NAVIGATING CHILDREN'S PRIVACY AND PARENTAL CONSENT UNDER THE DPDP ACT 2023

Towards a safe and enabling ecosystem for India's young digital nagriks

Authors

Aparajita Bharti, Nikhil Iyer, Rhydhi Gupta, Sidharth Deb

NOTE:

This paper is an independent, non-commissioned piece of work by The Quantum Hub (TQH), a public policy firm based in New Delhi.

Attribution: Navigating Children's Privacy and Parental Consent Under the DPDP Act 2023. November 2023. The Quantum Hub (TQH) and Young Leaders for Active Citizenship (YLAC).

ABOUT THE AUTHORS:

Aparajita Bharti, Founding Partner, TQH
Nikhil Iyer, Senior Analyst, TQH
Rhydhi Gupta, Analyst, TQH
Sidharth Deb, Public Policy Manager, TQH

FOREWORD:

RAKESH MAHESHWARI
Former Sr. Director and GC (Cyber Laws and Data Governance)
Ministry of Electronics and IT (MeitY)

During my tenure at the Cyber Laws division in the Ministry of Electronics and Information Technology (MeitY), I have engaged closely with discussions around data protection since its early stages. I have seen the conversation evolve from the Justice BN Srikrishna committee of esteemed experts 2018 report along with the accompanying draft Bill, to where we are in the present day where India has enacted the landmark Digital Personal Data Protection (DPDP) Act, 2023. The next challenge for Indian policymakers is to bring this law into action; and MeitY will play a pivotal role through its rulemaking functions.

Among the Act's many facets, one area of implementation that requires technical, legal and ecosystem sophistication pertains to the law's treatment of children's data processing. Section 9 of the DPDP Act is a step towards informed consent for processing children's data but also doubles up as a tool for active parental supervision on the online activity of children. The process of discerning a child user from an adult, establishing the parent-child relationship and obtaining verifiable parental consent needs careful calibration, balancing the need for accuracy in age verification and the privacy of individuals.

Globally, the conversation around age assurance and age verification has been in the works for over twenty years now. Countries across the world have experimented with varied age assurance mechanisms and regulatory codes, however, what works best to protect children is still very much an unsettled debate. In this global context, India has the opportunity to lead by example offering solutions that draw on India's digital public infrastructure while balancing challenges like digital divide, shared device usage, low digital literacy and gender norms around internet access. To operate in this complex environment, we need to experiment with innovative and flexible solutions to ensure that no child gets left behind, even as we ensure a safe online environment for our young digital nagriks.

This discussion paper by TQH comes at an opportune time, when the central Government is working on framing the Rules, to propose approaches that are likely to work for India. It proposes moving away from a one-size-fits-all approach and exploring alternate age assurance mechanisms such as capacity testing, facial analysis, family center etc. in accordance with the degree of risk and the nature of services provided by various platforms. It makes a case for putting more safeguards on platforms to keep young users safe instead of solely banking upon parents' ability to give informed consent. It also tries to take a considered approach towards practical difficulties in creating grounds for exemptions based on platform functionalities due to their ever-evolving nature.

I hope this paper sparks a considered conversation around children's privacy in India. I look forward to the active engagement and dialogue around this issue by platforms, civil society and policymakers, so that India puts its best foot forward in protecting children's interests and keeping them safe online.

TABLE OF CONTENTS

EXECUTIVE SUMMARY:

The Digital Personal Data Protection Act, 2023 (Section 9) requires all data fiduciaries (platforms, browsers, OS providers, etc.) to take 'verifiable parental consent' if they are processing data of a user who is below 18 years of age. Any mechanism to fulfil this legal requirement must look to satisfy three elements:

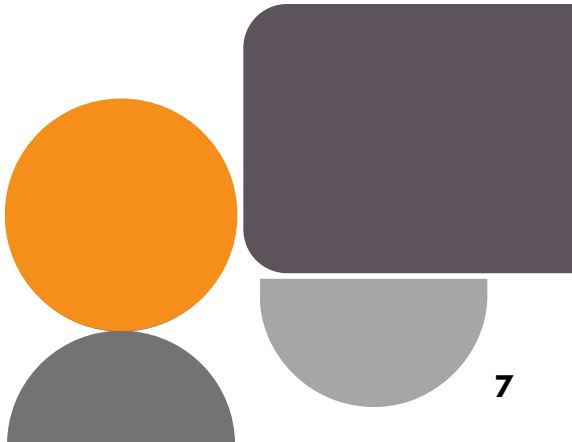
- verify the age of the user with reasonable accuracy,
- ascertain the legitimacy of the relationship between the user and the parent or guardian,
- and show evidence of their consent.

As the Government of India considers rules to implement this provision under Section 40(2), this paper delves into potential implementation mechanisms for this provision and provides a quick summary of global discussions around age verification. Across jurisdictions, age verification is a matter of heated debate with legitimate concerns around safety of children on one side and limitations of verification methods on the other. While hard verification mechanisms (i.e. based on documentary evidence using government IDs) have been proposed across countries, there are concerns that they create inequity in internet access, inadvertently cause privacy concerns, and impose cost and other practical barriers in enabling children to engage with online experiences. There are also legitimate concerns around circumvention by children and the feasibility of verifying parental consent at scale. India faces further complications owing to gender divide, low digital literacy, language barriers and shared device usage in low-income households. In this paper, we therefore discuss some possible alternative approaches to hard verification. These include facial analysis, capacity testing, family centre, etc. We present a qualitative assessment of these mechanisms and evaluate their pros and cons from a user and business perspective.

Our analysis suggests that given India's varied levels of digital adoption, aspirations to build a strong digital economy, and other legal and practical concerns, we should avoid a one-size-fits-all approach that mandates hard age verification for all digital products and services. Instead, a list of methods should be suggested by the government that would fulfil the purpose of parental consent for most data fiduciaries. For those fiduciaries that offer goods or services that are prohibited for children under other laws, hard verification of age and parental consent may be better suited.

To give effect to this approach, we recommend that the Government of India develop a code of practice for age assurance that prescribes a range of age assurance mechanisms, corresponding to the level of risk involved in data processed by a particular data fiduciary. Under this code, each data fiduciary should be asked to proactively publish a self-assessment of risk at regular intervals, justifying reasons for its decision to prefer a certain mechanism and how it keeps children safe. If such a mechanism is enacted, failure to conduct this assessment, or inability to prevent systemic harm from accruing to child users could expose the data fiduciary to liability under Section 9 of the DPDP Act, 2023.

We envisage that this approach will enable India's youth to meaningfully engage with the growing digital economy while keeping them safe online. Our proposals envisage a vital role for civil society, organisations working with children, academia and media in this discussion going forward. The underlying premise of our recommendations is to balance privacy concerns of young citizens vis-a-vis their agency online and ensure that the opportunity afforded by the internet is not lost on India's children.



I. CONTEXT:

The Digital Personal Data Protection (DPDP) Act, 2023 was passed by the Parliament of India in August 2023, and received Presidential Assent on 11 Aug, 2023.[1] Section 9 of the Act addresses the governance of children's data and children's privacy. This is reflective of the growing recognition internationally that there is a need for specialised data governance frameworks for children as they often lack the foresight to appreciate the long-term implications of the processing of their personal data.[2]

However, the DPDP Act's approach at regulating children's data is widely discussed as one the most contentious parts of India's new law.[3] It requires all data fiduciaries[4] (platforms, browsers, OS providers, search engines, etc.) to take 'verifiable parental consent' if they are processing the data of a user below 18 years of age unless they have been deemed 'verifiably safe'. This provision's operationalisation not only requires changes to interface and platform design, but the extent of its application can also have unintended consequences on children's safety, autonomy, and anonymity. As such any legislation that attempts to protect children's privacy over the internet has a complex task of balancing these objectives against competing rights like agency and autonomy.[5]
As the Government of India exercises its rule-making powers under Section 40(2)(i) and (j) to implement Section 9, our paper begins by discussing the elements that data fiduciaries will have to satisfy to meet the consent requirement, the range of age assurance mechanisms available, and their impact on equitable access to and safety on the internet.[6] We review major jurisdictions' approach to children's data protection and online safety and draw insights from their experiences. We discuss a range of solutions, their effectiveness in ascertaining age of the user, challenges in compliances including feasibility and scalability, and impact on children from marginalised communities, amongst other considerations. Further, we suggest a potential approach for India, that could inform the discussion on operationalisation of parental consent.

1 *The Digital Personal Data Protection Act, 2023 (DPDP Act hereafter), August 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.*

2 *Emma Day. Data governance for children: An emerging priority area for privacy professionals. UNICEF. May 2022. https://www.unicef.org/globalinsight/stories/data-governance-children-emerging-priority-area-privacy-professionals.*

3 *As per Section 2(i) of DPDP Act, 2023, 'data fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.*

4 *Nikhil Iyer. Go back to a clean slate on data protection for children. Mint. August 2023. https://www.livemint.com/opinion/online-views/go-back-to-a-clean-slate-on-data-protection-for-children-11692891748097.html.*

5 *Sonia Livingston et. Al. Children's data and privacy online Growing up in a digital age: An evidence review. London School of Economics and the UK Information Commissioner's Office (ICO). December 2018. https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf.; Joseph A. Cannataci, Artificial intelligence and privacy, and children's privacy: Report of the Special Rapporteur on the right to privacy. Human Rights Council. United Nations. A/HRC/46/37. January 2021. https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F46%2F37&Language=E&DeviceType=Desktop&LangRequested=False*

6 *Age assurance is a broad term which includes age declaration (by user or parent), estimation (by algorithmic methods, facial characterisation, etc.) and age verification (based on Government ID document, biometrics, etc.). Each of these have differing levels of efficiency and pose varying risks to the users.*

Requirement of Section 9(1): The children's data and parental consent issue:

Section 9(1) of the DPDP Act requires all data fiduciaries[7] (platforms, browsers, OS providers, etc.) to take 'verifiable parental consent' if they are processing the data of a user below 18 years of age. Any mechanism to fulfil this legal requirement must look to satisfy three elements:

- It provides for the accurate age of the user (to determine the person is indeed a child, or an adult);
- It ascertains the legitimacy of the relationship between the user and the parent or lawful guardian;
- It verifies the identity and consent of the parent or lawful guardian.

Failure to meet any of these three elements may lead to an outcome where the mandate in Section 9(1) is not met, and the data fiduciary may incur penalties under the DPDP Act, 2023 which may extend up to Rs. 200 crores.[8] The Act also carves out an exception for a yet undefined class of 'verifiably safe' entities. These entities will be exempt from complying with Section 9(1) which imposes the parental consent requirement, and from Section 9(3), that prohibits them from tracking, behaviourally monitoring, and targeting advertising at children.

Operational Details

Currently, the DPDP Act provides no guidance on operationalising parental consent. The Indian Government is empowered to notify the procedure and requirements for "verifiable consent" through delegated legislation ("rules"). There have been public statements by India's Minister of Electronics and Information Technology ("MeitY") that the rules could mandate data fiduciaries to use "DigiLocker" for parental consent.[9] DigiLocker is an online repository of verified government-issued documents, from where data fiduciaries would be able to directly fetch documents pertaining to the child and their parents and obtain parental consent. Media reports suggest there are plans to enable platforms to access a parental consent artefact which will be stored on DigiLocker and be used to satisfy the requirement in Section 9(1) of DPDP Act. In a similar vein, India's Minister of State for Electronics & IT has also been quoted saying that this 'verifiably safe' exemption will be available to entities who achieve '100% KYC',[10] indicating a preference for identity-document based verification, commonly termed as hard verification.

Aside from the government, the users i.e., data principals and data fiduciaries, another key stakeholder group which effectuate parental consent under the framework are "consent managers'. The DPDP Act defines "consent managers" as person(s) registered with the Data Protection Board, who acts as a single point of contact to enable data principals to give, manage, review, and withdraw

---

7 *As per Section 2(i) of DPDP Act, 2023, 'data fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.*

8 *Schedule, DPDP Act, 2023.*

9 *Suraksha P. Soon, store parental consent in DigiLocker. The Economic Times. August 2023. https://economictimes.indiatimes.com/tech/technology/soon-store-parental-consent-in-digilocker/articleshow/102954908.cms*

10 *Aashish Aryan & Surabhi Agarwal. Exemptions in new data bill limited to national security, public order: MoS IT Rajeev Chandrasekhar. The Economic Times. August 2023. https://economictimes.indiatimes.com/tech/technology/exemptions-in-new-data-bill-limited-to-national-security-public-order-mos-it-rajeev-chandrasekhar/articleshow/102407336.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.*

her consent through an accessible, transparent, and interoperable platform.[11] Consent managers will also deal with consent of children and parents, and will play a critical role in the data governance ecosystem.

India's approach to data protection and ensuring equitable access and safety on the internet has caught the eye of regulators in other countries such as Norway and South Africa.[12] As a sizable digital economy and India's impetus for exporting digital public infrastructure (DPIs), there is recognition of India's unique vantage point to approach the conundrum of age verification through both technological and a regulatory lens.[13]

What is at stake?

Major jurisdictions including the European Union, the UK, the US, Australia, and others are experimenting with various regulations which protect the interests of children online. This includes protections against exposure to inappropriate or illegal content, cyberbullying, hate speech, addiction, exploitation, and abuse by other online persons, etc. At the same time, access to the internet is an important indicator of the opportunities an individual has in today's world. Research by international experts like Danielle Citron from the University of Virginia suggests that the tendency towards constant oversight and monitoring of children's online activities can negatively impact their personal development and long-term socio-economic prospects.[14] Research suggests that such systems cause a chilling effect on children where they may refrain from using the internet to learn new skills and explore new activities.

Thus, the impact any regulation has on the development, well-being and prospects of children should be at the forefront of policy makers' thinking. Factors such as low digital literacy among parents, shared device usage, gender divide and social norms around usage of the internet by young women also need to be considered while evaluating technical solutions for operationalizing parental consent.

II. INTERNATIONAL DEVELOPMENTS AROUND AGE ASSURANCE:

In this section, we explore the main discourse around age assurance (verification and estimation) across various jurisdictions. For context, the UK's Information Commissioner's Office (ICO)-- its nodal data protection authority- defines age assurance[15] as "... *a range of techniques for estimating*

---

11 Section 2(g), Digital Personal Data Protection Act, 2023.

12 Governments abroad call Data Protection Bill a 'landmark' regulation. Business Standard. August 2023. https://www.business-standard.com/technology/tech-news/governments-abroad-call-data-protection-bill-a-landmark-regulation-123081600241_1.html.

13 How India is using digital technology to project power. The Economist. June 2023. https://www.economist.com/asia/2023/06/04/how-india-is-using-digital-technology-to-project-power.

14 Danielle Citron. The Surveilled Student. Stanford Law Review. v. 76. August 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4552267.

15 Age assurance – estimating or verifying the age of service users. UK Information Commissioner's Office. https://bitly.ws/Z8AY.

or verifying the ages of children and users, including:

- *self-declaration*
- *AI and biometric-based systems;*
- *technical design measures;*
- *tokenised age checking using third parties; and*
- *hard identifiers like passports."*

On a review of such developments across the globe on this front, four key themes emerge:

1. There is widespread recognition of the trade-off between hard age verification, that mandates some form of documentary evidence, and freedom of speech and privacy of citizens. Courts in countries like the United States have ruled against hard verification mandates, arguing that it will affect citizens' ability to freely navigate the internet and express themselves.[16]

2. Similarly, regulators like the ones in Australia[17] and France,[18] have concluded that none of the existing age assurance technologies satisfy standards of sufficiently reliable verification, complete coverage of the population and upholding privacy of citizens.

3. Irrespective of these trade-offs, no one technology solution has emerged that is universally accessible to people across different socio-economic backgrounds and is not reasonably prone to circumvention.[19] Thus, the latest evidence would suggest a one size fits all approach is unable to ensure the entire ecosystem is successfully covered under the framework.

4. Further, while there has still been much exploration of age assurance mechanisms, there has been lesser research on establishing parent/guardian-child relationships to a reasonable extent to verify parental consent. For instance, while the USA's COPPA law mandates obtaining verifiable parental consent for children below 13 years of age, there are issues of privacy, efficacy, accessibility, etc. with all methods currently used by platforms.[20]

16 *Online age verification: balancing privacy and the protection of minors. CNIL. September 2022. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.*

17 *Age Verification. Australia eSafety Commissioner. 2023. https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification.*

18 *Online age verification: balancing privacy and the protection of minors. CNIL. September 2022. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.*

19 *Mihnea Dumitrascu. Age Verification and Data Protection: Far More Difficult than it Looks. IAPP. January 2022. https://iapp.org/news/a/age-verification-and-data-protection-far-more-difficult-than-it-looks/.*

20 *Report on Verifiable Parental Consent. Future of Privacy Forum. June 2023. https://fpf.org/blog/fpf-releases-report-on-verifiable-parental-consent/.*

With the above context the following analysis serves as an overview of key developments across major jurisdictions:

COUNTRY: UNITED KINGDOM

Approach: The Children's Code [formerly known as the Age-Appropriate Design Code (AADC)] came into force in 2021. It conferred flexibility in age verification and age assurance mechanisms based on the type of content that could be accessed and the level of risk involved in the online activity. In April 2023, Information Commissioner's Office (ICO) published a detailed draft guidance on what "***likely to be accessed***" by children means in the context of its Age-Appropriate Design Code ("Code"). It noted that a simple self-declaration of age is "unlikely" to be an effective way of restricting access to over-18s. The guidance does not provide a detailed account on effective age-gating but gives the example of a website offering adult content that uses "robust age assurance methods through several third-party technological solutions". It gives the Information Commissioner's Office (ICO) powers to fine businesses that do not comply with the Code with penalties up to 4% of their global annual turnover.[21]

Under the Online Safety Act (OSA), passed in the UK in October 2023, pornography companies, social media platforms and other services will be explicitly required to use age verification or estimation measures to prevent children accessing harmful content. The details of the law's implementation have been left to the UK's regulation agency, the Office of Communications (Ofcom). Under the proposals Ofcom is expected to be required to produce a code of practice on age assurance. Providers will have to choose systems that are "highly effective at correctly determining whether or not a particular user is a child" [S12 (6)]. Providers can even be required to distinguish between children of different ages, for the purpose of determining whether they can be permitted to access certain content. A range of approaches to age verification and age estimation will be identified by platforms and then a code of practice will officially be crystalised by the regulator.

ICO's Strategy for 2025[22]mentions possible changes to the AADC to align it closely with the OSA. It also mentions pressing for platform changes to correctly assess children's ages to conform with the code. However, it does not mention specific methods of doing so. Through the Digital Regulation Cooperation Forum (DRCF) work plan for 2022-23, the ICO and Ofcom will conduct joint research on age assurance.[23]

---

21 *The penalties are imposed under the UK's Data Protection Act, 2018 and the Privacy and Electronics Communications Regulations, 2003. See UK ICO's Age Appropriate Design Code: A Code of Practice for Online Services. September 2020. https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf.*

22 *ICO25-Empowering You through Information. UK ICO. July 2022. https://ico.org.uk/media/about-the-ico/documents/4020926/ico25-plan-for-consultation-20221407-v1_0.pdf*

23 *Families Attitudes toward Age Assurance: A study commissioned by ICO and Ofcom. Digital Regulation Cooperation Forum. October 2022. https://www.ofcom.org.uk/__data/assets/pdf_file/0026/245195/DRCF-Ofcom-ICO-age-assurance.pdf.*

Impact:

Actions by platforms

- Since AADC came into force, some platforms have gradually introduced interventions to make children's online experience safer and healthier.[24] For example the UK ICO observes that the Code has prompted changes across social media, online media and video streaming industries.[25] Children's accounts are set to private by default, adults are blocked from directly messaging children, and platforms have started turning off notifications at bedtime. Moreover, Facebook and Instagram limited targeting to age, gender, and location for under-18s. Both Facebook and Instagram began asking for people's date of birth at sign up, preventing them from signing up if they repeatedly entered different dates, and disabling accounts where people can't prove they're over 13. Additionally, YouTube turned off autoplay by default and turned on take a break and bedtime reminders by default for Google accounts for under 18s.[26]

- Additionally, platforms are relying on third party age assurance providers such as Yoti,[27] a digital ID solution that has emerged as a one-stop solution for platforms to comply with the AADC. Users can take a selfie and scan a passport or driving licence with their smartphone, which is transformed into a digital identity on Yoti's app. For consumers, their digital identity lets them authenticate their identity in seconds. Yoti offers its age check services for free to businesses, earning from its other offerings such as KYC, identity verification checks, etc.[28] Yoti claims to use advanced hybrid encryption to secure user details, promising that they do not sell user's personal data to third parties.[29]

Enforcement of penalties

ICO has been undertaking investigations under the AADC to check for non-adherence by social media, gaming and other companies processing children's data. In May 2023, the ICO issued a £12,700,000 fine to TikTok for several breaches of data protection law, including failing to use children's personal data lawfully. ICO's investigation found that TikTok processed the data of children under the age of 13 without appropriate parental consent.[30] ICO announced that it found that TikTok did not do enough to check who was using their platform. The only age gateway or age verification process in place at the point of entry to the platform, was a self-declaration of age by the user.[31] Per the ICO, TikTok had an estimated 1.4 million underage UK users during a two-year period, between May 2018 and July 2020, contrary to terms of service stating users must be 13 or older.

24 "Children are better protected online in 2022 than they were in 2021" UK ICO. September 2022. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/children-are-better-protected-online-in-2022-than-they-were-in-2021/.

25 Ibid.

26 Ibid.

27 Age Verification Tools for Online Customers and Custom-Built Apps. Yoti. September 2023. https://www.yoti.com/business/age-verification/.

28 David Murphy. Yoti to Offer Digital ID Age Checking to Businesses for No Fee. Mobile Marketing. June 2023.

29 Our Approach to Security and Privacy. Yoti. December 2019. https://www.yoti.com/blog/our-approach-to-security-and-privacy/

30 Penalty Notice to Tiktok. UK ICO. April 2023. https://ico.org.uk/media/4025182/tiktok-mpn.pdf

31 Ibid.

Reactions of Stakeholders to the Online Safety Act

- Policymakers in the UK are alert to the challenge of ensuring that children only access age-appropriate content. They have been warned that the requirements of the new OSA could lead to users losing access to platforms such as Wikipedia, which has in response threatened to leave the UK jurisdiction due to fears that the law could lead to "age-gating" the website, which currently does not require age verification. [32]

EUROPEAN UNION (EU)

Approach: The EU does not have an independent law for children's data protection. Its General Data Protection Regulation (GDPR) requires data controllers undertake verification with regard to age and parental consent. Currently, the GDPR allows individual Member States limited flexibility in determining the national age of digital consent for children: between the ages of 13 and 16. Critically, the GDPR offers digital services the flexibility to make reasonable efforts to secure parental consent, taking into consideration available technology.[33] Likewise, the Audio-visual Media Services Directive (AVMSD)[34] requires the adoption of appropriate measures to protect children from online harmful content, including through age verification.[35] We discuss two country specific examples below.

France - Article 3 of Decree No. 2021-1306 of 7 October 2021 entrusts French regulator-Arcom,[36] with the task of drawing up guidelines detailing the reliability of the technical procedures that adult websites must implement to prevent access by minors.[37] This Decree relates to the terms of implementation of measures aimed at protecting minors against accessing sites disseminating pornographic content. Recently in March 2023, legislation was passed[38] in France's National Assembly which required social media services to put in place technical solutions to verify the age of their users and to verify if users under the age of 15 have received parental consent. The law has not been approved by the European Commission and the modalities of implementation are not clear.[39]

32 Wikipedia could stop being accessible in the UK due to Online Safety Law. Engineering and Technology. July 2023. https://eandt.theiet.org/content/articles/2023/07/wikipedia-could-stop-being-accessible-in-the-uk-due-to-online-safety-law/.

33 Article 8(2), General Data Protection Regulation. European Union.

34 Protection of minors in the AVMSD. European Union. https://digital-strategy.ec.europa.eu/en/policies/avmsd-protection-minors.

35 Audiovisual Media Services Directive. European Union. March 2010. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02010L0013-20181218

36 Arcom is the French public regulatory authority for audiovisual and digital communications. This regulation operates in the service of freedom of expression in the public interest and in consultation with professionals.

37 Decree No. 2021-1306 of October 7, 2021 relating to the modalities of implementation of measures aimed at protecting minors against access to sites disseminating pornographic content. Legifrance. October 2021. https://www-legifrance-gouv-fr.translate.goog/jorf/id/JORFTEXT000044173388?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp

38 Bill to secure and regulate the digital space. The Senate Galaxy. June 2023. https://www.senat.fr/basile/visio.do?id=d0150842&idtable=d172203-114375_20%7Cd0150842&_c=m%C3%A9dias&rch=ds&de=20230615&au=20230630&dp=15+jours&radio=dp&aff=72203&tri=p&off=0&afd=ppr&afd=ppl&afd=pjl&afd=cvn

39 Hannah Fang. France Senate passes legislation requiring age verification for minors on social media. Jurist. June 2023. https://www.jurist.org/news/2023/06/france-senate-passes-legislation-requiring-age-verification-for-minors-on-social-media/.

France forbids social media platforms to register users who are minors under the age of 13. However, according to the French National Commission for Technology and Freedoms, 63 percent of children under the age of 13 have at least one social media account, and over half of the children aged between 10 and 14 use social media sites. Lawmakers are also working to restrict access to porn sites. CNIL[40]worked with Ecole Polytechnique professor Olivier Blazy to develop a solution that attempts to minimise the amount of user information sent to a website. The proposed method involves using an ephemeral "token" that sends a challenge to a browser or phone when accessing an age-restricted website. That challenge would then get relayed to a third party that can authenticate age, for instance a bank, internet provider, or a digital ID service, which would issue its approval, allowing one to access the website. The system's goal is to make sure a user is old enough to access a service without revealing any personal details, either to the website they're using or the companies and governments providing the ID check. The third party only knows about an age check but not for what purpose. The system is in its trial stage.

Germany - Germany is one of the European member states that has implemented age verification and has also provided a list of age verification vendors.[41]Age verification for closed user groups must be ensured through two interconnected steps:

- **Initial Verification:**[42]through at least one-time identification (age verification), which must generally take place via personal or upstream contact. The prerequisite for a reliable adulthood check is the personal identification of natural persons, including verification of their age. Personal identification is necessary to avoid the risk of counterfeiting and circumvention. "Personal contact" is basically a facial check among those present ("face-to-face" check) with comparison of official identification data (identity card, passport).
- **Periodic Check:** through authentication during individual usage processes. Authentication serves to ensure that only the identified and age-verified person has access to closed user groups and is intended to make it more difficult for access authorizations to be passed on to unauthorised third parties/younger users.

Broader European Efforts for Interoperable Parental Consent:
The European Commission has also begun working on an EU browser-based interoperable age verification method called euCONSENT[43]since 2021, which will allow users to verify their identity

40 Online age verification: balancing privacy and the protection of minors. CNIL. September 2022. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

41 Age Verification Systems. KJM (German Commission for Protection of Minors). https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme.

42 In closed user groups, certain otherwise impermissible content - certain offers that are harmful to minors and simple pornography - may be distributed if it is ensured that children and young people do not have access to it. Closed user groups are ensured using the age verification system (AVS). They are only available on the internet.

43 Electronic Identification and Trust Services for Children in Europe. euConsent. https://euconsent.eu/

online by choosing from a network of approved third-party services.[44] Since this would give users the ability to choose the verification they want to use, this means one service might ask a user to upload an official government document, while another might rely on facial recognition. A user can undergo age verification for one particular site with that site's preferred verification partner, and then reuse that verification on subsequent sites. They will be able to use one age check that works on multiple sites without requiring additional actions from the verified person. The person will be anonymous in the transactions. The software is also being built to accommodate parental consent for minors. **The system was successfully proven through three pilots by over 2,000 children, adults and parents from 5 European Member States.**

The European Commission will also issue a standardisation request[45] for a European standard on online age assurance / age verification in the context of the eID proposal from 2023.[46] eID is a set of services provided by the European Commission to enable the mutual recognition of national electronic identification schemes (eID) across borders. It allows European citizens to use their national eIDs when accessing online services from other European countries.[47] The proposed eID will enable minors, based on national laws, to use the Digital Identity Wallet, to prove their age without disclosing other personal data.

Impact:

Actions by Platforms

- In 2022, Instagram started testing [48] a vouching tool to ensure users are as old as they say they are; it has also started using biometric technology for facial analysis in some cases.
- Twitter verified parental consent requiring documentation (ID/birth certificate, etc.). The platform says that the documents are treated confidentially and deleted after verification.[49]
- e-Commerce sites selling adult products and services such as gambling, alcohol or pornography have a wide range of age verification methods such as credit and scratch cards and biometrics.[50]

44 B2B Services, private companies.

45 The Commission will work with Member States (who in line with national legislation can choose to issue electronic IDs to the under-18s under the recent proposal on a European Digital Identity), relevant stakeholders and European standardisation organisations to strengthen effective age verification methods, as a priority. This work will encourage market solutions through a robust framework of certification and interoperability.

46 A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+). European Commission. May 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A212%3AFIN

47 eID Offers digital services capable of electronically identifying users from all across Europe. European Commission. https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eID.

48 Introducing New Ways to Verify Age on Instagram. Meta. June 2022. https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/

49 About Parental Consent on X. X. https://help.twitter.com/en/using-x/parental-consent.

50 Shiona McCallum. Can age verification stop children seeing pornography?. BBC. November 2022. https://www.bbc.com/news/technology-63794796.

Reactions of Stakeholders

According to the European Parliamentary Research Service, despite the widespread use of age verification methods in some sectors, there are still fears that they pose privacy and cybersecurity risks given the quantum and sensitivity of personal data that will be collected in the process.[51] Similarly, the French regulator CNIL in its report[52] analysed several existing solutions for online age verification, checking whether they have the following properties: sufficiently reliable verification, complete coverage of the population and respect for the protection of individuals' data and privacy and their security. It found that there is no solution currently that satisfactorily meets these three requirements. It therefore calls on public authorities and stakeholders to develop new solutions, following the recommendations described above.

AUSTRALIA

Approach: Australia's Privacy Act 1988 protects an individual's personal information regardless of their age. It doesn't specify an age after which an individual can make their own privacy decision. For their consent to be valid, an individual must have capacity to consent.

Platforms must decide if their user aged under 18 has the capacity to consent on a case-by-case basis. As a general rule, a user under the age of 18 has the capacity to consent if they have the maturity to understand what's being proposed. However, if they lack the required maturity, it may be appropriate for a parent or guardian to consent on their behalf.

Australia recently unveiled draft legislation on a universal digital ID aiming to streamline citizens' interaction with government and third-party organisations through a single government-run identification platform. The platform would consolidate various official ID documents, such as passports and driver's licences, enhancing efficiency in accessing services. The current digital ID, MyGovID,[53] is limited to accessing government services and verifying individuals biometrically against their passports. The proposed universal system aims to allow for a national, economy-wide biometric identity verification system.[54]

Australia's government has recently decided against imposing a mandatory age verification regime for online pornography and other adult content, citing the immaturity of current technology options.[55]

51 Online age verification methods for children. European Parliamentary Research Service. February 2023. https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf.

52 Online age verification: balancing privacy and the protection of minors. CNIL. September 2022. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

53 Common questions and issues setting up your myGovID. Australian Government. https://www.dewr.gov.au/digital-identity-accessing-dewr-online-services/common-questions-and-issues-setting-your-mygovid.

54 Australia unveils plans for universal digital ID and AI taskforce. Biometric Update. September 2023. https://www.biometricupdate.com/202309/australia-unveils-plans-for-universal-digital-id-and-ai-taskforce

55 Australian government opts against online age verification mandate. Biometric Update. August 2023. https://www.biometricupdate.com/202308/australian-government-opts-against-online-age-verification-mandate#:~:text=Australia%27s%20Albanese%20government%20has%20opted,on%20forthcoming%20online%20safety%20codes

The Government observed that for age assurance to be effective, it must: [56]

- work reliably without circumvention;
- be comprehensively implemented, including where pornography is hosted outside of Australia's jurisdiction; and
- balance privacy and security, without introducing risks to the personal information of adults who choose to access legal pornography.

In March 2023 Australia's eSafety Commissioner concluded that age assurance technologies cannot at the time meet all these requirements. While industry is taking steps to further develop these technologies, the Roadmap for age verification[57] finds that the age assurance market is, at this time, immature. **The government will instead rely on forthcoming online safety industry codes:**[58] The new tranche of codes will be developed by eSafety commissioner, to educate parents on how to access filtering software and limit children's access to such material or sites that are not appropriate, following the implementation of the first set of industry codes in December 2023.

Impact:

Actions by Platforms

- In March 2022, Google announced a new age verification step for Australian users of YouTube. When attempting to access age restricted content on YouTube or downloading on Google play, some Australian users may be asked to provide additional proof of age. Google will use this additional step to assure whether a user is above 18, regardless of the age associated with the user's account. If Google is unable to substantiate that the user is over 18, that user is asked to verify their age, by providing either a photograph of a government-issued ID or by allowing an authorisation on their credit card.
- Yubo, a location-based social media app for teenagers to connect with other young people in their local area, announced the introduction of an age verification system developed in partnership with Yoti to allow users to be confident they are interacting with others of a similar age group. Yubo first launched the use of Yoti's facial age estimation technology for users aged 13-14, with the goal of scaling the technology across its entire user base by the end of the year.
- In June 2022, Meta announced it was testing new options for users to verify their age on Instagram, to give them age-appropriate experiences. In addition to providing ID, new options for users included asking others to vouch for their age and taking a video selfie to be shared with Yoti for facial age estimation. In March 2023, this trial was rolled out in Australia.

56 Government's response to the Roadmap on Age Verification. Australian Government. August 2023. https://www.infrastructure.gov.au/sites/default/files/documents/government-response-to-the-roadmap-for-age-verification-august2023.pdf

57 Age Verification. Australia eSafety Commissioner. 2023. https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification.

58 Australian government opts against online age verification mandate. Biometric Update. August 2023. https://www.biometricupdate.com/202308/australian-government-opts-against-online-age-verification-mandate#:~:text=Australia%27s%20Albanese%20government%20has%20opted,on%20forthcoming%20online%20safety%20codes

Reactions of Stakeholders

- The eSafety organisation has proposed establishing a regulatory framework[59] for accrediting and supervising age assurance providers. They also acknowledged the ongoing efforts to create a similar regulatory framework for the Australian Government's Digital Identity System.

UNITED STATES (US)

Approach: The US Congress enacted the Children's Online Privacy Protection Act (COPPA)[60] in 1998. COPPA requires the Federal Trade Commission (FTC) to issue and enforce regulations concerning children's online privacy. The Commission's original COPPA Rule became effective on April 21, 2000. The Commission published an amended Rule on January 17, 2013 which took effect on July 1, 2013. Operators covered by the rule must provide direct notice to parents and obtain verifiable parental consent, with limited exceptions. **The term "verifiable parental consent"[61] means any reasonable effort (taking into consideration available technology) by which the parent receives notice and is informed about the collection and processing of the child's personal data.** The way verifiable parental consent is implemented under this framework is detailed below. Notably, a "child" under the COPPA framework is defined as an individual below the age of 13 years.

COPPA covers operators of (a) general audience websites, or (b) online services only where such operators have actual knowledge that a child under age 13 is the person providing personal information.

The Rule does not require operators to ask the age of visitors. However, an operator of a general audience site or service that chooses to screen its users for age in a neutral fashion may rely on the age information its users enter, even if that age information is not accurate. In some circumstances, this may mean that children are able to register on a site or service in violation of the operator's Terms of Service. If, however, the operator later determines that a particular user is a child under age 13, COPPA's notice and parental consent requirements will be applicable.

The Future of Privacy Forum finds that due to low levels of enforcement compared to the high costs and challenges with COPPA consent requirements has led to digital service operators being disincentivised from even attempting to design COPPA-compliant sites and services.[62] At the time

59 Australia could finalize digital ID legislation by mid-2024, but long road still ahead. Biometric Update. July 2023. https://www.biometricupdate.com/202307/australia-could-finalize-digital-id-legislation-by-mid-2024-but-long-road-still-ahead

60 Complying with COPPA: Frequently Asked Questions. Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#C.%20Privacy%20Policies.

61 Children's Online Privacy Protection Act, 1998. United States of America. http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

62 The State of Play: Is Verifiable Parental Consent Fit for Purpose?. Future of Privacy Forum. June 2023. https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf.

of writing, the US Congress is considering a number of Bills for online child safety despite the presence of COPPA which may be viewed as structurally unsound owing to the drastically evolving online landscape.

One such bill- the Protecting Kids on Social Media Act has five major components proposals which are as follows:

1. It proposes mandating social media companies to verify the ages of all account holders, including adults.
2. It proposes an absolute ban on on children under age 13 using social media.
3. It mandates social media companies obtain parental or guardian consent to allow minors between the ages of 12–17 years use social media.
4. It proposes a ban on the data of minors (anyone over 12 years old and under 18 years old) being used to inform a social media platform's content recommendation algorithm.
5. It proposes creating a digital ID pilot program, instituted by the Department of Commerce, for citizens and legal residents, to verify ages and parent/guardian-minor relationships.

Other Federal Bills [63] such as the Kids Online Safety Act and the COPPA 2.0 have also been introduced as bipartisan legislative proposals. KOSA would ban kids 13 and under from using social media and require companies to acquire parental consent before allowing children under 17 to use their platforms. COPPA 2.0 will potentially raise the age of protection under the Children's Online Privacy Protection Act from 13 to 16 years of age, along with similar age-gating restrictions.

States are also witnessing a lot of action in this domain. For example:

The **California Age-Appropriate Design Code (CAADC**) is a law geared toward technology companies that provide online services 'likely to be accessed' by children under age 18. This age limit is one of the biggest differences from COPPA, which only covered minors under age 13. It requires covered businesses to estimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business. The law will take effect on July 1, 2024.[64]However, a federal judge has recently granted a preliminary injunction[65] to block the CAADCA saying that the law likely violates free speech rights under the First Amendment both, for users who may be required to provide hard identifiers to access online services, as well as businesses, who will be barred from using the data for different purposes (including for preventing children from indulging in any harmful behaviour).[66] The State of California is likely to appeal against this injunction.

63 Makena Kelly. Senate panel advances bills to childproof the internet. July 2023. https://www.theverge.com/2023/7/27/23809876/kosa-coppa-2-child-safety-privacy-protection-social-media.

64 How age verification systems can help you prepare for CA AADC. Persona. https://withpersona.com/blog/age-verification-systems-ca-aadc#:~:text=The%20law%20takes%20effect%20on,sending%20private%20messages%20to%20minors.

65 NetChoice v. California. Northern District Court of California. September 2023. https://netchoice.org/wp-content/uploads/2023/09/NETCHOICE-v-BONTA-PRELIMINARY-INJUNCTION-GRANTED.pdf.

66 Gabby Miller. Fight Over State Child Online Safety Laws May Last Years. Tech Policy Press. September 2023. https://techpolicy.press/fight-over-state-child-online-safety-laws-may-last-years/.

Similarly, a US District Judge blocked an Arkansas law on social media age verification that was set to go in effect on 1st September 2023. The legislation was aimed at requiring age verification for use of social media; and to clarify liability for failure to perform age verification for use of social media and illegal retention of data. It is believed that this would have been the first law in the US requiring age verification from new social media users, and to require parental consent.[67]

Meanwhile, Utah's Department of Commerce released a proposal under Utah's social media regulation law, S.B. 152,[68] which requires social media companies to use an age verification process that accurately identifies whether a current or prospective Utah account holder is not a minor. It also requires companies to provide written confirmation to users within 72 hours explaining the method of age verification employed, the result of the verification, and the date the company will delete the age verification information. Parental consent requires both a written attestation from the parent or guardian and the use of a method that verifies parental consent as established under the COPPA.

Impact:

Actions by platforms

The current FTC approved methods for obtaining Verifiable Parental Consent (VPC) includes physical consent forms, credit card authentication, video conferencing, call to toll free number, government-issued ID verification against database, knowledge-based challenges, facial recognition, etc.[69] The FTC's list is not exhaustive for acceptable methods of getting VPC.

Some providers of online services have explored or are exploring additional requirements to verify their users' ages.

- The dating app Tinder requires users in some locations to submit a copy of their driver's licence, passport, or health insurance card to verify their age; it does not allow verification with a resident card, temporary driver's licence, or student identification (ID) card[70]
- In June 2022, Instagram started to test three options for users to verify their age. Users can record video selfies, which are analysed by Yoti, provide ID proof, or ask mutual friends to verify their age.[71]
- In January 2023, Pornhub started requiring users in Louisiana to verify their age with the LA Wallet app—a digital wallet that allows users to upload their driver's licence, in addition to other information.[72]

Enforcement of penalties

TikTok settled with the FTC for $5.7 million over allegations that it violated the Children's Online Privacy Protection Act in February 2019. The FTC complaint alleged that TikTok violated COPPA

67 Ibid.

68 Utah's Proposed Social Media Rule https://socialmedia.utah.gov/wp-content/uploads/2023/10/Social-Media-Regulation-Act-Proposed-Rule.pdf

69 Complying with COPPA: Frequently Asked Questions. Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#C.%20Privacy%20Policies.

70 How does Age Verification Work?. Tinder. https://www.help.tinder.com/hc/en-us/articles/360040592771-How-does-age-verification-work-#:~:text=The%20minimum%20age%20requirement%20for,with%20our%20Terms%20of%20Use.

71 Introducing New Ways to Verify Age on Instagram. Meta. June 2022. https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram#:~:text=If%20someone%20attempts%20to%20edit,friends%20to%20verify%20their%20age.

72 Adi Robertson. Louisiana now requires a government ID to access Pornhub. The Verge. January 2023. https://www.theverge.com/2023/1/3/23537226/louisiana-pornhub-age-verification-law-government-id.

by collecting personal information from kids without parental consent.[73]

In October 2019, Google agreed to pay $170 million to settle charges by the FTC and the New York Attorney General that YouTube illegally collected children's personal data without parental consent.[74] YouTube violated the COPPA Rule by collecting personal information—in the form of persistent identifiers that are used to track users across the Internet—from viewers of child-directed channels, without first notifying parents and getting their consent. The COPPA Rule requires that child-directed websites and online services provide adequate notice of their information practices and obtain parental consent prior to collecting personal information from children under 13, including the use of persistent identifiers to track a user's Internet browsing habits for targeted advertising. While YouTube claimed during the proceedings to be a general-audience site, some of YouTube's individual channels—such as those operated by toy companies—are child-directed and therefore must comply with COPPA.

Reactions of Stakeholders

The US court system has struck down efforts to implement online age verification several times in the past.[75] In 1997, the US Supreme Court ruled parts of the 1996 Communications Decency Act (CDA) unconstitutional, partially because it contained provisions requiring age verification for site visitors of adult sites.[76] Justice Sandra Day O'Connor, in her partial dissent, found that erstwhile Internet technologies were insufficient for ensuring that minors could be excluded while still providing adults full access to protected content. She viewed the CDA as ultimately unconstitutional, while permitting such a law at some point in the future when Internet zoning was technologically feasible.[77]

More recently, a federal court found in 2016 that a Louisiana law, which required websites that publish material harmful to minors verify users' ages, creates a chilling effect on free speech.[78] The law, enacted as H.B. 153,[79] required that "any person or entity in Louisiana that publishes material harmful to minors on the Internet shall, prior to permitting access to the material, require any person attempting to access the material to electronically acknowledge and attest that the person seeking to access the material is eighteen years of age or older." A failure to age-verify, even if no minor ever tried to access the material, would have been a crime subject to a $10,000 fine. To comply with the law, booksellers and publishers would have had either to place an age confirmation button in front of their entire websites, thereby restricting access to

73 Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law. Federal Trade Commission. February 2019. https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy.

74 Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law. Federal Trade Commission. September 2019. https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law

75 Emma Roth. Online age verification is coming, and privacy is on the chopping block. The Verge. May 2023. https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety.

76 Reno v. American Civil Liberties Union. US Supreme Court. 1997. https://supreme.justia.com/cases/federal/us/521/844/.

77 Ronald Kahn. Reno v. American Civil Liberties Union (1997). Free Speech Center. 2009. https://firstamendment.mtsu.edu/article/reno-v-american-civil-liberties-union-1997/.

78 Garden District Book Shop v. Stewart. Middle District Court of Louisiana. April 2016. https://law.justia.com/cases/federal/district-courts/louisiana/lamdce/3:2015cv00738/48815/48/

79 House Bill No. 153. Legislature of Louisiana. 2015. http://www.legis.la.gov/Legis/ViewDocument.aspx?d=959974.

materials that may be appropriate for all ages, or to attempt to review all of the books or magazines available at their websites and place an age confirmation button in front of each individual page that might be inappropriate for any minor.[80]

Recently in September 2023, a federal judge blocked a Texas law requiring age verification for viewing pornographic websites, a day before the law was set to take effect. The Judge found that the law violates First Amendment free speech rights and is too vague.[81] The Judge said that age verification raises privacy concerns especially when done using government-issued ID, given the government is not required to delete data regarding access.[82] This raises concerns about accessing controversial speech when the state government can log and track that access.

A recent report[83] by the US' Congressional Research Service (CRS) updated in March 2023 found that many kids aged 16 to 19 might not have a government-issued ID, such as a driver's licence, that they can use to verify their age online. While it says kids could use their student ID instead, it notes that they may be easier to fake than a government-issued ID. The CRS is not on board with relying on a national digital ID system for online age verification either, as it could raise privacy and security concerns.

II. ALTERNATIVE APPROACHES OF AGE VERIFICATION AND SEEKING PARENTAL CONSENT:

In addition to the techno-legal developments studied in the previous chapter, it is also important to understand the technical taxonomy of age estimation and verification tools which are currently being considered across technology ecosystems. This chapter carries out a qualitative assessments of alternative age verification, and parental consent methods being deployed globally.

Please note that the levels of assurance indicated in the table below are the authors' assessments and are subject to critical review and feedback. A combination of the methods listed in Table III.A (to ascertain age of user) and in III.B (to verify parent-child relationship and parental consent) may be necessary to satisfy the three requirements of Section 9(1) as enlisted in the beginning of this paper. The intention of this discussion is to highlight each method's efficiency and varying impact on users and on data fiduciaries.

80 Court Blocks Louisiana's Online Age-Verification Law for Violating First Amendment. ACLU. October 2016. https://www.aclu.org/press-releases/court-blocks-louisianas-online-age-verification-law-violating-first-amendment.

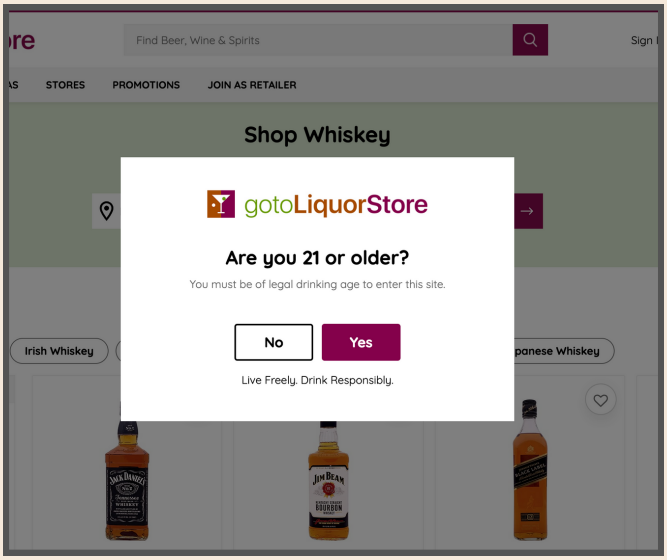
81 Free Speech Coalition v. State of Texas. Western District Court of Texas. August 2023. https://storage.courtlistener.com/recap/gov.uscourts.txwd.1172751222/gov.uscourts.txwd.1172751222.36.0.pdf.

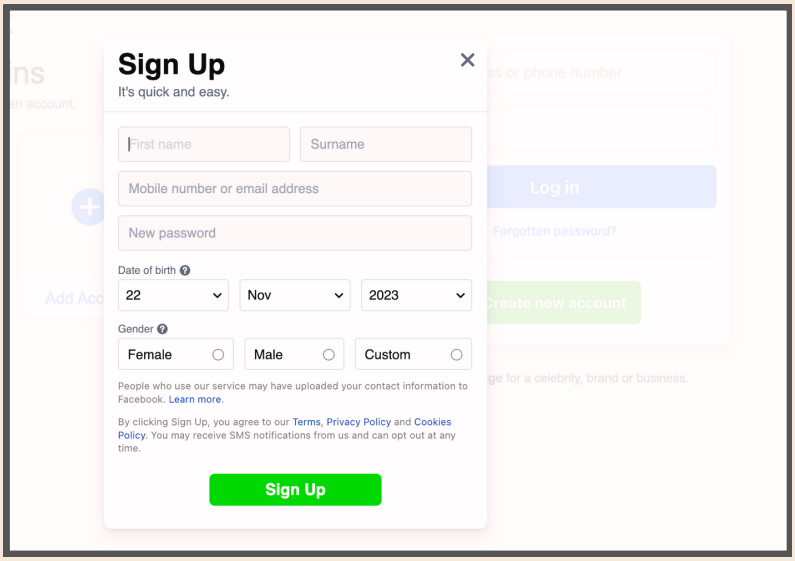
82 Emma Bowman. A Texas law requiring age verification on porn sites is unconstitutional, judge rules. NPR. September 2023. https://www.npr.org/2023/09/01/1197380455/a-texas-law-requiring-age-verification-on-porn-sites-is-unconstitutional-judge-r#:~:text=A%20federal%20judge%20has%20blocked,was%20set%20to%20take%20effect.

83 Challenges with Identifying Minors Online. Congress Research Service. Updated March 2023. https://crsreports.congress.gov/product/pdf/IN/IN12055#:~:text=Potential%20Challenges%20with%20Identifying%20Minors,as%20those%20younger%20than%2013.

Table III.A – Methods to Ascertain User's Age

AGE ASSURANCE SOLUTION	ABILITY TO ASCERTAIN AGE	SAFETY, PRIVACY AND ACCESS FOR USERS	EASE OF DOING BUSINESS
Self-Declaration			
Self-declaration of Date of Birth by the child at the time of registering on a platform or accessing a website. This method is used widely by platforms globally. Has been used by digital services across the entire internet.	This method exhibits low levels of assurance since it is very easy for children to lie about their age.[84]	• This method has low privacy risk as the platform does not require verification using Government ID. • It is more digitally inclusive as it does not require much technical competence of children. • This can lead to the unintended consequence of children of lower maturity accessing unsuitable content or engaging in unsafe behaviour.[85]	• This method incentivises frictionless innovation. • It is easy to operationalise since it does not require significant architectural changes on the platform. • While data principals have a duty to provide accurate data about themselves under the Act, if a platform processes children's data without adequate protections, it may open them up to litigation for causing 'detrimental effect to their well-being' under Section 9(2).





84 But how do they know it is a child?. 5Rights Foundation. October 2021. https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf

85 Sally Weal. One in 10 children 'have watched pornography by time they are nine'. The Guardian. January 2023. https://www.theguardian.com/society/2023/jan/31/one-in-10-children-have-watched-pornography-by-time-they-are-nine

AGE ASSURANCE SOLUTION	ABILITY TO ASCERTAIN AGE	SAFETY, PRIVACY AND ACCESS FOR USERS	EASE OF DOING BUSINESS
Analysis of User Behaviour			
Profiling, user behaviour on the platform Estimates are based on a user's online public profile and how they interact with an online service – their interests, their friends, their school etc.[86]	This method exhibits low levels of assurance as it cannot determine an exact age, and has a wider margin for error and risk of evasion. However, it may be able to determine an age range with a reasonable degree of assurance.[87] Where there is an incorrect estimation, the platform may have to invest in alternative methods. While tracking is prohibited under Sec. 9(3) of the Act, the Government can consider allowing an exemption under Sec. 9(4) to facilitate this method for ascertaining age of user.	• This method is likely to perpetuate biases and discriminatory behaviour as browsing history is likely to indicate social, regional, sexual identifiers.[88] • It can lead to tracking user behaviour on all websites. Cookies are used by websites to track the time a particular user spends on the website and to find the links the user clicks on that particular website.[89] This may pose a privacy risk in itself as individuals may be personally identified using this data.	• This method can allow for dynamic assessment of risks and allow platforms to take added consent or age assurance when it deems that a certain profile is more vulnerable to the negative aspects of a platform. It is more likely to be utilised by big tech platforms who have sufficient user behaviour data to process. • Similarly, startups will be able to scale up investments in age assurance depending on the risk profile of its platform and the propensity for harmful usage by people below the age of 18. • It also allows startups to undertake timely investments into age assurance systems only once its platform hits a certain scale and usage patterns contribute to an inordinate risk level. • Consequently, there is some scope for startups to scale in the digital economy using lean operational models.

86 How do you check age online?. Age Verification Providers Association. https://avpassociation.com/avmethods/.

87 But how do they know it is a child?. 5Rights Foundation. October 2021. https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.

88 Thomas Ploug. The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling. Philosophy and Technology. v. 36. 2023. https://link.springer.com/article/10.1007/s13347-023-00616-9. 1

89 Michael Trusov et. al. Crumbs of the Cookie: User Profiling in Customer-Base Analysis and Behavioral Targeting. Marketing Science. v. 35. April 2016. https://www.researchgate.net/publication/301715599_Crumbs_of_the_Cookie_User_Profiling_in_Customer-Base_Analysis_and_Behavioral_Targeting

AGE ASSURANCE SOLUTION	ABILITY TO ASCERTAIN AGE	SAFETY, PRIVACY AND ACCESS FOR USERS	EASE OF DOING BUSINESS
Natural language processing Social media users frequently disclose their birthday or their age in their biography. Simple Natural Language Processing detects age related patterns and it provides the first prediction of age. This is then compared with profile picture analysis and ages of mutual friends to predict a user's age.	This method exhibits low levels of assurance as it could misestimate the age of the user and include a child who has mature interests or exclude adults who might be neurodivergent. Where there is an incorrect estimation, the platform may have to invest in alternative methods. Additionally, they must provide users with adequate means for transparent and accountable grievance redressal for incorrect divisions.	• This method is likely to present a major privacy risk since language models can memorise sensitive personal information such as Aadhaar details/ birthdays. [90] • It can also perpetuate biases against marginalised communities. [91]	• Similar to the profiling method, this can be utilised by big tech platforms who have sufficient user data and capacity to process it. • At the same time both this method and the user profiling option do not sufficiently assure compliance with the requirement of "verifiable parental consent". Thus, any inaccuracies using these methods will leave digital services i.e., data fiduciaries open to litigations and heavy fines under the DPDP Act.

90 Nicholas Carlini. The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks. arXiv. 2018. https://arxiv.org/abs/1802.08232.

91 Tolga Bolukbasi et. al. Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings. NIPS. 2016. https://papers.nips.cc/paper/2016/file/a486cd07e4ac3d270571622f4f316ec5-Paper.pdf.

AGE ASSURANCE SOLUTION	ABILITY TO ASCERTAIN AGE	SAFETY, PRIVACY AND ACCESS FOR USERS	EASE OF DOING BUSINESS
Biometrics/Facial Recognition			
Biometrics Facial scans, hand geometry, voiceprints, gestures and keystrokes (how you type)[92]are used to estimate the age of the user. The facial estimation technique described here is quite distinct from facial recognition as no images are being matched for the purpose of estimating age.	This method exhibits low levels of assurance since it has limited accuracy in distinguishing a 17 year old from an 18 year old which is crucial for operationalising the provisions of the Act.[93]	• This method needs a smartphone with a camera. Some studies observe that in 2022 over 74.8% of Indian households had access to a smartphone [94]Yet, there is a stark gendered digital divide, since over 60% men in India are reported to own a mobile phone, compared to less than 31% women.[95] Even where the household has a smartphone, access for women is likely to be curtailed due to patriarchal reasons.[96] • Access to the camera on the user's device during an initial enrolment with a third party,	• With the proliferation of camera friendly smartphones and an increase in digital literacy, this method can be operationalised gradually. • Various platforms such as dating websites, fintech platforms etc have already adopted this method. Institutionally such a system will require setting up an alternative dispute resolution method for users, which will require additional investment from the platforms as well as investments in regulatory capacity at the level of the Data Protection Board of India.[97]

92 How do you check age online?. Age Verification Providers Association. https://avpassociation.com/avmethods/.

93 Ashley Johnson. AI Could Make Age Verification More Accurate and Less Invasive. ITIF. April 2023. https://itif.org/publications/2023/04/05/ai-could-make-age-verification-more-accurate-and-less-invasive/

94 Saurav Anand. India has over 1.2 bn mobile phone users: I&B Ministry. Mint. November 2022. https://www.livemint.com/technology/gadgets/india-has-over-1-2-bn-mobile-phone-users-i-b-ministry-11668610623295.html

95 Rahul Singh. Only 31% women own mobile phones, says Oxfam Report on India Digital Divide. Hindustan Times. December 2022. https://www.hindustantimes.com/technology/only-31-women-own-mobile-phones-says-oxfam-report-on-india-digital-divide-101670317918778.html.

96 Barkha Dutt. India's persistent gendered digital divide. Rest of World. October 2023. https://restofworld.org/2023/india-gender-gap-digital-divide/.

97 Scott Brennen & Matt Berault. Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?. Center for Growth and Opportunity. June 2023. https://www.thecgo.org/research/keeping-kids-safe-online-how-should-policymakers-approach-age-verification/

Facial recognition may be used to check that a user relying on a previous age check is still the same individual who completed the check, but that is a separate process required for "authentication" rather than age estimation?[99]		or a one-off verification by the same third party, can later become a source of blackmail via the webcam when accessing a website.[98] • There is no need for age estimation to retain any information about an individual, as the result is immediate, and the facial image can be instantly deleted. The technology does not require enough data for that data to be unique to the individual.	

98 https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors
99 https://avpassociation.com/avmethods/

Capacity Testing The user is required to undertake a language test, solve a puzzle or undertake a task that gives an indication of their age or age range.	This method exhibits moderate level of assurance since there is a high possibility of circumvention due to online sharing of responses which can open platforms to legal liability.	• This method could potentially perpetuate biases against individuals with less developed reading comprehension skills, language proficiency and can even be impacted by communities' access to education, schooling, digital skill development, etc. [100] • It avoids transfer of personal data, adhering to the principle of data minimisation.	• This method is easier to implement than other methods if a third party provides this service.
Existing account holder confirmation An adult who has already been age-verified, provides confirmation that a child is of a certain age. For example, an adult may open an account for watching video content online and create a profile for their children to use that account in a limited age-appropriate manner.	The efficiency of this method is predicated on the accuracy of the verification of the parent and the parent-child relationship. It relies on the honesty and involvement of a parent or legal guardian, and it is also not easy to confirm that the person creating the child's profile has the legal power to do so.	• This method needs parents' ID/age to be confirmed which depends on their IT proficiency and can be bypassed by knowledgeable children. • Given the constant evolution of tech, it will only solve for the most widely used platforms, as parents will be unable to predict all the platforms the child will use. • Such an approach to parental oversight could be excessive and lead to an overall chilling effect on children's use and skills development using digital platforms.(see Danielle Citron) [101]	• This method requires the platform to verify age at the parents' level, which may involve costs and changes in the platform's architecture. • The platform does not have to collect huge volumes of data to verify the age of the child which helps in saving costs related to data storage, data audits etc.

100 Samarth Bansal & Pramit Bhattacharya. The Geography of Learning Outcomes in India. Mint. January 2019. https://www.livemint.com/education/news/the-geography-of-learning-outcomes-in-india-1548178547466.html.

101 Danielle Citron. The Surveilled Student. Stanford Law Review. v. 76. August 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4552267.

AGE ASSURANCE SOLUTION	ABILITY TO ASCERTAIN AGE	SAFETY, PRIVACY AND ACCESS FOR USERS	EASE OF DOING BUSINESS
Hard Verification through Government IDs			
Platform level The proposal to verify users' age through government ID instruments which are stored in DigiLocker would fall under this. On a related note the Account Aggregator ecosystem for financial services in India is also an example of a consent management ecosystem which is being scaled on top of a designated consent architecture (DEPA)![102] [103] The AA Model could be a template for hard parental consent.	These methods exhibit the highest levels of assurance, provided that the ID provided by the user/ verified through a consent manager is authentic. There exists a minor chance that hard verification may be circumvented if an individual manages to input fake personal information when providing the ID.[104]	• This method exposes the user to the highest level of privacy risk, since a data breach in this context may involve various sensitive personal information points such as name, age, address, blood group, etc. linked to the kind of content they are consuming online. Moreover, information like biometrics are immutable and thus the privacy and security risks naturally increase. • It also goes against the purpose of data minimisation as the platform is forced to collect information which may not be necessary to verify age.	• The platform/device, etc. may collect the ID information directly from the user, or through a third party consent manager. • Either way, this method is likely to increase compliance burden for businesses as they would need to build brand new API flows to provide for such age verification. • In the case of device level verification, this method could potentially offer a one-time solution to ascertain the user is a child, since a presumption arises that the phone is being accessed exclusively by a minor. This will significantly reduce friction for platforms/apps which the user accesses through the phone.

102 Data Empowerment and Protection Architecture.

103 What are Account Aggregators?. Sahamati. https://sahamati.org.in/what-is-account-aggregator/.

104 Scott Brennen & Matt Berault. Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?. Center for Growth and Opportunity. June 2023. https://www.thecgo.org/research/keeping-kids-safe-online-how-should-policymakers-approach-age-verification/.

Device, app store, or wider value chain level controls This would apply to upstream entities in the value chain such as device manufacturers, browser operators, app store operators, email service providers, third party ID verification providers, and other API-based user registration facilitators. The idea is to create a 'children's phone', making features, services and content child appropriate by default.	As with platform level, these methods exhibit the highest levels of assurance, provided that the ID provided by the user/ verified through a consent manager is authentic. There exists a minor chance that hard verification may be circumvented if an individual manages to input fake personal information when providing the ID.	• This method will not be effective in case of shared devices since one phone could be used by adults and children alike, making age verification redundant. It may violate the principle of data minimisation since the Government ID provided may contain information beyond what is required for age verification. Further such data may also be susceptible to illegal processing and breaches	

The methods listed above describe various means to fulfil the first element of the three we identified at the beginning of this paper. After verifying that the user is indeed a child, the platform then has the onus of ascertaining the relationship between the person purporting to be the child's parent/guardian, and taking such person's consent on behalf of the child.

We foresee that these latter two elements may be fulfilled in the following manners. In both methods below, the platform may be required to incur costs of sending an OTP to the parents' mobile/email ID, to be able to verify their consent.

Table III.B – Methods to Collect Parental Consent

PARENTAL CONSENT SOLUTION	ABILITY TO ASCERTAIN RELATIONSHIP AND CONSENT	SAFETY, PRIVACY AND ACCESS FOR USERS	SAFETY, PRIVACY AND ACCESS FOR USERS
Hard verification of relationship based on Government issued ID Card followed by consent The child user will be required to share their parents ID information, such as by uploading an image of the ID document, inputting the ID Card No., etc. Once the information is provided, the platform can review it internally or rely on third-party services to verify the information. The Government of India's intention to use DigiLocker services is likely to fall under this method.	This method offers the highest level of certainty in establishing the parent-child relationship, since the ID Card is likely to provide this information directly. The OTP received on the mobile number/email linked to the ID Card shall be presumed to be proof of the parent's consent. The underlying premise here is that the platform can rely on online verification services provided by the entities managing the ID Cards, such as UIDAI for Aadhar, Income Tax Department for PAN Card, etc.	• The ID Card provided by the child user/parent is likely to contain other information as well which may not be relevant to the issue of obtaining verifiable parental consent. In this context of existing solutions, this hard verification method would seemingly be against the principle of data minimisation, as it will push platforms to collect more information than is necessary. • Data minimisation may be upheld if there is a technological solution where platforms have access only to the limited extent of ascertaining parental relationship, and their consent via OTP.	• This method is likely to impose significant costs on platforms, as they may either have to set up internal review processes, or rely on third-party services. There are also the added costs of sending OTPs due to SMS charges. • Platforms may also have to bear investments towards data security and safeguards for the sensitive personal information being collected due to this method, and may incur liability in case of data breaches. • This is likely to cause friction for the sign-up process for new users. For instance, the parent may not be available to give consent at the time when the child is trying to sign up. This issue is more relevant in the case of working parents. This can lead to a significant increase in cost of customer acquisition.

After the relationship is ascertained, the user can be required to share an OTP received on the parent's linked mobile number.		• Users lacking access to the relevant ID Card may face difficulties in accessing the digital product/service and scanning and uploading requires a degree of tech usage sophistication as well assumes smart device access. This could disproportionately impact low-income groups.	
Self-declaration by child of parental relationship followed by consent from parent The child user can self-declare the details of the parent. For instance, the child can input the parent's mobile number or email ID, and be required to share an OTP received by the parent.	The platform's ability to ascertain the relationship between the purported parent/guardian and the child is low in this method. This method can be circumvented as the child may input phone numbers of friends, personal secondary numbers, etc. or may create new email addresses in the name of their parents to gain consent. In households where parents rely on children to navigate the digital world, children also have access to their parents' phone and may be able to easily input the OTP from the parent's device. There is also a high incidence of shared device usage in India, which raises questions on the efficacy of this solution.	• These effects will be pronounced in settings like low-income households where children use shared devices and/or parents have scarcity of time due to the nature of their work (for instance daily wage earners).	• This method creates a layer of 2 factor authentication (self-declaration of age by child, and OTP by parent), which is likely to increase friction for businesses as the process of signing up as a new user becomes more tedious.

IV. KEY TAKEAWAYS BASIS GLOBAL DEVELOPMENTS AND AVAILABLE TECHNOLOGICAL SOLUTIONS

An overview of global developments and various age assurance methods in vogue offers some useful insights for India.

1. **Lack of consensus on age assurance mechanisms and need for feasibility studies**

While many countries are actively discussing how to best ensure children's safety online, there is a stark diversity in their approaches and the technologies being used to achieve the intended goals. This indicates the complex nature of the problem at hand. **There are strong concerns that age assurance mechanisms may lack efficacy, create inequity in access, lead to privacy concerns, and impose cost barriers and inconveniences in enabling children to engage with online experiences**.[105]

As recently as in August 2023, the Australian Government chose against mandating hard age verification on platforms by relying on the Australian eSafety Commissioner's report, noting "it is clear from the report that at present, each type of age verification or age assurance technology comes with its own privacy, security, effectiveness and implementation issues."[106] The French data regulator CNIL concurs, describing age verification as a "complex issue with significant privacy risks' since the identity of internet users is verified often through collection of sensitive data, and it can be then linked to their online activity."[107] It continued, that any such mechanism ought to have "sufficiently reliable verification, (have) complete coverage of the population and respect for the protection of individuals' data and privacy and their security". Eventually CNIL found that there was no solution at the time of publication (in September 2022) which met all three requirements.[108]

Acknowledging these limitations, regulators are working with children, parents, consent managers and platforms to understand online attitudes towards various mechanisms, online behaviour, aspirations, etc.[109] It is in this context that regulators like the UK's ICO have also commissioned

105 *The State of Play: Is Verifiable Parental Consent Fit for Purpose?. Future of Privacy Forum. June 2023. https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf.*

106 *Government's response to the Roadmap on Age Verification. Australian Government. August 2023. https://www.infrastructure.gov.au/sites/default/files/documents/government-response-to-the-roadmap-for-age-verification-august2023.pdf.*

107 *Online age verification: balancing privacy and the protection of minors. CNIL. September 2022. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.*

108 *Ibid.*

109 *Informing the Age Appropriate Design Code. ICO-Revealing Reality. 2019. https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf; Families Attitudes toward Age Assurance: A study commissioned by ICO and Ofcom. Digital Regulation Cooperation Forum. October 2022. https://www.ofcom.org.uk/__data/assets/pdf_file/0026/245195/DRCF-Ofcom-ICO-age-assurance.pdf; Young people's attitudes towards online pornography and age assurance. Australia eSafety Commissioner. 2023. https://www.esafety.gov.au/research/young-peoples-attitudes-towards-online-pornography-and-age-assurance.*

studies to study the feasibility of various available options.[110] **It would be appropriate for the Indian Government to also consider conducting similar studies by involving interested stakeholders on a periodic basis to deliberate on the feasibility of solutions as it looks to implement the requirements of Section 9 of the DPDP Act, 2023.**

2. Shift away from self-declaration of age towards adopting a flexible range of age assurance mechanisms

Data protection laws for children typically come into effect only after a platform knows that their services may be accessed by children, or when they have actual knowledge that the user is below a certain age threshold. The primary question here that platforms must deal with is whether the user is a child. For instance, the COPPA in the US was one of the earliest laws dealing specifically with children's data, and it has arguably had the largest impact on digital users' experience worldwide. Under its mandate, platforms began to offer the option to self-declare their age to the user. In that scenario, the COPPA's mandate of obtaining verifiable parental consent kicked in only if the user said they are below 13 years of age.[111] Businesses preferred this option as it caused least friction in the signup process, even though there exists scope for users to lie about their age. Alert to this challenge, data protection regulators are now considering other options to determine the age of the user. These options, some of which are described in the table above, may be useful in different contexts and use cases, with most countries experimenting with a mix of these. This is typically elaborated in the data regulator's guidance on the issue of children's data and age assurance - such as in the UK ICO's Opinion on Age Assurance Mechanisms,[112] the US FTC's Guidance on Complying with COPPA,[113] Ireland's Data Protection Commission's 'Fundamentals for a Child-Oriented Approach to Data Processing', etc.[114] In most jurisdictions, the flexibility to use a particular age assurance mechanism corresponds to the risk that a particular data processing activity poses. This could depend on factors such as the collection of sensitive information, nature of interactions the child has on the platform, scope for exposure to inappropriate or illegal content, etc.

3. Risk of exclusion due to demographic and digital realities

Apart from the risk of theft or misuse of data collected in the process of age verification, insistence on certain hard verification methods such as identity documents or credit card information leads to concerns around inequitable access and exclusion of vast swathes of society.

Estimates from the National Statistical Office (78th Round 2020-21) reveals that less than 40% Indians know how to copy or move files on a computer, with an even lesser proportion having knowledge of internet use. The survey also found that digital literacy is better in lower age groups,

110 *Tony Allen et. al. Measurement of Age Assurance Technologies: A Report for the UK ICO. Age Check Certification Services. 2022. https://ico.org.uk/media/about-the-ico/documents/4021822/measurement-of-age-assurance-technologies.pdf.*

111 *FTC Settles COPPA Violation Charges Against Yelp and TinyCo. Hunton Andrews Kurth. September 2014. https://www.huntonprivacyblog.com/2014/09/23/ftc-settles-coppa-violation-charges-yelp-tinyco/.*

112 *Information Commissioner's Opinion: Age Assurance for the Children's Code. UK ICO. October 2021. https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf.*

113 *Complying with COPPA: Frequently Asked Questions. Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#C.%20Privacy%20Policies.*

114 *Fundamentals for a child-oriented approach to data processing. Irish Data Protection Commission. December 2021. https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf.*

and reduces among older populations. Further, digital literacy is worse off in rural households. Despite this context, the Bill relies on parental consent, assuming parents to be better placed to understand the potential risks of online data processing. This ignores abundant empirical evidence of the digital divide faced by the elderly as well as anecdotal evidence wherein parents in fact seek advice from their children about navigating digital devices and the internet. For instance, in a survey of around six thousand secondary school children conducted by the Delhi Commission for Protection of Child Rights (DCPCR) and the Young Leaders for Active Citizenship (YLAC), over 80% of the respondents said that their parents take their help to use digital devices.[115]

These issues would be further exacerbated by gender dynamics around shared device usage within a household, where one mobile phone may be shared between members for different purposes.[116]

V. WAY FORWARD FOR INDIA

A review of global discussion on age assurance methods highlights the complexity of the issue. The practical, moral and legal hurdles in mandating a hard identification requirement implies that a one size fits all approach is likely to impede access to the internet for young digital nagriks.

We propose an approach where India allows diverse age assurance mechanisms to be used by platforms and families. The age assurance mechanism in use should correspond to the nature of the data processed, purposes it is processed for, risks associated with it such that the chosen mechanism causes the least detrimental impact to the child in terms of access, equity and safety on the internet. Our proposed approach which we recommend to Indian policymakers is as follows:

Step 1: MEITY is empowered under Section 40(2)(i) to publish rules on the ***'manner of obtaining verifiable consent'*** under Section 9(1). MEITY can work with industry players, parent associations, organisations working with children, etc. and publish rules in the form of a **code of practice on age assurance** mechanisms that a platform should deploy, corresponding to their use-case and risk from their data processing. The Government ought to use this opportunity to consider various mechanisms being used by platforms globally, and do a cost-benefit analysis of the commercial/institutional ease of use, degree of certainty of estimating the user's age, and associated risks.[117]

Step 2: Platforms ought to be encouraged to conduct and publish a **self-assessment of the nature of risks** to children emanating from their data processing activities. This assessment should describe what data is collected, how it is processed (for what purposes and risks emanating from it which could harm children) and measures taken to mitigate these risks. An assessment of risks in this manner is likely to have the two-fold effect. Firstly, it will increase public scrutiny of the platform's design and data processing practices and would provide better

115 YLAC-DCPCR Digital Champions survey 2023

116 Dr. Lina Sonne. Women's Mobile Phone Access and Use: A Snapshot of Six States in India. Dvara Research. June 2021. https://www.dvara.com/research/wp-content/uploads/2021/06/Womens-Mobile-Phone-Access-and-Use-A-Snapshot-of-Six-States-in-India.pdf.

117 Scott Brennen & Matt Berault. Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?. Center for Growth and Opportunity. June 2023. https://www.thecgo.org/research/keeping-kids-safe-online-how-should-policymakers-approach-age-verification/

incentives for thoughtful platform design where privacy and data protection are factored in to avoid reputational risks. Second, the Data Protection Board will be able to hold platforms accountable on their own assessments and policies, if a case was to be heard.

Step 3: Based on the self-assessment of risk, and the MEITY's Guidance, the platform must decide the age assurance mechanism that is appropriate for their product or service. If a platform fails to conduct age assurance (estimation or verification) in accordance with the risk emanating from their product/service, they would incur penalties under Section 9(2) of the DPDP Act, 2023 - for processing data in a manner 'likely to cause detrimental effect to the well-being of the child'. These penalties could result either from a complaint from a data principal or on a reference from the Central or a State Government. We envisage two outcomes which may emerge as a result.

1.Hard verification for high-risk use-cases which children are legally prohibited from accessing

Mechanism: The suggestion to have KYC-based verification to access online services can be classified as 'hard verification'. It includes methods such as identity-cards, credit card information, DigiLocker etc., which allows the platform to verify the user's age with highest level of certainty (due to its reliance on documentary proof), but risks sharing of other sensitive information as well. While news reports suggest that the Government is considering creating a mechanism to allow sharing of only a consent artefact and thereby eliminate the sharing of other unnecessary information,[118] there persist privacy risks since the user's ID will be linked to all such products/services where it is used for age verification. This creates security and privacy risks from malicious actors, both state and non-state, due to risk of data breach, cybercrimes, etc.[119] These methods would be appropriate where there exists a high-level of risk to a child user, in terms of how their data could be processed or if they end up accessing age-inappropriate content.

Platforms covered: Typically, this would include services such as websites intended for adult use such as to access pornographic audio-visual content or to purchase alcohol or tobacco, etc. to which access is not legally permitted but which children nonetheless may access in status quo. The United Kingdom is also considering the role of app-stores in allowing children's access to inappropriate or illegal content and may require them to deploy hard verification mechanisms.[120]

Intended Outcome: Products and services deemed unsuitable for children under any other law will be inaccessible to children. Hard verification will be a useful tool to ensure that children are protected against porn or other online content prohibited under IT Rules, 2021; cigarettes and alcohol which they are prohibited from under COPTA, 2003 and excise laws, etc.

2. Option to use other appropriate age assurance mechanisms

Mechanism: If a platform claims that the data processed from their product/service poses a lower

118 Suraksha P. Soon, store parental consent in DigiLocker. The Economic Times. August 2023. https://economictimes.indiatimes.com/tech/technology/soon-store-parental-consent-in-digilocker/articleshow/102954908.cms.

119 Creating a good ID system presents risks and challenges, but there are common success factors. World Bank Identification for Development. https://id4d.worldbank.org/guide/creating-good-id-system-presents-risks-and-challenges-there-are-common-success-factors.

120 Online Safety Bill bolstered to better protect children and empower adults. Government of UK. June 2023. https://www.gov.uk/government/news/online-safety-bill-bolstered-to-better-protect-children-and-empower-adults; Online Safety Bill, Consideration of Lords Amendments, House of Commons. Local Governments Association. September 2023. https://www.local.gov.uk/parliament/briefings-and-responses/online-safety-bill-consideration-lords-amendments-house-commons.

level of risk to the child, it can choose from other prescribed age assurance mechanisms. This could include options such as biometrics, maturity tests, profiling based on user activity on the platform, cross-account authentication, etc. offer varying levels of certainty of the user's age. This option can be offered to platforms that are either collecting less sensitive data due to the nature of product/service being offered, or are designed in compliance with prescribed risk mitigation and prevention strategies. In both instances, the age assurance would correspond to the likelihood of detriment being caused to the child. Such platforms should continue to periodically assess risk and as their platform reaches maturity or its risk profile changes should be willing to escalate to more sophisticated forms of age assurance and parental consent.

Platforms covered: Other than legally prohibited and/or adult oriented platforms, all others such as social media, skilling and educational platforms for topics on personal development, finance, language, gaming, streaming apps, etc.

Intended outcome: Platforms which have adequate data protection standards and processes in place can choose from a range of age assurance mechanisms, which is most suitable to the interests of their users and their business. This offers children access to products/services that they are legally entitled to. Platforms are also likely to improve their design since doing so would enable them to choose a softer verification, which reduces user friction.

Step 4: Empower a consent manager ecosystem: Over time, a consent manager ecosystem can be developed where players offer a range of age assurance services to platforms. As part of their operational requirements, the Data Protection Board can prescribe that consent managers have to regularly consult with children, parents, organisations working with children, etc., to factor in feedback on their safety, privacy, ability to freely access information over the internet, and other considerations in the child's best interests. Platforms should be allowed to partner with one or more registered consent managers, to increase choice for the users and encourage market competition.

Further, their services can also be used by actors across the value chain, for instance by app stores and device manufacturers, in case the Government issues that mandate. The government should propose a willingness to set up a working group with all ecosystem actors to build protocols for scalable parental consent which allows other digital services to easily validate a child's access. This step is intended to develop scalable and interoperable consent solutions to work towards a smooth, equitable and safe experience on the internet. The consent manager ecosystem can be integrated with India's rapidly developing digital public infrastructure (DPI) initiatives. This will increase operational flexibility for platforms on these DPIs, such as e-commerce, healthcare, payments platforms, etc.

Finally, the Indian Government should develop and recognise progressive standards for age assurance, akin to the ones currently under development at international standards development organisations like the ISO.[121] MeitY could form a working group of industry and subject matter experts to work with the Standardisation Testing and Quality Certification (STQC) Directorate and the Bureau of Indian Standards (BIS) on this matter.[122] This could be an initial step which helps India shape international discourse on standardisation of age assurance.

121 Age Assurance Systems Framework. ISO/IEC AWI 27566-1. ISO. https://www.iso.org/standard/80399.html#lifecycle.

122 Standardisation Testing and Quality Certification I(STQC) Directorate, Ministry of Electronics and Information Technology. Government of India. https://www.stqc.gov.in/.

VI. CONCLUSION

The discussion around children's data privacy and protection in India is still nascent. India has the opportunity to bring in necessary innovation to age verification/assurance ecosystems while acknowledging constraints posed by user sophistication and accessibility. The ability to achieve the goal of striking the right balance between children's privacy, safety, and agency to access the digital world is also contingent on how well we understand the user group including intra-household dynamics between children and their parents. It is vital that the governance ecosystem acknowledge the differential gender dynamics in digital access, usage of shared devices, and different online behaviour and aspirations. Many countries undertake large scale surveys to better understand children's internet usage, which evolves rapidly. To help formulate policy in the future, the Indian government, too, must consider setting up a clear mandate to regularly collect evidence through surveys to understand digital habits of young users, and to involve multiple stakeholders who work closely with children and young adults themselves in the consultative process.

मातृभूमि न्यूज़

@matrabhuminews

देशहित की बात

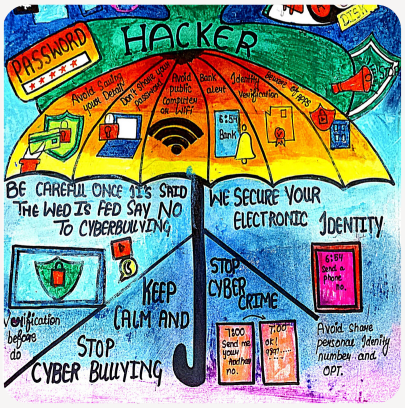
डिजिटल पेज www.matrabhuminews.com रविवार, 23 सितंबर 2023

डिजिटल चैंपियन बने और सुरक्षित रहें

जयपुर के 3000 से ज्यादा स्टूडेंट्स को करवाएंगे निशुल्क डिजिटल सेफ्टी ट्रेनिंग कोर्स

जयपुर (मातृभूमि न्यूज)। दिनांक 23 सितम्बर 2023 को आगाज एडटेक फाउंडेशन और वायलेक आर्गेनाइजेशन की और से जयपुर मौलाना आजाद यूनिवर्सिटी के जयपुर ऑफिस में डिजिटल चैंपियन प्रोग्राम के लिए टीचर्स ट्रेनिंग आयोजित की गयी। आगाज एडटेक फाउंडेशन के फाउंडर मोहम्मद शहजाद ने बताया की इस प्रोग्राम के जरिये जयपुर शहर के 3000 से ज्यादा कक्षा 8 से 12 के स्टूडेंट्स को डिजिटल चैंपियन बनाया जाएगा जिससे वे भविष्य में इन्टरनेट का सही इस्तेमाल और ऑनलाइन दोखाधडी से स्वयं का और अन्य लोगों को बचाव कर सकेंगे। कार्यक्रम का उद्देश्य 13 से 18 वर्ष की उम्र के छात्रों को ऑनलाइन सुरक्षा के विभिन्न पहलुओं के बारे में जानकारी देना है। यह कार्यक्रम छात्रों को इंटरनेट पर संभावित खतरों से, फेकन्यूज से, टेक्नोलॉजी के मानसिक प्रभावों से अवगत कराता है। वायलेक दिल्ली की टीम से सुश्री हिमानी और अनुष्का और आगाज की ओर से रानीया और यासिर ने टीचर्स के साथ प्रोग्राम की डिटेल जानकारी साझा करते हुए यह भी बताया की प्रोग्राम किस तरह से स्कूल्ज में कियान्वित किया जाएगा। इस निःशुल्क ट्रेनिंग प्रोग्राम से जुड़ने के लिए आगज एडटेक फाउंडेशन से संपर्क किया जा सकता है।

विज्ञापन और ख़बर भेजने के लिए matrabhuminews@gmail.com पर ईमेल करें या 9461844343 पर व्हाटसएप करें



In pictures: Teacher trainings, school orientations, winning entries from the poster making competition under the YLAC Digital Champions Program.

ABOUT TQH

Founded in 2017, The Quantum Hub (TQH) is a multi-sectoral public policy research and consulting firm. Within its technology policy practice, it has been working on various digital economy and governance issues, and has closely tracked discussions around data protection and online safety. The firm has written widely and commented on these issues, tracing back the conversation to the Justice Srikrishna Committee report in 2017, up to the current conversation around a new Digital India Act. Taking a leaf from its sister organisation YLAC's work with teenagers and adolescents, TQH was one of the early voices to highlight the impact of the age verification and parental consent provisions on this demographic, and also on other digital users in India. It also works with technology companies to navigate these provisions and regularly participates in the tech policy ecosystem discussions on these topics.

ABOUT YLAC

Founded in 2016, Young Leaders for Active Citizenship (YLAC)'s interventions are designed to equip young people with a better understanding of the society they live in and the challenges that it confronts. One of the verticals of YLAC's work is around digital citizenship under the 'YLAC Digital Champions' Banner. This program is aimed at enabling young adults to learn about various facets of online safety, such as risks and potential threats on the internet, becoming conscious consumers of information, and fostering a healthy and meaningful relationship with technology, along with using the internet for individual and their community's growth.

The program targets students between the ages of 13 and 18 and is delivered to students via collaborations with schools across the country. It is designed keeping in view the limited access to devices amongst students from government and affordable private schools and is delivered through a self-paced model on an easy-to-navigate platform. First piloted in 2021, the program has reached more than 20,000+ students and 100+ schools as of November 2023.

November 2023

www.thequantumhub.com

The Quantum Hub (TOH)
No. 29-30, Lala Lajpat Rai Marg, Lajpat Nagar III
Delhi - 110024
+91-11-4084-5940

office@thequantumhub.com