Briefing Paper

CUTS® International

Global Technological Developments in Age Verification and Age Estimation

Children, while accessing the internet, are vulnerable to different kinds of online harms like cyber-bullying, addiction, accessing age-restricted content, and personal data processing among others. These may hamper their overall development and well-being. In this context, there has been a global call for making the internet a safer space for children by adopting two principle measures - offering age appropriate content and restricting the personal data processing of children by data fiduciaries. To adopt these measures, it is essential to verify the age of online users through technological means. To establish a legislative compliance requirement for this, in India, the draft Personal Data Protection Bill (PDPB), 2019 mandates data fiduciaries to conduct age verification and obtain parental consent before processing children's data. It further empowers the proposed Data Protection Authority (DPA) to prescribe Codes of Practice for the same.

Globally, technology to verify the age of online users is rapidly evolving. In light of the PDPB proposing to mandate age verification, it is imperative to analyse such developments. Without specifically delving into the issues of content moderation and personal data processing of children, the objective of the Briefing Paper is to create an understanding about the existing and emerging global technological developments in age verification and age estimation (collectively termed as age assurance) for accessing online services so that young persons and children can be protected from online harm. A comparative analysis of different methods has been done based upon parameters such as privacy, ease of use for children, accessibility and inclusivity, accuracy and feasibility.

The DPA may utilise the stated parameters as design principles for issuing Codes of Practice for the manner of age verification. It is important to take into consideration the feasibility of adoption and thus, a combination of methods to verify age may be utilised. Further, choosing an appropriate age assurance method requires understanding the viewpoint of children and their parents so that children's privacy, data, and interests can be protected and the DPA should take into account the same while formulating Codes of Practice. In this regard, CUTS International is conducting a survey which captures views of children and parents on the issue.

Introduction: Need for having Age Verification

The internet penetrates across socio-economic classes through various means. Today, we are surrounded by internet-enabled devices and platforms and use them for various purposes. Children, too, use them for things like education, entertainment, social interactions, etc. With the COVID-19 pandemic-induced lockdowns being imposed, children's use of the internet for accessing online education, social media and online gaming apps has tremendously increased (Jain, Gupta, Satam, & Panda, 2020).

Children's use of the internet can promote their overall well-being, which includes mental and social well-being. The internet acts as a powerful communication tool and gives children the potential to create strong social networks which can promote their well-being (Castellacci & Tveito, 2018; Bekalu, McCloud, & Viswanath, 2019). Further, it also provides them with accessibility to various resources, helping in their mental development. However, internet usage also makes children vulnerable to different kinds of online harm, which needs to be addressed (UNICEF, 2020; Jain, Gupta, Satam, & Panda, 2020). A broad classification of the different kinds of online harms children face while accessing the digital world is necessary. The same is given below:

1. **Cyber-Bullying:** Cyber-bullying is the practice of using the internet to bully a person. This may include but is not limited to intimidating and harassing an individual through text messages or other means, threatening to cause sexual exploitation and abuse, emotional abuse by trolling and posting derogatory comments, and forced demand of sharing pictures/videos online, etc. Sometimes, children may also be lured to meet the stalker offline and thus, may be at risk of sexual assault, child trafficking, etc.

2. **Financial Harms:** This may include financial frauds. Such frauds may occur while doing financial transactions on e-commerce, gaming and other entertainment websites. This may also include instances where children addicted to specific services, such as gaming apps, end up making financial transactions of massive amounts.

3. **Addiction:** Easy access to the digital world also leads to children developing an addiction to social media and online gaming apps. Such addiction severely hampers their overall well-being and may lead to poor sleep, mental health issues and body image concerns which cause disordered eating (OECD, 2018).

4. **Access to Age-Restricted Goods, Services and Content** (Nash, O'Connell, Zevenbergen, & Mishkin, 2013):
   a. Goods: Alcohol, tobacco, etc.
   b. Services: Gambling; websites/apps allow users to provide adult service where children are vulnerable to be sex-groomed.
   c. Content: Adult film, gaming, pornographic content, etc.

5. **Radicalisation:** Social media is also a place where children may easily be radicalised on religious or ethnic lines.

6. **Personal Data Processing and Advertisement Targeting:** Children's personal data collected by data fiduciaries like social media intermediaries could be

processed and used for marketing and targeted sale of products. The data collected may further be shared or sold to third parties. Thus, there is a severe risk of invasion of the privacy of children. Further, even if children are providing their consent for processing their data, such consent may be uninformed as many of them may not fully understand the concept of data privacy. Thus, the principles of data minimisation and purpose limitation need to be emphasised upon.

In the light of the above-mentioned online harms and to ensure the safety and well-being of children, it is vital to create and provide a safer online environment for children. In this regard, recently, there have been several global developments like the introduction of the Kids Internet Design and Safety Act and the Children and Teens' Online Privacy Protection Act in the United States Congress[1], the United Kingdom's (UK's) Information Commissioner issuing Age Appropriate Design as code of practice for online services[2] as well as the UK parliament contemplating on the Online Harms Bill.[3] Further, the Global Privacy Assembly also adopted a Resolution on Children's Digital Rights.[4] The Chinese government has also put in restriction on online gaming apps for children.[5] Given these developments, several data fiduciaries are already are being criticised[6] and recent revelations have also shown that social media can be dangerous for teen users.[7] Since these developments, some of them have started adopting measures like restricting targeted advertisements at minors,[8] and giving more agency to young users.[9] However, for a having robust protective framework from the stated online harms, across the global policy landscape, age verification has been understood as an important tool which will make data fiduciaries adopt practices to provide a children a safer internet. Further, in addition to helping data fiduciaries ensure the safety of children from online harm and protecting their personal data, having age verification will also enable them to tailor information and content for particular age groups. For instance, social media platforms may deploy child protection tools with respect to the content children can view, or search engines may restrict showing alcohol or tobacco ads, or an online gaming company may allow access to its service only for a particular amount of time (Nash, O'Connell, Zevenbergen, & Mishkin, 2013). While age verification does not ensure protection of all children from all online harms, it offers a part of the solution which may be leveraged to provide children a safer internet environment.

Therefore, for this purpose, a legislation which mandates age verification in order to protect personal data of children is important. In India, developments such as the Rajya Sabha Ad-hoc Committee Report on Pornography on Social Media and its Effect on Children and the Society as a whole[10], the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 as well as the Personal Data Protection Bill (PDPB) 2019 aim at highlighting the online harms faced by children and protecting them from the same. Specifically, Section 16 of the PDPB 2019 has provisions for age verification which will help in protecting children's data.[11]

16. (*1*) Every data fiduciary shall process the personal data of a child in such a manner that protects the rights of and is in the best interests of the child.

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

As per the PDPB, data fiduciaries need to obtain the consent of the parents or guardians for processing children's data. Since self-declaration is prone to misrepresentation and false declarations, the bill also mandates data fiduciaries to verify the user's age before processing any personal data.[12]

The bill states that several factors will be taken into account while deciding the method of age verification. These include the volume of data being processed, the proportion of such personal data likely to be that of a child and the possibility of harm arising out of the processing of personal data.[13]

The Central Government may also issue further delegated legislation in this regard.[14] Further, the bill empowers the proposed Data Protection Authority (DPA) to provide Codes of Practice (CoP) as specific regulations to specify the age verification methodology to be used.[15]

> **94.** (1) The Authority may, by notification, make regulations consistent with this Act and the rules made thereunder to carry out the provisions of this Act.
>
> (2) In particular and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:— (*e*) the manner of obtaining the consent of the parent or guardian of a child under sub-section (*2*), the manner of verification of the age of a child under sub-section (*3*), application of the provision in modified form to data fiduciaries offering counselling or child protection services under sub-section (*6*) of section 16;

In light of this, it is important to understand the various age verification alternatives available so that an appropriate method or a combination of methods can be utilised by data fiduciaries based upon the different context such as the socio-economic status of users, their awareness level etc. The methods should be: (1) privacy-conscious and respect data minimisation; (2) user-friendly and do not overburden the data fiduciaries; (3) do not limit children's opportunities provided by the Internet (Macenaite & Kosta, 2017). The idea is to establish an age assurance system that is robust in protecting children from online harm, respects the privacy of individuals, is easy for a child to use, is accurate, accessible and has the feasibility of large-scale adoption.

While certain methods verify age, others can be used to estimate the age or the age group of a user. Age verification and estimation are collectively termed age assurance (5RightsFoundation, 2021). The following section discusses such technologies in detail.

Assessment of Key Age Assurance Methods

There are different kinds of age assurance methods. One of the methods is to establish the requirement of having an online identifier that is linked to a government identity proof. Other methods include utilising technology like using artificial intelligence and machine learning tools for estimating the age of a user. A comparison should be made to highlight the unique features of each of them while also analysing the plausible impacts on users, especially their privacy.

Nash et al. (2013) state that attributes-based age verification which uses the assigned attributes like name, nationality etc. or related attributes like work details etc., of an individual can address privacy concerns and is a flexible model. There are three different types of attributes (Nash, O'Connell, Zevenbergen, & Mishkin, 2013):

1. **Immutable attributes:** These attributes cannot change, i.e.,

biological parents, date and place of birth, identifiable biometrics (iris, fingerprint), etc.

2. **Assigned attributes:** These are recorded biographical information i.e., name, signature, gender, nationality etc.
3. **Related attributes:** These result from interaction with the world, i.e., work details, address, skills, financial/government interaction, internet use, etc.

A good framework to assess the utilisation of these attributes for age assurance is to understand what the method is setting out to achieve. It can be classified into three types. (5RightsFoundation, 2021)

1. **Identification Methods (ID):** Obtain the true identity of the user.
2. **Age Verification Methods (AV):** Exact age without user identification.
3. **Age Estimation Methods (AE):** Estimating the age of the user.

Therefore, while utilising certain attributes may lead to identification, others may be used for age verification or age estimation. Nash et al. (2013) suggest utilising non-identifiable attributes to carry out a transaction to preserve the user's privacy. Further, new age verification and age estimation technologies discussed in the next section can minimise data collection and thus respect user privacy.

However, all these methods have their utility, advantages and disadvantages. The comparison has been made based on a set of parameters mentioned below (5RightsFoundation, 2021):

1. Privacy-friendliness: Principles of data minimisation and purpose limitation must be upheld and the user should not be identified.
2. Ease for the child to use: An easier method would not put undue burden on children.
3. Accessibility and inclusivity: The methods should be accessible to children while taking into account the developmental capacity, the socio-economic status, and access to parents etc.
4. Level of accuracy: It is important that the method used for age verification can accurately identify the age of the user.
5. Feasibility of large-scale adoption: Given the state of awareness about safely accessing the internet, digital infrastructure and connectivity in India, etc., many methods may not be feasible for adoption at large scale and if adopted, may lead to exclusion. Hence, feasibility of large scale adoption needs to be looked at.

While privacy friendliness, ease for the child to use and accessibility and inclusivity are considered as parameters to capture the young consumers' interest, accuracy and feasibility of adoption are considered as parameters to capture the challenges and perspectives of data fiduciaries that adhere to the age verification norms.

The table in the next section compares different currently available age assurance methods based on the above-stated parameters. The comparison will help understand how these methods can be used by data fiduciaries so that they can verify the age of online users and comply with provisions of the PDPB 2019.

Comparing Age Assurance Technologies: A Tabular Presentation

Various technologies for assuring age have been compared based on the identified parameters and the same is presented in the table below. The aim of presenting this tabular analysis is not to judge the best technique available but to bridge the information gap and provide insights so that a better policy decision can be made regarding age assurance.

S. No.	Method[1]	Type of Method	Attributes Used	Parameters					Remarks
				Privacy-Friendly	Easy for children to use	Accessible & Inclusive	Provides Accuracy	Feasible for Adoption	
1	Self-Verification	Identification (ID)	None	Yes: No identifiable attributed shared.	Yes: Only requires clicking a checkbox.	Yes: Ensures accessibility to most users.	No: Relies on the honesty of the user and, therefore, is prone to be inaccurate.	Yes: Already being used. Minimal additional costs for providers and end-users.	Relies on the honesty of individual users. May exclude persons with disabilities.
2.1	Hardline identification by uploading a scanned copy of a physical government ID proof or by receiving an OTP of Aadhar verification	ID	Government ID Proof (Related attribute)	No: User is identified. Goes against the principle of Data Minimisation and Anonymity.	No: Need to upload an ID proof.	No: Most citizens may have a government ID. However, not everyone may be willing to share their ID proof.	No: Reliable and trustworthy data source but children may upload ID proofs of adults like their parents or access their OTP.	Yes: Has been adopted earlier in sectors like stock trading.	Manual checking required. User may also upload a false ID proof.

[1] Please refer the annexure for a detailed explanation of each of the stated technologies and additional details of their performance against the stated parameters.

S. No.	Method[1]	Type of Method	Attributes Used	Parameters					Remarks
				Privacy-Friendly	Easy for children to use	Accessible & Inclusive	Provides Accuracy	Feasible for Adoption	
2.2	Hardline identification by using government e-ID and providing biometrics. (Example: e-KYC through Aadhaar Card)	ID	Government ID Proof, Biometrics (Immutable and related attributes)	No: User is identified. Goes against the principle of Data Minimisation and Anonymity.	No: e-KYC is required.	Yes: Most citizens have Aadhaar Card.	Yes: Reliable and trustworthy data source.	No: User needs to visit a kiosk centre for e-KYC. Good for one-time verification. Costly to create architecture for e-verification on users' devices using Aadhaar data	May increase compliance cost for data fiduciaries
3	Using bank-related documents like credit or debit cards	ID/ Age Verification (AV)	Banking Details/ Financial Details (Related attribute)	No: Users have to share credit/ debit details. Goes against the principle of Data Minimisation and Anonymity.	Yes: Most children do not have credit/debit cards and will not require entering details	No: Digital Divide in India: low accessibility. Fraudsters increasingly have access to credit data due to data breaches	No: Does not verify if the person providing the information is an actual person or not. Less reliable with false positives when common names are used	No: Digital Divide in India and hence, not highly feasible. People with thin credit profiles or people who very rarely use financial services may be excluded.	

S. No.	Method[1]	Type of Method	Attributes Used	Parameters					Remarks
				Privacy-Friendly	Easy for children to use	Accessible & Inclusive	Provides Accuracy	Feasible for Adoption	
4	Third-Party e-ID card Issuers. The e-ID is verified using a Government ID proof and can be used by other data fiduciaries	AV	Government ID Proof and third party e-ID (Related attribute)	No: User is identified by a third party. Provides some degree of privacy but against anonymity.	Yes: Easy to use. Needs one-time verification.	Yes: Requires users to create one-time e-ID.	Yes: Reliable and trustworthy data source, hence accurate.	Yes: Has been in use in other countries for age verification.[16] Third party private players may set up such a service in India.	User identity revealed to only one third-party e-ID card issuer. Other data fiduciaries can use it for age verification (Refer Annexure)
5.1.1	Hardline identification using iris scan stored in a government database or with a third-party provider	ID	Biometrics (Immutable attribute)	No: User is identified. Against Data Minimisation and Anonymity.	No: Requires Iris scanning.	No: Low accessibility of iris scanner.	Yes: Reliable and trustworthy data source, hence accurate.	No: Additional hardware may be required. Creating a new de-centralised database with multiple third-parties is difficult	
5.1.2	Hardline identification using fingerprint stored in government database (similar to 2.2) or with a	ID	Biometrics (Immutable attribute)	No: User is identified. Against Data Minimisation and Anonymity.	Yes: Fingerprint can be easily used	Yes: Smartphone devices have a fingerprint scanner	Yes: Reliable and trustworthy data source, hence accurate.	Yes: Additional hardware is not required. A new de-centralised database with multiple third-	For third-party providers, the creation of a new database is required, which contains a fingerprint

S. No.	Method[1]	Type of Method	Attributes Used	Parameters					Remarks
				Privacy-Friendly	Easy for children to use	Accessible & Inclusive	Provides Accuracy	Feasible for Adoption	
	third-party provider							parties can be created	
5.2.1	Facial Features ID: A centralised database like Aadhaar needs to be created	ID	Biometrics (Immutable attribute)	No: User is identified. Against Data Minimisation and Anonymity.	Yes: Only requires scanning of the face	No: Requires creation of a new central database.	Yes: Technology for facial recognition exists.	Yes: Additional hardware not required. A new database can be created	
5.2.2	Facial Features AV: A third party may conduct age verification	AV	Biometrics (Immutable attribute)	No: Data processing on servers of data fiduciary	Yes: Only requires scanning of the face	No: Requires creation of a new central database	Yes: Technology for age verification through facial recognition exists	Yes: Additional hardware not required. A new database can be created	
5.2.3	Facial Features AE: Machine learning and AI algorithms used to estimate the age.	Age Estimation (AE)	Biometrics (Immutable attribute)	No: Data processing on servers of data fiduciary	Yes: Only requires scanning of the face	Yes: Only requires users to scan their face using a smartphone	Yes: Technology for age-group estimation exists.	Yes: Additional hardware and a new database are not required	
5.3	Level of fingerprint development	AE	Biometrics (Immutable attribute)	No: Data processing on servers of data fiduciary	Yes: Fingerprint can be easily used.	Yes: Only requires users to scan their fingerprint using a smartphone.	Yes: Technology for age-group estimation exists	Yes: Additional hardware and a new database not required	
6.1	AI & Data Processing on	AE	Biometrics (Immutable	Yes: Data Processing	Yes: Facial Scan/	Yes: Only requires users	Yes: Dependent on training the	Yes: Has been tried in other	

S. No.	Method[1]	Type of Method	Attributes Used	Parameters					Remarks
				Privacy-Friendly	Easy for children to use	Accessible & Inclusive	Provides Accuracy	Feasible for Adoption	
	Device using facial imaging and level of fingerprint development (analysis on device)		attribute)	on user's device	Fingerprint can be easily used	to scan face/ fingerprint using a smartphone	neural networks	countries[17]	
6.2	User's physical movements or interactions with a device (analysis on the device)	AE	Touch and Motion data (Related attribute)	Yes: Data Processing on user's device	Yes: Such data can easily be obtained	Yes: Only requires users to use their smartphone	Yes: Dependent on training the neural networks	Yes: Such data can easily be processed	
6.3	Static long-term physical and biometric characteristics of the user (analysis on the device)	AE	Long-term static physical and biometrics characters (Immutable)	Yes: Data Processing on user's device	Yes: Such data can easily be obtained	Yes: Only requires users to use their smartphone	Yes: Dependent on training the neural networks	Yes: Such data can easily be processed	
7	Semantic Analysis & Knowledge-Based Authentication (KBA)	AE	User Behaviour (Related attribute)	Yes: Personal data not shared. Data processing on user's device	Yes: Only requires answering texts etc.	No: Doesn't require additional hardware. Many children in India don't have access to quality education, may result in	No: Not fully accurate as still in infancy stage of development. Moreover, persons have different levels of maturity.	Yes: Low-cost adoption.	-Problematic in multilingual culture like India. -Good as supplement to self-certified information and gives an additional verification level. - Easy to discover

S. No.	Method[1]	Type of Method	Attributes Used	Parameters					Remarks
				Privacy-Friendly	Easy for children to use	Accessible & Inclusive	Provides Accuracy	Feasible for Adoption	
						exclusion			answers.
8	Parental Control for Device.	AV	Parental Control (No attribute of child used)	No: Parents are required to reveal details about their child to the data fiduciary. Privacy of parents also not ensured.	Yes: Only requires parental monitoring.	Yes: Parents may choose the level of monitoring while giving an internet-enabled device to their child.	Yes: If parents are providing consent, data fiduciaries can be confident in providing service to a child	No: Making parents aware of the process of providing consent may not infeasible. Only operating system providers will provide the service.	Not all parents are digital literates to use the method. Subversion for illegitimate purposes like monitoring others like one's spouse etc.

The above analysis shows that there are several methods for age assurance. While some of these methods do not provide the adequate privacy, others are good at ensuring privacy as well as stand well against all the mentioned parameters. Therefore, a single method or a combination of methods may be used for age assurance. The annexure provides a detailed understanding of each of the above mentioned technological methods.

Conclusion and Way Forward

Age assurance can be used to provide children a safe space on the internet. In this Briefing Paper, different methods of age assurance have been compared based upon specific parameters like privacy, ease of use for children, accessibility and inclusivity, accuracy and feasibility. The DPA may utilise the stated parameters as design principles for issuing Codes of Practice for the manner of age verification. For providing children a safer online environment, several other factors also need to be considered. These are mentioned below:

- In India, different legislations have different definitions of persons between the ages group 0 to 18. While some recognise persons under 14 years of age to be children and persons between 14 to 18 years of age to be adolescents, others recognise anyone under 18 to be a child (Sikda, 2012). These categorisations are based on the level of risk a child may face. The PDPB defines any person younger than 18 years of age to be a child[18] and mandates parental consent before processing any personal data belonging to a child. This approach seems to equate maturity as well as the privacy of a child, adolescent, and a young person and may restrict young users from the opportunities internet services can provide. It is important to understand the capability of children in dealing with online harms. While some children may have the maturity to understand certain online risks, others may not. With changing cultural and regional contexts, the maturity level of children of the same age group may also vary. Thus, the imposition of a single legal age threshold may disproportionately restrict the rights and opportunities of the child. A possible solution is to have graded age groups where regulations are specified as per the age group of children. Therefore, it might be worth considering adoption of different age limits (Macenaite & Kosta, 2017). Children and young users should not be excluded from the opportunities the internet provides and a one-size fits all approach should be avoided.
- Further, though children are digital natives and maybe more capacitated than their parents in utilising the internet, they may perhaps be less likely to understand the meaning of privacy. Thus, there is a need to have more transparent and better designed privacy notices for children. Further, striking a balance between ensuring privacy to children from their parents and giving control to parents so that their children are not exposed to online harm is important.
- The acceptability of the different age assurance methods among children and parents must also be considered. Further, data fiduciaries should also be given a choice in this regard. As per the feasibility and the principles laid out by the DPA, a combination of methods may be utilised.

Finding solutions to these issues requires a more subjective understanding and views of the most critical stakeholders, i.e., children and parents, must be taken into account. Their inputs on the level of restriction required for accessing digital services, privacy concerns, parental consent mechanisms, age assurance technologies, etc. need to be considered. Therefore, the DPA while issuing Codes of Practice should take into account the views of both parents and children. In this regard, CUTS International is conducting a survey administered to users aged 16 and 17 years and parents to obtain deeper insights.

Annexure

Method 1: Self Confirmation/Declaration of Age [Method Type: Age Verification]

This method relies on users making a statement of self-confirmation of them being above a particular age group. It is one of the most used methods by social networking websites. They have an age limit for using the service: generally, 13 years. WhatsApp has changed the age limit to 16 in the European Union region to respond to the EU GDPR (General Data Protection Regulation) (Pasquale & Zippo, 2020). These websites/apps do not allow users to register by entering an age below the stated age limit. However, it relies on the honesty of the user and assumes that users will be truthful. The method is not foolproof, as anyone can tick the confirmation box and report a falsified age, thus misrepresenting information (Pasquale & Zippo, 2020).

Therefore, though the age verification method best protects the privacy and is cost-effective, it is not robust as a user can circumvent the age verification mechanisms by entering a false age.

Method 2: Hardline Identification using Government ID [Method Type: Identification]

Hardline identification means that the user has to provide a government ID proof such as passport, Aadhaar card, PAN card etc., which can be used to identify the user. The idea here is to utilise an existing centralised large database to verify a person's identity through government-issued ID proof. Since this method identifies a person, it offers a high level of accuracy. The data fiduciary/processor collects all personally identifiable attributes. It is cost-effective and easy to scale.

Governments across the world have come up with e-ID cards. It is a government-approved ID card that gives an electronic identity to a citizen. The e-ID card can be used for identification, signing electronic documents and using public services. In India, Aadhaar card is an example of e-ID card.

In countries like Denmark and Spain, different examples of good practice whereby the regulator allows gambling operators' access to the electronic identity database to cross-check asserted identity details are present (Nash, O'Connell, Zevenbergen, & Mishkin, 2013). Therefore, either the data fiduciaries can ask the users to upload physical copies of their identity proofs or perform a check through the e-ID card.

Uploading a copy of government ID proof

For using certain services like financial transactions in the securities market, crypto-currency trading etc. identification is required. Stock trading platforms need to carry out the process mandated by the Reserve Bank of India (RBI).

In most cases, users are requested by data fiduciaries to submit a selfie holding their government identity proof. Stock trading and crypto-currency trading platforms complete the KYC norms by asking users to submit their government ID proof and a selfie holding the same ID proof in their hands.[19]

In Germany, an attempt to use an age verification system based on the identity card or passport number coupled with the postal code of the city of its issuance has been declared by the German Federal Supreme Court as an effective barrier to prevent minors from accessing online age-restricted content.

However, such a practice does not respect user privacy (Macenaite & Kosta, 2017).

Using a government-issued e-ID card

One of the examples of this method currently being used in India is the e-KYC (e-Know Your Customer) process which identifies a user based upon the centralised stored database Aadhaar. The Aadhaar biometric-based e-KYC process is already being used in India by telecom operators and fin-tech data fiduciaries who operate payment banks and provide payment wallets (like PayTM, Airtel Money etc.).

This process requires users to scan their fingerprints at select stores which offer e-KYC services. Belgium's e-ID card has been said to be ineffective as it is too intrusive and disproportionate due to the use of the National Registry identification number embedded in the e-ID card revealing the date of birth and the gender of the child (Macenaite & Kosta, 2017).

It is important to note that the internet offers a host of services that may not require financial transactions to be made and therefore, identification may not be required at all. To comply with the PDPB, only age verification is required so that data fiduciaries can avoid children's access to inappropriate content & providing them with a safe online experience. Further, even if financial transactions are to be conducted in industries like e-commerce, data fiduciaries certainly do not require knowing a user's identity for selling all products.[20]

The whole process goes against the principle of data minimisation. As the user is identified, data fiduciaries and the data processors can use the data in any manner possible, as has been highlighted before. While it may protect children from online harm, it does not protect a user's privacy but infringes it.

Further, the method is not perfect as there have been cases reported where adult online services like Only Fans have failed to stop children from accessing their services. Children as young as 13 have utilised government ID proofs of adults to access these services (Feehan, 2021). Moreover, a process like e-KYC cannot be mandated to access every service (website/app) on the internet.

Therefore, this identification method may be the least preferred and only be adopted for industries that necessarily need identification, as mentioned earlier.

Method 3: Age Verification/Identification using non-Government and Existing Online Database [Method Type: Age Verification/ Identification]

This method leverages existing online systems having a range of publicly accessible data. An example of this is present in the UK. A study by Nash et al. (2013) finds that the UK has a good system of age verification for online gambling wherein data aggregators and credit reference agencies cover 85-90 per cent of the UK adult population, offering one approach to identity and age verification not reliant upon a single central identity database.

Here, credit card holders are considered to have attained the age of 18 and are allowed to enter the online gambling world. Combining other methods of authentication can improve success rates but can be cumbersome (Nash, O'Connell, Zevenbergen, & Mishkin, 2013).

Unlike the government ID proof identification method, this method uses a decentralised system and provides a better level of privacy. Here, the method may be used for identification or age verification, depending on the system being set up. It may also be cost-effective for data fiduciaries/ processors.

However, this method is good only for industries where financial transactions happen, as discussed in the previous method. For utilising services like social media and online entertainment services, the data fiduciary does not need to know the user's identity. Even if the method is being used just for age verification, the data fiduciary will have access to the credit/debit card details, which is not desirable as these are sensitive personal details. Data minimisation is still absent, and the data fiduciaries can utilise the information received for targeting advertisements etc., to children.

Moreover, the principle of purpose limitation sees a gross violation here. The reliance on data initially collected for purposes other than age verification goes against one of the fundamental privacy principles. The same has been accepted as a salient feature in the PDBP.[21] Therefore, such a method can be termed unfair and may lead to unlawful processing of personal data.

Further, the method is far from being accurate. Though a credit card is given to over 18s in the UK, there are clear circumstances where under-18s can obtain and/or use such credit cards. An adult can present an under-18 with a legally held credit card in anyone else's name where an over-18 pays the bill. There have been cases reported where people below the age of 18 have used a credit card to access services. In this case, using a credit card cannot be used robustly as a proxy for age, although the retailer has no mechanism to detect if this is the case.

Furthermore, the feasibility of using this method is also weak. The use of banking data for age verification is not a good idea as banks say that data is asked at opening an account but not stored in an easily queried way. Finally, there exists a significant digital divide in India. A large proportion of the population does not either own or regularly operate credit/debit cards. Therefore, the method cannot be used as a universal method for age verification.

Method 4: Age Verification/Identification using third party non-government e-ID card [Method Type: Age Verification/ Identification]

This method does not let all data fiduciaries get access to personal identifiable information like name, date of birth, etc. The real identity remains hidden; third-party non-government e-ID card issuers are present in some countries who verify the identity of a user by authenticating it against a government-issued ID card.[22]

Therefore, the e-ID card issuer becomes an intermediary between the user and the data fiduciary for age verification. Users may also choose to use the e-ID card for identification purposes. These services generally remain free for users and only charge a small amount from businesses that use their service.[23] Since businesses need to comply with the age verification laws, they are willing to utilise the services offered by such e-ID card issuers.

This method has observed widespread adoption as it is easy to use, accessible, and can be adopted at a large scale. However, the method still requires the third-party e-ID card issuer company to verify an individual's identity using government ID proof. Therefore, the privacy of an individual is compromised.

Method 5: Utilising Biometrics [Method Type: Identification/Age Verification]

Biometrics can also be utilised for identification for age verification. Different kinds of biometrics may be used and they are listed below in the table along with their pros and cons based upon the parameters of comparison identified earlier.

Biometric	Pros	Cons
Speech	• Moderate accuracy • No additional hardware required	• Easy to circumvent • Low reliability for children aged 11-13
Finger-print	• High accuracy	• Requires fingerprint reader • Low anonymity
Facial Features	• High accuracy • No additional hardware required	• Easy to circumvent
Iris	• Low accuracy	• Requires Iris Reader • Low Anonymity

There are several ways in which biometrics can be utilised for age estimation or identification. These are listed below:

Hard-line Identification/Age Verification using Unique Biometrics [Method Type: Identification/Age Verification]

Fingerprint and iris are unique biometrics and cannot be the same for any two individuals. Therefore, as discussed earlier in Method 1 of self-verification, a hardline identification can happen through biometric verification. In this method, there needs to be a centralised database that stores the biometrics of individuals.

In India's case, Aadhaar is used for this purpose. However, as discussed earlier, this process goes against the principle of preserving a user's privacy and should be used only in limited industries that require such identification. Moreover, the implementation of this requires users to have fingerprint and iris scanners and therefore, the feasibility of implementation at a large scale remains very low.

Similar to method 4 where a third party became an e-ID card issuer, a third-party company may store biometric details of users and act as an intermediary between the user and the data fiduciary for age verification. In this case, a de-centralised system is adopted rather than having a centralised database stored with the government. However, similar to method 4, the method only provides limited anonymity and privacy and, therefore, is not preferred.

Further, biometrics that do not require additional hardware like speech recognition features cannot be used for this purpose because they are easy to circumvent. Facial recognition is covered in the next section.

Facial Features [Method Type: Identification/Age Verification/Age Estimation]

Facial features may be used for identification, age verification as well as age estimation.

- **Identification:** Here, a centralised database will have to be maintained. This is against data minimisation and also does not preserve the privacy of the user. The only upside here is that it requires no additional hardware.
- **Age Verification:** A third party, similar to method 4, may conduct age verification.
- **Age Estimation:** Machine learning and AI algorithms may be used to estimate the age of users. Details are mentioned below.

One method for age estimation using facial features may be to create a digital ID. If the prediction tells that the age is above 25, the user is granted access. If the prediction is 18-24 years, the user is asked to verify using a government ID proof. If the prediction is below 18 years, users' are restricted from accessing inappropriate content.[24]

However, the processing of data for age estimation here happens on the cloud (online). This means that a photo with the user's face is recorded and sent to the third-party servers to process and figure out the age. While the third-party company may claim that it does not store the user's facial images, the data still travels to its servers, thus compromising privacy.

Moreover, there are several other problems with using facial features for age estimation. One's lifestyle affects how the face ages. Faces of individuals of the same age but with different lifestyles will appear different. Exposure to drug and psychological stress affects skin texture and colour making skin complexion spotted and blemished. Factors affecting perceived facial aging include diet, genetic makeup, ethnicity, skin infections, and cosmetics. General exposure to wind and arid air influence facial aging. An arid environment and wind dehydrate the skin leading to wrinkle formation (Angulu, Tapamo, & Adewumi, 2018).

Further, some facial expressions like smiling, frowning, surprise, and laughing may introduce wrinkle-like lines on some regions of the face. These wrinkle-like lines may be registered as wrinkles during age estimation hence having an impact on age estimation performance (Angulu, Tapamo, & Adewumi, 2018).

Level of Development of Fingerprint [Method Type: Age Estimation]

Age estimation can be done by analysing the level of development of the user's fingerprint using artificial intelligence. The method can determine the user's age group with high levels of accuracy (Saxena, Sharma, & Chaurasiya, 2015). However, here too, since the analysis happens on the servers of the data fiduciaries, data privacy again remains compromised.

Method 6: Local Device Based implementation of Artificial Intelligence and Processing of Data for Age Estimation [Method Type: Age Estimation]

Almost all methods listed before this method require users to either disclose their identity to one or the other entity and/or submit their personal identifiable information, including biometrics. Even if the user is not submitting such details and age estimation is being carried out using facial features or fingerprint development analysis, the data processing still happens on cloud servers of the data processors.

Therefore, to truly preserve privacy, methods should be developed where storing and processing of users' data happens so that their personal identity is not disclosed to any entity. This can be done by utilising EDGE computing where the storing and processing of data happens on users' devices and their privacy is well preserved. Data fiduciaries can utilise a software development kit to incorporate an age estimation mechanism that leverages machine learning.[25] For easier integration, an API may be created which can be integrated with any app.

EDGE computing techniques and artificial intelligence may be used with different kinds of data. These are mentioned below:

- Device-level verification through artificial intelligence using facial imaging and level of development of fingerprint

- Data derived by user's physical movements or interactions with a device (touch data and motion analysis on a device)

  Data derived from static long-term physical and biometric characteristics of the user

Method 7: Semantic Analysis & Knowledge-based Authentication [Method Type: Age Estimation]

Another method that can be used for age estimation is semantic analysis. Semantic analysis means analysing text written by a user and estimating age using the same. The age estimation software can put forward some questions to users and ask them to respond. This method is also capable of preserving the privacy of the user.

Technology to analyse social media profile or behaviour for determining age range through data generated by users while using an app, service, or platform may be used.

However, the method may not be very reliable as it requires a high amount of training before desired accuracy levels are reached. It is also prone to be circumvented as users might obtain the questions through online search.

Method 8: Parental Control [Method Type: Age Verification]

In this method, parents may put in parental control while giving their child a smartphone or an internet-enabled device. This will enable them to control what their children are using the device for. Certain data fiduciaries are already providing this.[26]

It enables parents to monitor and control their children's use of android/iOS smartphones. Features include parents being able to view the screen time of their children etc. However, the product may not block inappropriate content and therefore, children may still be vulnerable to being exposed to harmful content.[27]

Another critical concern here is that parents from different socio-economic backgrounds might understand technology and the internet differently. While some may understand the risks of online harm better, others may not. Therefore, the layer of parental control and permission is also flimsy. The fundamental problem is that children know how to use technology like VPNs but are not responsible enough. Parents are responsible but do not know how to use technology.

Further, in the name of protecting children's privacy, parents may be required to divulge more personal data about their children. Some technologies might give parents a false sense of their child's security online. Furthermore, there may be a subversion of the technology for illegitimate purposes, such as monitoring one's spouse.

References

5RightsFoundation. (2021, March). *But how do they know it is a child? Age Assurance in the Digital World.* Retrieved August 04, 2021, from 5Rights Foundation: https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf

Angulu, R., Tapamo, J. R., & Adewumi, A. O. (2018). *Age estimation via face images: a survey.* Retrieved August 05, 2021, from EURASIP Journal on Image and Video: https://jivp-eurasipjournals.springeropen.com/track/pdf/10.1186/s13640-018-0278-6.pdf

Bekalu, M. A., McCloud, R. F., & Viswanath, K. (2019). Association of Social Media Use With Social Well-Being, Positive Mental Health, and Self-Rated Health: Disentangling Routine Use From Emotional Connection to Use. *Health Education and Behavior*, https://doi.org/10.1177/1090198119863768.

Castellacci, F., & Tveito, V. (2018). Internet use and well-being: A survey and a theoretical framework. *Research Policy, Elsevier*, vol. 47(1), pages 308-325.

Feehan, K. (2021, May 27). *Children use fake IDs to sell X-rated videos on OnlyFans.* Retrieved August 04, 2021, from The Daily Mail Online: https://www.dailymail.co.uk/news/article-9624827/Girls-young-thirteen-tricking-OnlyFans-age-verification-share-explicit-content.html

Jain, O., Gupta, M., Satam, S., & Panda, S. (2020, August–December). *Has the COVID-19 pandemic affected the susceptibility to cyberbullying in India?* Retrieved August 10, 2021, from Computers in Human Behavior Reports: https://doi.org/10.1016/j.chbr.2020.100029

Macenaite, M., & Kosta, E. (2017, May 10). *Consent for processing children's personal data in the EU: following in US footsteps?* Retrieved August 5, 2021, from Information & Communications Technology Law: https://doi.org/10.1080/13600834.2017.1321096

Nash, V., O'Connell, R., Zevenbergen, B., & Mishkin, A. (2013, December). *Effective age verification techniques: Lessons to be learnt from the online gambling industry.* Retrieved July 2021, from Oxford Internet Institute: https://www.oii.ox.ac.uk/archive/downloads/publications/Effective-Age-Verification-Techniques.pdf

OECD. (2018). *Children & Young People's Mental Health in the Digital Age: Shaping the Future.* Retrieved August 10, 2021, from https://www.oecd.org/els/health-systems/Children-and-Young-People-Mental-Health-in-the-Digital-Age.pdf

Pasquale, L., & Zippo, P. (2020, May 21). *A Review of Age Verification Mechanism for 10 Social Media Apps.* Retrieved August 04, 2021, from CyberSafe Ireland: http://hdl.handle.net/10197/11991

Sarkar, D. (2020, May 20). *Swiggy starts home delivery of alcohol with a new verification feature.* Retrieved August 05, 2021, from The Times of India: https://timesofindia.indiatimes.com/gadgets-news/siwggy-starts-home-delivery-of-alcohol-with-new-verification-feature/articleshow/75864041.cms

Saxena, A. K., Sharma, S., & Chaurasiya, V. K. (2015). Neural Network-based Human Age-group Estimation in Curvelet Domain. *Procedia Computer Science*, doi:10.1016/j.procs.2015.06.092.

Sikda, S. (2012, June 15). *Who is a child?* Retrieved July 30, 2021, from The Hindu: https://www.thehindu.com/news/national/who-is-a-child/article3528624.ece

UNICEF. (2020, April 14). *Children at increased risk of harm online during global COVID-19 pandemic.* Retrieved July 29, 2021, from UNICEF: https://www.unicef.org/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic

Endnotes

[1] https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2021/11/kids-act-bill--nov-2021.pdf and https://www.markey.senate.gov/imo/media/doc/children_and_teens_online_privacy_protection_act.pdf

[2] Age Appropriate Design Code by UK's Information Commissioner: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/

[3] Research Briefing on Regulating online harms, UK Parliament House of Commons: https://commonslibrary.parliament.uk/research-briefings/cbp-8743/

[4] 43rd Closed Session of the Global Privacy Assembly, Adopted Resolution on children's digital rights, October 2021: https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Childrens-Digital-Rights-Final-Adopted.pdf

[5] China has restricted children's usage of online gaming apps: https://www.cnbc.com/2021/08/30/china-to-ban-kids-from-playing-online-games-for-more-than-three-hours-per-week.html

[6] https://www.trtworld.com/magazine/snapchat-tiktok-and-youtube-under-fire-over-child-safety-51090

[7] https://www.standard.co.uk/news/uk/instagram-safety-mps-people-tiktok-b962435.html

[8] https://www.livemint.com/companies/news/google-follows-facebook-apple-with-new-child-safety-tools-for-its-apps-11628662981729.html

[9] https://news.bloomberglaw.com/privacy-and-data-security/social-platforms-feel-policy-pressure-on-teen-privacy-controls and https://www.trtworld.com/magazine/snapchat-tiktok-and-youtube-under-fire-over-child-safety-51090

[10] Report of the Adhoc Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and its Effect on Children and Society as a whole. The report is accessible at: https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/71/140/0_2020_2_16.pdf

[11] The section 16, clause 50(6) (h) and clause 57(2) (b) in the Personal Data Protection Bill 2019 (Bill No. 373 of 2019) contain provisions for protecting children's data. The Bill, currently being deliberated upon by the Joint Parliamentary Committee (JPC), is accessible at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[12] Sub Section (2) of the Section 16 in the Personal Data Protection Bill 2019

[13] Sub Section (3) of the Section 16 in the Personal Data Protection Bill 2019

[14] Clause 93(2) (b) in the Personal Data Protection Bill 2019

[15] Clauses 50(6)(h) and 94(2) (e) in the Personal Data Protection Bill 2019

[16] Yoti (in the UK) and Integrity ID-Direct (in the USA) are two well know third party e-ID issuers. Details accessible at https://www.yoti.com/personal/ and https://integrity.aristotle.com/solutions/#iddirect

[17] https://engagestandards.ieee.org/rs/211-FYL-955/images/IEEESA-Childrens-Data-Governance-Report.pdf

[18] Sub-section (8) of Section 3 in the Personal Data Protection Bill 2019

[19] The same process is used by Swiggy for age verification for alcohol delivery (Sarkar, 2020).

[20] Example: E-commerce giant Amazon has been offering cheaper priced services as a part of their Youth programme. A user aged between 18 and 24 can get the Amazon Prime product at a cheaper price if s/he carries out an age verification process by uploading his/her ID proof which may include Aadhaar card, or other IDs. This is a violation of privacy as under its Privacy Notice; it may use any information of the user for advertisement and also share user information with a third party. Details: https://www.amazon.in/b?ie=UTF8&node=15307611031 and https://www.amazon.in/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ

[21] Clause 4 in the Statement of Objects and Reasons in the Personal Data Protection Bill 2019

[22] Yoti (in the UK) and Integrity ID-Direct (in the USA) are two well know third party e-ID issuers. More details accessible at https://www.yoti.com/personal/ and https://integrity.aristotle.com/solutions/#iddirect

[23] More details accessible at https://www.growthbusiness.co.uk/yoti-the-start-up-phasing-out-id-cards-2551771/

[24] A method utilising this technology has been developed by Yoti. White Paper accessible at: https://www.yoti.com/wp-content/uploads/Yoti_Age_Scan_White_Paper.pdf

[25] Privately SA, a start-up based in Geneva has created such a product. More details are accessible at https://engagestandards.ieee.org/rs/211-FYL-955/images/IEEESA-Childrens-Data-Governance-Report.pdf

[26] Family Link by Google

[27] Google explicitly mentions this in the FAQs section on its product's website. It is accessible at: https://families.google.com/familylink/faq/

This Briefing Paper is authored by Prince Gupta, Research Associate, CUTS International and prepared as a part of the project 'Highlighting Inclusive and Practical Mechanisms to Protect Children's Data.'

This Briefing Paper is published by CUTS Centre for Competition, Investment & Economic Regulation (CUTS CCIER), D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India. Ph: +91.141.228 2821, Fx: +91.141.228 2485, E-mail: c-cier@cuts.org, Web: www.cuts-ccier.org.
Also at Delhi, Calcutta and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland); and Washington DC (USA).

December, 2021