treat them differently.

These findings related to developmental differences among children below 18 years should also influence how the term 'well-being' used under section 9(2) of the Act can be interpreted. Given differential maturity levels of children being ages 0-8, 9-12, and 13-17, varied use cases of the internet, diversity in benefits and risks, and distinct abilities to take actions to protect themselves from potential harms, a graded approach to create benchmarks of well-being could be designed.

To this end, a blacklist could be created and items falling within it could be presumed to be against the well-being of children of all ages. This could contain predefined list of items, content types, or categories (e.g., content, or advertisements). These items would automatically be presumed to negatively impact the well-being of children and

164 Ibid.

165 Id at 319, referring to the United States COPPA.

would therefore be restricted or prohibited from being shown to them. For example, a blacklist could include advertisements for alcohol, tobacco, gambling, or violent content, ensuring that children are not exposed to such material. In addition, an age-appropriate risk-based approach to determine the extent to which behaviour monitoring and targeted advertisements could be allowed could be designed to help preserve balance and ensure that personalisation benefits children.

Key Takeaways at a Glance
An age-appropriate framework for personalisation is crucial to addressing the issue at hand, considering the developmental differences among children and teenagers. Research highlights that children's ability to understand online content, including advertisements, varies significantly with age. Younger children, particularly those under age 8, are less discerning about commercial content, while older children and teenagers (ages 13-17) demonstrate a more nuanced understanding of online interactions and the trade-offs between personalisation and privacy. Teenagers, in particular, are more aware of risks such as privacy violations and online harm and are generally capable of critical thinking, risk assessment, and understanding the implications of online interactions. However, they may still struggle with impulsive behaviour and peer influence. This developmental differentiation calls for a differentiated approach to digital well-being and regulation of behaviour monitoring and targeted advertisements. Younger children, tweens, and teenagers should be treated as distinct groups with varying levels of maturity and understanding. Furthermore, teenagers should be recognised as active digital consumers, capable of making informed choices about their online interactions.

7. An Optimal Way Forward on Personalisation

Based on our secondary and primary research and expert consultations, we suggest that the following approaches may be considered to ensure beneficial personalisation for children under India's Digital Personal Data Protection Act, 2023:

Experts on the way forward for tracking or behavioural monitoring and targeted advertising (n=116 responses for 35 respondents)

Age-Appropriate Design

- The research and stakeholder consultations clearly highlight the developmental differences between children of different ages. The implementation of the DPDP Act must take into account these differences, and treat teenagers as consumers of

and contributors to the digital economy.[166] It is crucial to ensure that advertising practices are transparent and do not exploit children's data while remaining beneficial to them, and to be in *the best interests of the child,*[167] which includes their right to access the internet, privacy, to play and engage in recreational activity, non-discrimination, freedom of information, freedom of opinion and thought, and freedom of association and identity forming.[168]

We recommend that India's forthcoming data protection rules segregate the definition of 'child' further in the rules to incorporate the differences between young children (aged 8 years and below), tweens (aged 9-12 years), and teenagers (13-17 years). Exemptions under the Fourth Schedule of the draft Rules must consider these differences.

Transparency and Control

- Regarding the agency of tweens and teenagers and digital literacy, we recommend including transparency, more algorithmic control, and appropriate language/ modes of communication as additional tests that can be applied while granting exemptions under the Fourth Schedule. Since algorithms are an 'experience' technology, mere digital literacy campaigns may do little to ensure that teenagers truly understand how personalisation algorithms work in practice. "*Children must be properly informed about how their data is used. This information should be age-appropriate and accessible so that users can effectively understand and take advantage of their rights*."[169] Policymakers must take an 'empowerment' approach towards tweens and teenagers, where they work towards empowering them with information and tools to navigate the internet safely, in collaboration with parents/guardians, civil society and industry, particularly in rural areas.

- Privacy information, along with terms, policies, and community standards, should be clear, concise, and written in language appropriate for the child's age. Service providers should provide simple, understandable explanations of how personal data is used at the point of activation. They must avoid misleading interfaces, nudges, and dark patterns while involving the interfaces children interact with.

---

166 Accordingly, the Consumer Protection Act, 2019, and other legislations must address issues surrounding advertising to children, including misuse of behaviour monitoring for creating dark patterns, which should be prohibited

167 Fundamentals for Child-Oriented Approach to Data Processing, Irish Data Protection Commission, 2021, avai;lable at: https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

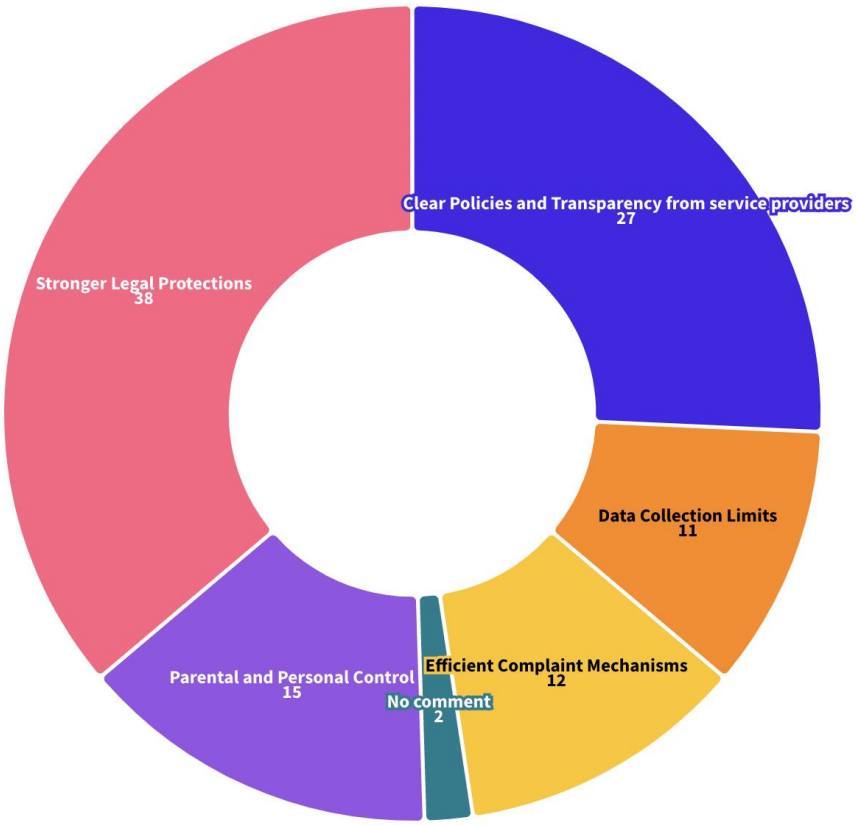
168 5 Rights Foundation, *Approaches to children's data protection, A comparative international mapping,* available at: https://5rightsfoundation.com/wp-content/uploads/2024/08/Approaches-to-Childrens-Data-Protection-.pdf and https://static.googleusercontent.com/media/publicpolicy.google/en//resources/youth-legislative-framework.pdf

169 Recommendations on the Digital Rights of Children (France), available at: https://www.cnil.fr/en/recommendation-6-strengthen-information-and-rights-children-design

Easy-to-access tools for children to exercise their data rights and report concerns should be available. Children must be able to exercise these rights at any time without barriers.[170]

This is supported by findings from our interaction with young users, who expressed a strong desire for clear policies and transparency from service providers.

Young users on measures to ensure safe practices (n=105 responses for 25 respondents)



The same has been proposed in the Kids Online Safety Act, put forth in the US Congress in 2022. It requires social media networks to provide children with tools to secure their information, disable addictive features, and opt out of personalised algorithmic suggestions. Platforms must also activate the strongest settings by default.[171]

[170] 5 Rights Foundation, *Approaches to children's data protection, A comparative international mapping,* available at: https://5rightsfoundation.com/wp-content/uploads/2024/08/Approaches-to-Childrens-Data-Protection-.pdf

[171] https://www.congress.gov/118/bills/s1409/BILLS-118s1409rs.pdf

Purpose Distinction and Evidence of Benefit vs. Harm

- There is a need to differentiate between different types and applicability of monitoring. For example, monitoring aimed at safety, such as detecting cyberbullying or grooming, time management, and enabling and enhancing digital access, among others is essential and could be considered beneficial. The current legislation lacks clear definitions or guidance on what constitutes permissible monitoring, creating uncertainty for companies. It might thus be useful to clearly define the scope of behaviour monitoring, targeted advertisements, and the well-being of children. This may help address high risk forms of automated processing of personal data, while preserving the collection and use of personal data for providing the service safely to children. As previously discussed, there are differing interpretations of these undefined terms, such as the view that targeted ads based on search queries or website visits, rather than personal data, falling outside the Act's scope. Clear definitions will help balance privacy protection with the compliance according to the Act.

  Policymakers must consult with platforms providing various kinds of services designed for children's use, experts, and civil society before finalising draft rules. Applications designed specifically to benefit children or undertake behaviour monitoring for protective purposes must be considered for exemptions under the Fourth Schedule of the Rules.

- In addition to individual exemptions, data fiduciaries might be grouped into classes with specific conditions. This approach could be more feasible and less burdensome, especially for smaller players and start-ups. In addition to app-specific exemptions, a purpose-specific approach could be considered, allowing platforms to use behavioural monitoring in a manner which allows only when it is necessary for the platforms to function properly and deliver fulfilling internet experiences for its target audience, i.e. children. These could include basic functions like health, safety and education, and it would also be possible to incorporate other facets of consumer welfare through nuanced analysis that may not be immediately apparent. For example, entertainment on music streaming platforms, as discussed earlier, is engaging and useful only because of technologies that enable behaviour monitoring and targeted advertisements. Like the EU, India must consider teenagers as active consumers and users of technology, not merely passive recipients.[172] Accordingly, the approach to legislation must involve conversations with several kinds of stakeholders, including industry, policy experts, children, including teenagers, and parents – an approach that has been recommended by the UN Committee on Rights of the Child.[173]

[172] See page 15, Lievens, Livingstone et al, Children's Rights and Digital Technologies, available at https://eprints.lse.ac.uk/84871/1/Children%27srightsanddigitaltech_revised_clean%20final.pdf. [Lievens]

[173] See page 7, Lievens.

Consequently, the government must consider crafting regulatory frameworks which can nudge platforms to provide the best and safest possible consumer experience to the youth. The focus must shift to providing adequate guardrails, agency, and safety mechanisms instead of banning the use of personalisation technologies completely. Experts also pointed to categorising advertisements according to age appropriateness and also linked to the age category of the content, is necessary for them to be beneficial. For example, ads that are meant for individuals aged 13 and above should not be displayed to younger audiences. Clear guidelines should nudge the industry to prevent unsuitable display of ensure that ads unsuitable to for certain age groups are not displayed to lower age groups.

- Furthermore, in our consultations, experts also provided certain potential metrics for assessing whether tracking or behavioural monitoring on a website could be permissible, under section 9(5) of the Act, and subsequently Part B of the Fourth Schedule of the rules. These could include:

  - **Privacy and Security**: Evaluate the extent to which children's data is protected from breaches and unauthorised access. The UNICEF Guidelines for Industry on Child Online Protection advises online platforms to adopt the highest privacy standards when it comes to collecting, processing and storing data from or about children.[174]
  - **Psychological Impact**: Assess the psychological effects on children from exposure to specific content or from being monitored.[175]
  - **Parental Satisfaction**: Measure parental satisfaction with the control and transparency offered by monitoring systems. [176]
  - **Data Minimisation**: Ensure that only necessary data is collected, stored, and processed to reduce the risk of misuse. The ICO also provides guidance on data minimisation, emphasising that only the necessary amount of personal data should be collected from children. [177]

Risk Based Approach

- A risk based approach that applies the rules proportionally to each age group of children and each purpose must be taken. Monitoring should be permitted where it provides a positive benefit and is proportionate to the associated risks. A graded

[174] UNICEF, *Guidelines for Industry on Child Online Protection,* 2015, https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf

[175] 5Rights Foundation, *Approaches to children's data protection*: *A comparative international mapping,* Oct. 2022, https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf

[176] Ibid.

[177] Ibid.

approach (with some off-limit purposes included in a black list), rather than a rigid cut-off, could facilitate more flexible and practical compliance.

Parental oversight and teenage digital literacy

- The internet must be made safer for teenagers with adequate protections that do not solely rely on parental oversight. This includes ensuring harmful content is inaccessible and appropriate guardrails are in place. Decisions should be made on a case-by-case basis, considering the child's age, context, and potential benefits versus risks. The concept of 'positive' rights versus 'negative' rights of a child must be kept in mind. Therefore, the rules must adequately consider the rights of a child to access the best version of a service while also being protected from harm. These guiding principles could be utilised while determining the scope of verifiably safe processing under section 9(5) of the Act and under Part B of the Fourth Schedule of the rules. Data processing, while protecting and empowering teenagers, must be allowed to balance the benefits and risks of the internet for children.

- The Government must collaborate with the industry, experts, and civil society to develop parental oversight tools that fit the priorities of the government while preserving the services provided by the platform. However, the proposed parental controls must align with data protection rules, ensuring they follow the principles of proportionality, transparency, and security. This includes considering the child's age, maturity, and interests, avoiding intrusive features like constant tracking, clearly explaining the parental controls used, and safeguarding the child's data to prevent unauthorised third-party access, such as geolocation data.[178]

- Additionally, the government along with industry, civil society, academics, youth leaders and parent representatives should work together to formulate a strategy for a teenage digital literacy programme. The Delhi High Court has also recently held that efforts to protect minors should go beyond teaching them about 'good touch' and 'bad touch' in the physical world. Invoking the concept of 'virtual touch', the court observed that minors must be equipped with the knowledge and tools to navigate online interactions safely and recognise potential risks lurking in cyberspace.[179]

[178] Recommendations on the Digital Rights of Children (France), available at: https://www.cnil.fr/en/recommendation-6-strengthen-information-and-rights-children-design and https://static.googleusercontent.com/media/publicpolicy.google/en//resources/youth-legislative-framework.pdf

[179] https://indianexpress.com/article/opinion/editorials/keeping-children-safe-online-while-ensuring-their-right-to-access-the-internet-9324428/

Privacy by Design and Default

- Products and services must prioritise children's privacy and data protection by design and default. When servicing children, privacy settings should be set to 'high privacy' by default, with minimal personal data collected unless necessary. Services must incorporate privacy from the outset of design, following the 'Bake It In' approach.[180] Children's personal data should not be shared with third parties unless absolutely necessary. Data uses, like personalisation, should require active consent from the child or parent/guardian while considering the child's age. Additionally, features like geolocation, microphone, and camera should be off by default, with clear communication to the child about any data usage.[181]

- Furthermore, platforms should adopt practices such as data anonymisation, which can balance personalisation with privacy protection, ensuring that sensitive information is processed securely. By implementing strict anonymisation processes, short data retention periods, and consent-based storage policies, businesses can build trust with users while offering personalisation services ethically.[182]

Data Protection Impact Assessments

- Service Providers should make Data Protection Impact Assessments (DPIAs) a core part of their services, focusing on identifying and mitigating risks, especially those affecting children. DPIAs should address risks related to content, contact, conduct, and consumer/contract, with the best interests of the child as a central criterion.[183] The draft rules mandate significant data fiduciaries to conduct annual data protection impact assessments and audits and report the assessment and audit to the Data Protection Board, to ensure that any algorithmic software they use to process personal data does not harm data principal's rights, including software for storage, hosting, and sharing data. These provisions can also be expanded to include fiduciaries managing children's data, ensuring the safety, privacy, and well-being of young users is prioritised.

---

180 The Irish Fundamentals adopt the "Bake It In" approach, which interprets Article 25(2) of the GDPR as: "*[D]ata protection measures should be built into the architecture and functioning of a product or service from the very start of the design process (rather than being considered after the development phase) and [...] the strictest privacy settings should automatically apply to a product of service.*"

181 5Rights Foundation, *Approaches to children's data protection*: *A comparative international mapping,* Oct. 2022, https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf

182 https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/balancing-personalization-and-data-security-key-considerations-for-retailersadopting-edge-ai-solutions/115921438?action=profile_completion&utm_source=Mailer&utm_medium=newsletter&utm_campaign=etciso_news_2024-12-03&dt=2024-12-03&em=dmRzQGN1dHMub3Jn

183 5Rights Foundation, *Approaches to children's data protection*: *A comparative international mapping,* Oct. 2022, https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf

Ensuring Beneficial Personalisation for Children
To ensure that personalisation benefits children, a comprehensive framework must adopt an age-appropriate design that recognises the developmental differences among young children, tweens, and teenagers. The definition of 'child' should be segmented to address their varying needs. For younger children, stringent protections and parental controls can be prioritised, while teenagers should have greater autonomy, supported by transparent and ethical personalisation mechanisms Privacy information should be communicated clearly using age-appropriate language, empowering children to exercise their data rights with minimal barriers. Parental oversight tools should strike a delicate balance between providing guidance and respecting the child's privacy. These tools must be developed collaboratively with industry experts and civil society to ensure they are effective, inclusive, and non-intrusive. Furthermore, digital literacy programmes tailored for teenagers can play a crucial role in empowering them to make informed and responsible choices in the digital space. A clear differentiation between beneficial and exploitative behavioural monitoring practices is essential. This can be done by adopting risk-based approach, permitting monitoring practices that offer a positive benefit, like cyberbullying detection, while remaining proportionate to the risks, like intrusion. The framework should allow varying levels of personalisation and monitoring based on the child's age and the specific purpose of data processing, ensuring flexibility and balanced compliance. Platforms must embed privacy by design and default principles, prioritising high-privacy settings, minimal data collection, and active consent mechanisms. Data Protection Impact Assessments (DPIAs) should be a cornerstone for all services aimed at children, proactively identifying and mitigating potential risks related to data processing and personalisation. Collaborative efforts between the government, industry, civil society, and experts are vital to developing policies and tools that enable safe, transparent, and positive online experiences for children.

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India
Ph: 91.141.228 2821, Fax: 91.141.228 2485
Email: cuts1@cuts.org, Website: www.cuts-international.org

Also at Delhi, Kolkata and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland) and Washington DC (USA).