Challenges with Age Verification of Minors in the Digital Economy

Indian Council For Research On International Economic Relations

September 2019

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

"[In the future], the Internet will disappear… you won't even sense it, it will be part of your presence all the time."[1]

The meteoric rise in the use of digital technology has also led to the internet influencing every aspect of modern human life, ranging from economies to societies to cultures.[2] Predictably, this has also meant that the internet has permeated the lives of children and impacted the way they experience the world. It is estimated that youth (ages 15-24) is the most connected age group in the world, and approximately 71% of youth are online in the world compared to 48% of the total global population.[3]

In recent times, it has been observed that children are accessing the internet at increasingly younger ages.[4] Globally, it is estimated that one in three internet users is a child under the age of 18.[5] Prior to examining the role played by children in the digital economy, an important question needs to be answered, when exactly does the Generation Z[6] go online? Some children are considered to have a presence online even before they are born since some parents use social media to announce their pregnancy to friends and family. The market is flooded with more than a thousand apps related to pregnancy, thereby providing parents with multiple options to monitor the growth, development, movement, and even heart rate of their foetuses. Once the child is born, parents also have the option of buying wearable devices embedded with sensors, to capture and send in real time, their child's biometric data such as heart and breathing rate, body position when sleeping, dietary intake, oxygen levels, skin temperature among other things onto the parents' smartphones. Furthermore, some parents share multiple pictures of their child on social media, while some also create a separate social media profile for their children.[7] In one way or another, children may be exposed to the online realm even before they are born, and grow in a world where the digital and internet spaces are native to their lives and not an adopted technology.

As children grow in an environment where digital technology has become ubiquitous, they also realise the crucial role technology can play in furthering their quest for knowledge by simplifying access to a range of enriching content. It also provides them with unlimited opportunities to learn from their peers, socialise[8] and participate in political processes. While educational purposes exist, it is important to note that children also use the internet to express themselves through innumerable forms ranging from social networking, digital storytelling, blogging, citizen journalism to online groups or networks.[9] With the advent of mobile devices such as smartphones and tablets, it has become more challenging to

[1] Eric Schmidt, Executive Chairman, Google, USA, Davos 2015.

[2] UNICEF, 'Children in a Digital World, available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, (last accessed on 29 May, 2019).

[3] UNICEF, 'Children in a Digital World, available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, (last accessed on 29 May, 2019).

[4] UNICEF, 'Children in a Digital World, available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, (last accessed on 29 May, 2019).

[5] Sonia Livingstone *et al.*, 'One in Three: Internet Governance and Children's Rights', Global Commission on Internet Governance Paper Series No. 22 (November 2015), available at: https://www.cigionline.org/sites/default/files/no22_2.pdf, (last accessed on 9 June 2019).

[6] Anyone born from 1997 onward is part of a new generation known as Generation Z, available at https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/, (last accessed on 11 June, 2019).

[7] Deborah Lupton and Ben Williamson, The Datafied Child: The Dataveillance of Children and Implications for Their Rights, 19(5) New Media & Society (2017).

[8] UNICEF, 'Children in a Digital World, available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, (last accessed on 29 May, 2019).

[9] Sonia Livingstone et al., 'One in Three: Internet Governance and Children's Rights', Global Commission on Internet Governance Paper Series No. 22 (November 2015), available at: https://www.cigionline.org/sites/default/files/no22_2.pdf, (last accessed on 9 June 2019).

distinguish between children's 'online' and 'offline' lives. Mobile phones have facilitated a 'bedroom culture', wherein children access the internet in the privacy of their bedrooms, thereby enabling a digital experience which is more personal, more private and less supervised.[10] Furthermore, these mobile devices are especially baby and toddler-friendly since they are intuitive to operate and do not require advanced motor skills. Consequently, pre-schoolers and toddlers are going 'online' as well, since they can navigate touchscreens without the assistance of an adult, unlike laptops or desktops that may be challenging for a toddler to operate independently.[11] Suffice to say, over the past 25 years, new information and communication technologies (ICTs) have transformed the way children interact and participate in society.

Undoubtedly, the digital economy provides children with ample opportunities for growth and self-development. However, it also makes them more vulnerable to harm in the online as well as the offline world.[12] With younger people going online with minimal adult supervision, children are at a higher risk of falling prey to dangers in the online space and making unfortunate choices without fully comprehending the consequences of their actions. Some of these risks include exposure to inappropriate content such as sexual, pornographic and violent images. Websites containing information related to dangerous behaviours such as self-harm, suicide and anorexia, or suffering reputational damage at the hands of cyber bullies or responding to unsafe contact from an adult such as online solicitation or grooming are other examples of potential risks. Constant digital connectivity has made children more accessible to predators through unprotected social media profiles and online game forums, making children even more vulnerable than before.

Moreover, anonymity offered by the internet reduces the risk of identification and prosecution, thereby emboldening offenders. There is no doubt that digital technologies and online spaces have expanded children's horizon through enriching content and provided them with platforms for free expression of ideas. However, it has also enabled far-reaching distribution of hate speech and other harmful content that will have a direct impact on children's world view. Online harm often spills over to offline spaces, since victims of cyberbullying are more likely to use alcohol and drugs, skip school, experience in person bullying, which sometimes leads to suicide or suicidal ideation. Another worrying aspect of constant access is 'digital dependency' and 'screen addiction' amongst children.[13]

While understanding these concerns, it is the age of a user that assumes high significance as a parameter in mediating the risks and benefits of internet use. According to the UNCRC, children's rights are to be addressed "according to the evolving capacity of the child".[14] The internet is predominantly accessible irrespective of age, and while some filters exist, their efficacy is variable. It is incorrect to assume all child users are media-savvy, possess a strong support group and are psychologically resilient. It has been observed that a significant proportion of children lack the age and maturity to fully comprehend the consequences of their behaviour in the digital space.[15] Furthermore, vulnerable and disadvantaged children may be less

[10] UNICEF, 'Children in a Digital World, available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, (last accessed on 29 May, 2019).

[11] Holloway, Donell, Green, Lelia and Livingstone, Sonia (2013) Zero to Eight: Young Children and their Internet Use, EU Kids Online, LSE London, available at: http://eprints.lse.ac.uk/52630/, (last accessed on 12 June, 2019).

[12] UNICEF, 'Children in a Digital World, available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, (last accessed on 29 May, 2019).

[13] UNICEF, 'Children in a Digital World, available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, (last accessed on 29 May, 2019).

[14] Article 5, UNCRC.

[15] Sonia Livingstone et al., 'One in Three: Internet Governance and Children's Rights', Global Commission on Internet Governance Paper Series No. 22 (November 2015), available at: https://www.cigionline.org/sites/default/files/no22_2.pdf, (last accessed on 9 June 2019).

likely to understand online risks, including loss of privacy, thereby becoming more susceptible to harm. It is in this context that regulatory frameworks emerge and attempt to recognise the distinct needs and rights of children.[16]

Children may be exposed to age-restricted or adult-oriented content in the digital space. Consequently, there must be safeguards in place to prevent them from accessing age-restricted services. In order to minimise the risks faced by children in the digital economy, industry, government, and civil society must work together to establish safety principles and practices. One of the tools that may be employed to protect children from harm is developing age-verification systems placing restrictions on children's consumption of adult-oriented services. Through age-verification systems, restrictions may also be placed on individuals with whom children may come in contact.[17] For instance, having a messenger app solely for children and not allowing people beyond a certain age to sign up for the service. In the offline world as well, there are age-restrictions in place for preventing children from potential harm, these include buying age-restricted goods such as alcohol, tobacco, watching movies with adult-rated content and gambling among other things. However, while incorporating appropriate safeguards to prevent children from potential harms of the digital economy, due consideration must also be given to children's rights to freedom of expression and access to information. This concern becomes especially challenging for service providers or product developers because age verification mechanisms introduce a layer of 'friction' in user experience and may affect usage or reduce the pace of adoption.

Through this paper, an attempt has been made to discuss the legal frameworks and age verification requirements in various jurisdictions protecting minors in the digital economy. Thereafter, the requirements proposed in India's Personal Data Protection Bill 2018 will be discussed. This is followed by a section on various age-verification methods currently in place in various parts of the world and its associated implementation challenges. The paper concludes with a snapshot of sectoral variation and recommendations for further policy thinking on this subject.

[16] UNICEF, 'Children in a Digital World, available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, (last accessed on 29 May, 2019).

[17] UNICEF, 'Guidelines for Industry on Child Online Protection', 2015.

2. LEGAL FRAMEWORKS AND AGE VERIFICATION REQUIREMENTS

It is a truism to state that the internet and digital technologies have the wherewithal to empower and benefit children immensely. However, a natural consequence of an increase in children's use of the internet is increased exposure to potential risks of online abuse, exploitation and other harms.[18] Children are perceived to be more vulnerable to risks in the digital space owing to their behavioural characteristics, emotional volatility, and impulsiveness. Consequently, children are seemingly at a higher risk in the digital environment as opposed to adults.[19] The United Nations Human Rights Council passed a resolution in 2017, which noted that violations and abuses of the right to privacy in the digital age may have "particular effects" on certain groups, among them children.[20] Therefore, children represent a vulnerable group of people on the internet and may need specific safeguards concerning their personal information.[21]

Several jurisdictions have acknowledged the need for data protection measures applicable to minors in the digital space. Most regulatory approaches have been based on the principles of parental consent. While approaches may vary, usually countries mandate or advise service providers to obtain verified parental consent, before offering services to, or collecting data from children below a certain threshold age.[22] This age, however, varies across geographies, for instance, it is 13 in the US,[23] 14 in Spain,[24] and 18 in South Africa.[25] Some legal frameworks such as the EU-GDPR and the Protection of Personal Information Act in South Africa protect minors' data under personal data protection laws, while others such as the Children's Online Privacy Protection Act in the US have specific legal frameworks dealing with children in the online space. In the following section, we will discuss some of those legal frameworks.

2.1 United States

The US enacted the Children's Online Privacy Protection Act (COPPA) in 1998, and it is one of the first pieces of legislation dealing specifically to protect the privacy of minors online. The COPPA predominantly enables parents or legal guardian to have control over what information is collected from their child under the age of 13.[26] The law requires operators of websites or online services directed to children under 13 years of age, that have actual knowledge of collecting personal information online from a child to obtain 'verifiable parental consent' for collection, use or disclosure of such personal

[18] UNICEF, 'Child Online Protection in India', available at: https://www.icmec.org/wp-content/uploads/2016/09/UNICEF-Child-Protection-Online-India-pub_doc115-1.pdf, (last accessed 27 May 2019) .

[19] Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's personal data in the EU: Following in US footsteps?', 26(2) Information & Communications Technology Law Journal (2017), available at: http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096, (last accessed 27 May 2019).

[20] UNICEF, 'Children in a Digital World, available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, (last accessed on 29 May, 2019).

[21] White Paper on Data Protection in India, available at: https://www.meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited, (last accessed on 29 May 2019).

[22] UNICEF, 'Children in a Digital World, available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, (last accessed on 29 May, 2019).

[23] Section 312.5, Children's Online Privacy Protection Act (COPPA).

[24] Article 7, Ley Orgánica de Protección de Datos (LOPD).

[25] Section 11, Protection of Personal Information (POPI) Act.

[26] 15 USC 6501-6505, COPPA.

information from children.[27] Personal information includes but is not limited to full name, home address, email address, persistent identifier that can be used to recognise a user over time, a photograph, and geolocation.[28]

The Federal Trade Commission (FTC) uses a sliding scale approach to parental consent and provides a list of possible methods that may be employed by the service provider to obtain verifiable parental consent,[29] with a more stringent verification method only required if the information is being disclosed to a third party. These include, for example:

- Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;
- Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment systems that provide notification of each discrete transaction to the primary account holder;
- Having a parent call a toll-free telephone number staffed by trained personnel;
- Having a parent connect to trained personnel via video conference; or
- Verifying a parent's identity by checking a form of government-issued identification against databases of such information.[30]

In case the operator does not "disclose"[31] the child's personal information to a third party, an email along with some additional steps such as:

- Sending a confirmatory email to the parent following receipt of consent; or
- Obtaining a postal address or telephone number from the parent and confirming the parent's consent through a letter or telephone call may suffice as a method to obtain verifiable parental consent under the COPPA.[32]

[27] Section 312.5 (a), COPPA.

[28] Section 312.2, COPPA

[29] Francoise Gilbert, Age Verification as a Shield for Minors on the Internet: A Quixotic Search? 5 SHIDLER J. L. Com. & Tech. 6 (2008), available at https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/420/vol5_no2_art6.pdf?sequence=1, (last accessed on May 31, 2019).

[30] Section 312.5 (b), COPPA.

[31] Section 312.2, COPPA.

[32] Section 312.5 (b), COPPA.

2.2 South Africa

The Protection of Personal Information Act, 2013 (The POPI Act), prohibits processing personal information of a child,[33] barring certain special conditions. The Act defines a child as a person under the age of 18 years, and processing of personal information of a child is authorised only if a competent person[34] has consented to such processing, or the processing is necessary for the establishment, exercise or defence of a legal obligation or serves a public interest among other things.[35]

2.3 European Union (EU)

With the adoption of the General Data Protection Regulation (GDPR),[36] the EU has explicitly recognised that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, and safeguards concerned and their rights in relation to the processing of personal data.[37] According to the GDPR, information service providers require parental consent prior to processing personal data of children below the age of 16.[38] An information service provider is defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.[39]

The GDPR also specifies that when the data subject is a child, information regarding what information is being collected and the purpose for which such information would be used should be simplified, in order to facilitate easy understanding by children.[40] Children also enjoy the right to have personal data concerning them rectified or removed and no longer processed ('right to be forgotten'). In cases of children, this right becomes even more significant as many a time while giving consent, a child may not be fully aware of the risks involved by the processing of personal data concerning him/her, and later may want to erase such personal data from the internet. The GDPR further clarifies that the data subject will be permitted to exercise his/her right of rectification/erasure irrespective of the fact that he or she is no longer a child.[41]

[33] Section 34, The POPI Act, 2013.

[34] Section 1 of The POPI Act, 2013 defines ''competent person'' as any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child

[35] Section 35, The POPI Act, 2013.

[36] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[37] Recital 38, EU GDPR.

[38] Article 8, EU GDPR.

[39] Article 1(1)(b) of Directive 2015/1535 of the European Parliament and of the Council.

[40] Recital 58, EU GDPR.

[41] Recital 65, EU GDPR

The GDPR also creates additional obligations for data controllers when they are processing children's personal data.[42] Even though, the provision dealing with profiling[43] does not make any distinction as to whether processing concerns an adult or a child's data, recital 71 states that solely automated decision-making, including profiling, with legal or similar significant effects, should not apply to children.[44] Furthermore, recital 38 while stating that children merit specific protection also states that such specific protection should, in particular, apply to the use of personal data of children for marketing or creating psychographic user profiles and the collection of personal data concerning children when using services offered directly to a child.[45]

While the GDPR sets 16 as the threshold age for considering a person as an adult, it allows the Member States to fix a lower national age threshold (not lower than 13 years). Due to this flexibility, some member countries in the EU have different threshold age for children, at which parental consent would be required. For instance, the data protection law in Spain states that data pertaining to data subjects over the age of 14 may be processed with their consent[46] and in the UK children aged 13 or above can provide their consent.[47] The GDPR does not prescribe any guidelines or best practices regarding the obtaining of verified parental consent. However, it requires the controller to make reasonable efforts to ensure that consent has been given or authorised by the holder of parental responsibility over the child keeping in mind the available technology at the time.[48]

2.4 Germany

The Interstate Treaty on the Protection of Minors in Germany (Jugendmedienschutz-Staatsvertrag - JMStV) mandates the use of Age Verification Solutions.[49] The law distinguishes children (less than 14 years), and adolescents (14-18 years)[50] and further provides for differentiated access according to age groups.[51] The law categorises content as absolutely illegal[52] (includes content likely to incite hatred against a particular ethnic group or violates human dignity of a person), content

[42] Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/67, European Commission, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, (last accessed on 30 May, 2019).

[43] Article 22, EU GDPR.

[44] Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/67, European Commission, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, (last accessed on 30 May, 2019).

[45] Recital 38, EU GDPR.

[46] Article 7, Ley Orgánica de Protección de Datos (LOPD).

[47] Section 9, Data Protection Act 2018.

[48] Article 8 (2), EU GDPR.

[49] Article 5(3) number 1, Interstate Treaty for the Protection of Minors in the Media, Background Report on Cross Media Rating and Classification of Age Verification Solutions, Safer Internet Forum, European Commission, 2008.

[50] Article 3, Interstate Treaty on the Protection of Minors in the Media.

[51] Article 11(3), Interstate Treaty on the Protection of Minors in the Media.

[52] Article 4(1), Interstate Treaty on the Protection of Minors in the Media.

endangering minors[53] and content that is harmful to minors.[54] Content endangering minors includes pornography and providers are required to employ a 'strict age verification method', to ensure that the content is only available to adults (or a closed user group).[55] For content considered harmful to minors such as violent games, a 'basic age verification method' is sufficient.[56] A strict age verification method requires a one-time physical identification, wherein the identity of the user is checked against a valid identity card at specific places which include the post office, point of sale in mobile phone shops or at lottery offices. In case of a basic age verification method, the user may verify his/her age through a one-time authentication and pin code provided by SMS.[57] A provider may also fulfil its obligation by scheduling the transmission of content at a time when children or adolescents do not usually see or hear the content.[58] According to the JMStV, The Kommission für Jugendmedienschutz (Commission for Youth Protection in the Media - KJM) is the competent authority to approve age verification methods in Germany.[59] Certifications are issued for a period of 5 years and may be renewed by the KJM.[60]

2.5 United Kingdom (UK) / Digital Economy Act

The UK passed the Digital Economy Act, 2017 (DEA), which is predominantly designed to regulate electronic communications infrastructure and services.[61] The DEA also makes age verification mandatory for "commercial providers of online pornography in the UK.[62] The law employs stringent age verification controls to ensure that pornographic content in the form of pictures, videos, and texts will only be accessible to individuals verified to be above 18. The law also provides for the appointment of an age verification regulator.[63] If the website hosting pornographic content does not have robust age verification checks for its users, the designated age-verification regulator will have the power to notify ancillary service providers such as social media and payment service providers.[64] The law does not mandate the use of a specific age verification method. Therefore, customers may choose the information through which they wish to be verified. The

[53] Article 4(2), Interstate Treaty on the Protection of Minors in the Media.

[54] Article 5, Interstate Treaty on the Protection of Minors in the Media.

[55] Article 4(2), Interstate Treaty on the Protection of Minors in the Media, *"…content is legal in telemedia services if the provider has ensured that such content is accessible for adult persons only (closed user group)."* and Background Report on Cross Media Rating and Classification of Age Verification Solutions, Safer Internet Forum, European Commission, 2008.

[56] Background Report on Cross Media Rating and Classification of Age Verification Solutions, Safer Internet Forum, European Commission, 2008.

[57] Background Report on Cross Media Rating and Classification of Age Verification Solutions, Safer Internet Forum, European Commission, 2008.

[58] Article 5(3) number 2, Interstate Treaty on the Protection of Minors in the Media.

[59] Article 11(2), Interstate Treaty on the Protection of Minors in the Media.

[60] Article 11(2), Interstate Treaty on the Protection of Minors in the Media.

[61] Summary of the Digital Economy Act, available at https://services.parliament.uk/bills/2016-17/digitaleconomy.html (last accessed on 31 May 2019).

[62] Section 14, Digital Economy Act, 2017.

[63] Section 16, Digital Economy Act, 2017.

[64] Section 21, Digital Economy Act, 2017.

regulator will also have the authority to order ISPs and mobile network operators to block non-complying websites[65] for UK users. The British Board of Film Classification (BBFC) has been selected as the age-verification regulator.[66]

However, the DEA only applies to commercial providers of pornographic content. Therefore, teenagers may still access porn at various social media platforms such as Reddit or Imgur since they do not offer pornographic content on a commercial basis. Furthermore, with Virtual Private Networks (VPNs) remaining legal in the UK, underage users will be able to obviate age-restrictions. The DEA has also been criticised for potentially enabling private companies to create a database of pornographic users and their sexual preferences. David Kaye, the United Nations special rapporteur on the promotion and protection of the right to freedom of opinion and expression also wrote an open letter to the British government, wherein he raised his concerns *"related to the bill's disproportionate measures, lack of data sharing safeguards and adequate judicial process"*.[67]

2.5.1 BBFC as an Age Verification Regulator

The role of BBFC as an age verification regulator is to assess whether an online pornographic service has effective age verification controls to ensure that explicit content is not normally accessible to individuals under the age of 18. While the BBFC does not provide an exhaustive list of approved age-verification methods, it states the criteria it will employ to assess a service provider. These include:

1. an effective control mechanism at the point of registration or access to pornographic content by the end-user which verifies that the user is aged 18 or above at the point of registration or access;
2. use of age-verification data that cannot be reasonably known by another person,;
3. a requirement that either a user age-verify each visit or access is restricted by manual or electronic controls. A consumer must be logged out by default unless they positively opt-in for their log in information to be remembered; and
4. the inclusion of measures which authenticate age-verification data and measures which are effective at preventing use by non-human operators including algorithms.[68]

Furthermore, the BBFC also categorically states that practices such as relying solely on the user to confirm their age, using a general disclaimer, or accepting age verification through online payment methods which do not set the threshold age at 18, will not be considered as complying with the requirements of DEA. The BBFC also recommends age-verification

[65] Section 23, Digital Economy Act, 2017.

[66] https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2019-04-24/HCWS1521/ (last accessed on 31 May 2019)

[67] Ceylan Yeginsu, To View Online Porn, First Show Your Papers: U.K. Will Begin Age Checks, The New York Times (online, 19 April, 2019), available at: https://www.nytimes.com/2019/04/19/world/europe/britain-age-checks-pornography.html, (last accessed on 20 June, 2019).

[68] Guidance on Age Verification Arrangements, BBFC, October 2018, available at https://www.ageverificationregulator.com/assets/bbfc-guidance-on-age-verification-arrangements-october-2018-v2.pdf, (last accessed on 31 May 2019).

providers to adopt good practice, which may include solutions that collect minimum data, include clear information for end-users on data protection and reduce the potential for misuse of a verified account.[69]

According to the DEA, when a UK IP address attempts to access a website with pornographic content, the person browsing the web will have to verify themselves. When the user first enters the website, a splash page is visible that does not show any explicit images. The verification methods are technology neutral, meaning the service providers have the prerogative to implement the technology that enables people to demonstrate that they are above the threshold age.

The following figure is a representational image of the website where the user's age will be verified.

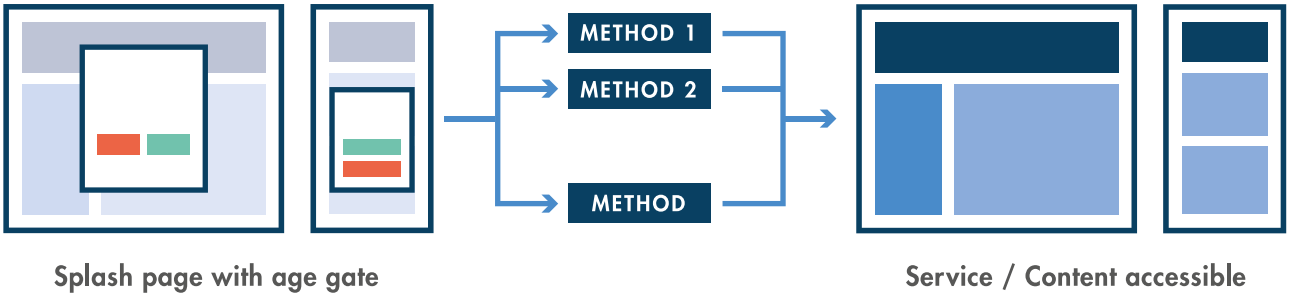

Figure 1: Representational image of a website using age verification.

[69] Guidance on Age Verification Arrangements, BBFC, October 2018, available at https://www.ageverificationregulator.com/assets/bbfc-guidance-on-age-verification-arrangements-october-2018-v2.pdf, (last accessed on 31 May 2019).

3. INDIA

A survey undertaken by the Internet and Mobile Association of India (IAMAI) in 2015 indicated that an estimated 28 million out of a total of 400 million internet users in India are school going children. The survey also stated that the proportion of children among rural internet users witnessed an increase from 5% in 2014 to 11% in 2015.[70]

Intel Security carried out a survey in 2015 which sought to examine the online behaviour and social networking habits of 8 to 16 years old in India. The survey had 2,370 participants, which included 1,185 parents and 1,185 children. As per the survey, 81% of the children were already active on social media, and approximately 77% of the children had a Facebook account before 13 years of age. In addition to being active on social media, Indian children also share personal data without realising the risks of indulging in such behaviour. For instance, children participating in the Intel Study reported that 69% had shared photographs, 58% posted their e-mail ids, and 42% disclosed their phone numbers. Furthermore, the study by Intel Security noted that in the US and Singapore, an estimated 70% of children use social media, which is lower than their Indian counterparts (81%).[71] An estimated 44% of the polled children stated that they would be willing to meet or have met a stranger they first encountered online.[72] This puts children at a significant risk of harm including but not limited to stalking, harassment, sexual abuse and trafficking.

The current regulatory regime in India does not make any distinction between an adult or a child's personal data. Further, it does not mandate online service providers to incorporate age verification mechanisms to prevent minors from harm. In 2013, the Delhi High Court had sought information from the Central Government regarding how individuals under the age of 18 are registering on social networking sites.[73] The Court was apprised that in India, there is no specific provision restricting the use of social media by minors. Facebook and Google were respondents in the case and clarified that these companies follow the COPPA, according to which children under the age of 13 are forbidden from opening an account. The Court expressed displeasure about the absence of mechanisms under the Indian law for verifying the age of a child online.[74] Therefore, as such, there are no formal age checks in place. However, some service providers may have undertaken voluntary measures for the protection of minors. Furthermore, there is a petition pending in the Delhi High Court seeking a ban on online gambling websites. The petition also highlights that most of these websites do not have any age restrictions in place owing to which minors can use these online gambling websites with ease, thereby exposing them to the ills of the gambling world. As such, most of these websites have been designed to lure young players and therefore these websites do not implement any age barriers for restricting minors' access.[75]

---

[70] UNICEF, 'Child Online Protection in India, available at: http://unicef.in/PressReleases/418/UNICEF-India-launches-the-first-comprehensive-report-on-Child-Onl, (last accessed on 11 June, 2019).

[71] Shruti Dhapola, More kids are online, but Indian parents are finally taking stock: Intel Study, The Indian Express (online, 25 December, 2015), available at: https://indianexpress.com/article/technology/tech-news-technology/more-kids-are-online-but-indian-parents-are-finally-taking-stock-intel-study/ (last accessed on 17 June, 2019).

[72] Almost 50% of Indian children admit to meeting a stranger they first met online, reveals Intel Security study, DataQuest, available at: https://www.dqindia.com/almost-50-of-indian-children-admit-to-meeting-a-stranger-they-first-met-online-reveals-intel-security-study/ (last accessed on 19 June, 2019).

[73] *K.N. Govindacharya v. Union of India*, W.P.(C) 3672/2012, Delhi Hight Court.

[74] Indian Court Orders Facebook, Google to Offer Plans for Protecting Children, 12 August, 2013, available at: https://www.orfonline.org/article/indian-court-orders-facebook-google-to-offer-plans-for-protecting-children/, (last accessed on 18 June, 2019).

[75] WP(C)5661/2019, Delhi High Court.

In July 2018, Justice Sri Krishna Committee released the first draft of the Personal Data Protection Bill, 2018, which recognises the need for protecting children's data in the digital economy.

3.1 Treatment of children's data in the personal data protection bill, 2018

The Srikrishna Committee report recognised that the treatment of children's data ought to be different from the treatment of an adult's data, as children are more likely to be unaware of the consequences of their actions. This problem is further exacerbated by consent being sought in a complicated manner that makes it difficult for children to navigate the digital world.[76] According to the draft, Personal Data Protection Bill, the Data Protection Authority (DPA) shall have the power to notify data fiduciaries who operate commercial websites or online services directed at children, or who process large volumes of personal data of children as 'guardian data fiduciaries'.[77] As such, the Committee has acknowledged that there may be two categories of data fiduciaries engaged in the processing of personal data of children, namely:

- Services offered primarily to children – for instance, YouTube Kids app, Hot Wheels and Walt Disney; and
- Social media services – such as Facebook and Instagram.[78]

3.1.1 Who is a 'child'?

A 'child' has been defined as a person below the age of 18 in the Personal Data Protection Bill, 2018.[79] Therefore, personal data of an individual under the age of 18 can only be processed based on prior parental consent. This is in line with the definition of a 'child' in The Convention on the Rights of the Child (CRC) to which India is a signatory.[80] Also, as per Section 11 of the Indian Contract Act, only a person who has attained the age of majority is competent to enter into a contract in India. The age of majority in India is 18 as per the Indian Majority Act.[81] The Srikrishna Committee, in its reasoning, stated 18 years as the recommended threshold age in order to ensure consistency with the existing legal framework in India.[82] However, children start using the internet for educational as well as recreational purposes from a very young age[83] and age limit of 18 may appear too high and impractical in the digital world.

3.1.2 Processing of a child's data

Furthermore, processing of a child's data will only be legal in case of prior parental consent. The only exception to parental consent requirement as per the Bill would be in cases where the guardian data fiduciary is exclusively engaged

[76] Srikrishna Committee Data Protection Report, A Free and Fair Digital Economy, 2018, Pg. 42.

[77] Section 23(4), The Personal Data Protection Bill, 2018.

[78] Srikrishna Committee Data Protection Report, A Free and Fair Digital Economy, 2018, Pg. 43

[79] Section 3(9), The Personal Data Protection Bill, 2018.

[80] Article 1, CRC.

[81] Section 3, The Indian Majority Act, 1875.

[82] Srikrishna Committee Data Protection Report, A Free and Fair Digital Economy, 2018, Pg. 44.

[83] Sheri Bauman and Tanisha Tatum, Web Sites for Young Children: Gateway to Online Social Networking? 13(1) Professional School Counselling (2009).

in the provision of counselling or child protection services.[84] This exception is in the best interests of a child because in many cases parents may be directly or indirectly related to the issue at hand such as child abuse or harassment by a family member, and requiring prior parental consent will render the purpose of such services infructuous.[85] This exception has also been provided for in the EU-GDPR.[86]

Guardian Data Fiduciaries shall be barred from data processing activities that have been found to be harmful for children. The harm may be tangible such as physical or reputational harm (cyberbullying, revenge porn, and impersonation) or intangible in terms of loss of autonomy (unable to distinguish between the real and virtual).[87] Consequently, guardian data fiduciaries are barred from undertaking any data processing activities that can cause harm to children, including but not limited to profiling, tracking, or behavioural monitoring of, or targeted advertising directed at, children.[88] Behavioural profiling also finds application in the education industry, wherein learning analytics are used to mine data about students while they perform learning tasks. These learning analytics systems enable real-time assessment of an individual and can be employed for future prediction of learning progress or recommendation of suitable educational pathways. The use of such data combined with machine learning techniques poses significant risks in limiting opportunities offered to children based on assumptions encoded in such algorithms.[89]

Tracking and profiling children's behaviour are harmful as they may expose children to age-inappropriate content, including ads selling alcohol or tobacco or popups for dating apps. According to a study, pornographic pop-up ads are the leading cause for children stumbling upon explicit content over the internet.[90] Furthermore, minors especially younger children lack the ability to distinguish between commercial content and non-commercial content, and their capacity to critically engage with advertisements is less developed, thereby rendering them more susceptible to the influence of online marketing.[91] Consequently, children are at a higher risk of falling into the consumeristic trap and are more likely to overspend, largely due to their inability to differentiate between content and commercial ads.

As per the Personal Data Protection Bill, all data fiduciaries will be required to incorporate appropriate mechanisms for age verification and parental consent in order to process personal data of children.[92] Appropriateness of the age-verification method incorporated by a data fiduciary shall be determined based on:

[84] Section 23(7), Personal Data Protection Bill, 2018.

[85] Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's personal data in the EU: Following in US footsteps?', 26(2) Information & Communications Technology Law Journal (2017), available at: http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096, (last accessed 30 May 2019).

[86] Recital 38, EU GDPR, "The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

[87] Srikrishna Committee Data Protection Report, A Free and Fair Digital Economy, 2018, Pg. 44.

[88] Section 23(5), The Personal Data Protection Bill, 2018.

[89] Deborah Lupton and Ben Williamson, The Datafied Child: The Dataveillance of Children and Implications for Their Rights, 19(5) New Media & Society (2017).

[90] The Protection of Children Online, OECD, 2012.

[91] The Protection of Children Online, OECD, 2012.

[92] Section 23(2), The Personal Data Protection Bill, 2018.

1. the volume of personal data processed;
2. the proportion of such personal data likely to be that of children;
3. possibility of harm to children arising out of the processing of personal data; and
4. such other factors as may be specified by the Authority.[93]

While the draft bill does not provide any guidance on the methods of age verification, it does indicate that appropriate age verification mechanisms may include mandatory login or date of birth input or other approved age verification mechanisms.[94]

The Personal Data Protection Bill, 2018 requires data fiduciaries to incorporate appropriate age verification mechanisms.[95] However, it does not provide any guidance on what methods data fiduciaries may incorporate for age verification. The Bill further states that the Data Protection Authority may issue codes of practice with respect to appropriate age-verification mechanisms.[96] However, unlike the age-verification regulator under the DEA or the KJM as per the German Interstate Treaty on the Protection of Minors, the Indian bill does not provide for any regulator or body certifying whether appropriate age-verification methods have been employed by the service provider.[97] In one of the stakeholder comments to the draft Bill, it has been opined that the Bill should incorporate certain principles of age verification and must not delegate all responsibility to the DPA.[98]

Majority of the stakeholders commenting on the Persona Data Protection Bill agreed with the Committee that the Indian law should have safeguards in place for children.[99] However, many stakeholders felt that '18' as the threshold age for consent is too high in the digital economy and does not take into account the realities of children's interaction with the internet.[100] It was also pointed out that in the case of *K.N. Govindacharya v. Union of India*,[101] the Delhi High Court recognised the general practice of fixing 13 as the minimum age to register on social media.[102] Some stakeholders while responding to the Personal Data Protection Bill suggested that minors may be categorised as: under 13 years of age (only consent by parents or guardians); 13-18 years (or 16 with parental consent) and above 18 years of age (consent of the user

[93] Section 23(3), The Personal Data Protection Bill, 2018.

[94] Srikrishna Committee Data Protection Report, A Free and Fair Digital Economy, 2018, Pg. 44.

[95] Section 23(2), The Personal Data Protection Bill, 2018.

[96] Section 61(6), The Personal Data Protection Bill, 2018.

[97] Inputs received from a Stakeholder.

[98] See Software Freedom Law Centre's comments to the Personal Data Protection Bill, 2018, available at: https://privacy.sflc.in/our-comments-draft-data-protection-bill/, (last accessed on 20 June 2019).

[99] The Ministry of Electronics and Information Technology, drafting India's Data Protection Bill, has not made the submissions public. Medianama has compiled a list of submissions available at: https://www.medianama.com/2018/10/223-personal-data-protection-bill-submissions/, (last accessed on 19 June 2019).

[100] See for e.g., Response of BSA-The Software Alliance, Information Technology Industry Council's comments to the White Paper. Also see, The Centre for Internet Society's comments and recommendations to the Personal Data Protection Bill, 2018, Broadband India Forum's comments to the Personal Data Protection Bill,

[101] WP(C)3672/2012, Delhi High Court.

[102] Submission made by Broadband India Forum at pg.27.

is sufficient).[103] Another area of concern highlighted by the stakeholders is the lack of provisions allowing data principal to withdraw the consent given by parents on behalf of the child.[104] As such, the Personal Data Protection Bill, 2018 in its present form does not provide for the withdrawal of consent by children.

The Srikrishna Committee report also states that from the perspective of the full, autonomous development of the child, the age of 18 may appear too high.[105] Nevertheless, the draft bill mandates parental consent for children under the age of 18 in order to ensure consistency with the age of majority in India. It is worth mentioning that subsequent to the new Juvenile Justice (Care and Protection of Children) Act, 2015, any 'child' between the age of 16-18 accused of committing a heinous crime can be tried as an adult under the Indian Penal Code.[106] Moreover, in the offline world, age restrictions vary depending on the goods or services being accessed by a user. The following table provides a few examples of variation in threshold age:

Goods/Services	Threshold Age
Alcohol	**21 years** for most States, **18 years** in Rajasthan, Himachal Pradesh, Andaman & Nicobar, Puducherry, Sikkim and Mizoram, **23 years** in Kerala, and **25 years** in Delhi, Punjab, Haryana, Chandigarh and Maharashtra.[107]
Tobacco	**18 years**.[108]
Content	**Films** – 'U' Certificate (All ages), 'UA' Certificate (Children under 12 require parental guidance) and 'A' Certificate (Above 18).[109]
	Television – Only movies with a 'U' certificate can be telecast. Programmes unsuitable for children must not be carried in the cable service at times when the largest numbers of children are viewing.[110]
	Video on Demand – Self Regulation.
Driving[111]	**Motorcycle without gears** – 16 years.
	Four-wheeler – 18 years.
	Transport vehicle – 20 years.

Table 1: Threshold ages for access to different services in India.

[103] See for e.g. CIS comments on the White Paper of the Committee of Experts on a Data Protection Framework for India, Broadband India Forum's comments to the Personal Data Protection Bill, 2018.

[104] See for e.g. submissions made by CCG and CIS.

[105] Srikrishna Committee Data Protection Report, A Free and Fair Digital Economy, 2018, Pg. 44.

[106] Section 15, Juvenile Justice Act, 2015.

[107] Explained Snippets | Legal drinking age: Mostly 21; 25 in Delhi and four other states, The Indian Express (online, 30 May 2018), available at: https://indianexpress.com/article/explained/explained-snippets-legal-drinking-age-mostly-21-25-in-delhi-and-four-other-states-5196264/, (last accessed on 19 June 2019).

[108] Section 6, The Cigarettes and Other Tobacco Products (Prohibition Of Advertisement And Regulation Of Trade And Commerce, Production, Supply And Distribution) Act, 2003

[109] CBFC Guidelines, available at: https://www.cbfcindia.gov.in/main/guidelines.html, (last accessed on 19 June 2019).

[110] Rule 6, Programme and Advertising Codes prescribed under the Cable Television Network Rules, 1994. (Restriction on broadcast of programmes unsuitable for minors is relaxed after 8 pm as per Self-Regulatory Content Guidelines by Indian Broadcasting Foundation.)

[111] Section 4, The Motor Vehicles Act, 1988.

Figure 2: An overview of methods for age verification.

4. AGE VERIFICATION METHODS

Age-verification is an evolving and dynamic technology[112] owing to which most countries mandating the use of age verification methods do not require the use of a specific mechanism to verify user age. A variety of methods are currently being used by service providers to verify a user's age in order to ensure that age-restricted services remain inaccessible to minors. Effectiveness of age-verification methods are dependent on a multitude of factors. These include ability to restrict minors from accessing adult content, costs involved in implementing a particular age verification method and balancing issues related to data protection and online privacy for minors while at the same time protecting and allowing for participation of minors in the digital economy.[113]

In this section, various age-verification methods are discussed along with their advantages and drawbacks.

I. Self-Certification Method

In this method, the user is inquired about their age when they enter a website that contains age-restricted content. Self-certification per se is not an age verification method. However, if the self-certification method incorporates a mechanism

[112] Guidance on Age Verification Arrangements, BBFC, October 2018, available at https://www.ageverificationregulator.com/assets/bbfc-guidance-on-age-verification-arrangements-october-2018-v2.pdf, (last accessed on 2 June 2019).

[113] Background Report on Cross Media Rating and Classification of Age Verification Solutions, Safer Internet Forum, European Commission, 2008.

to verify the veracity of the information disclosed by the user, then it can be a valid age-verification method.[114] While this method is easy to use, it relies on individuals disclosing their age truthfully. However, it has been observed that minors often lie in order to use various social media sites.[115] One way to minimise the chances of falsification is seeking information about the user's age in a neutral manner, that is, asking their date of birth when they enter the site without disclosing that a user has to be of a minimum age to access the service.[116] Additionally, a temporary or permanent cookie might be employed to prevent users from re-registering on the site with different age.[117] Examples of sites using this method include Facebook and Google.

Advantages	Disadvantages
• Simple to use • Service providers do not have to bear any additional costs	• Users lie about their age • Not very effective

Table 2: An overview of self-certification methods.

II. Credit/Debit Card Information

Users are made to enter their credit card/debit card information. This method relies on the premise that only adults or people over the age of 18 use credit or debit cards. However, that may not be the case in many jurisdictions. One of the main issues with using Credit or Debit card information is that they were not conceptualised as a potential tool for age verification.[118] For instance, in India, RBI issued a circular on May 6, 2014, wherein banks were advised to allow minors above the age of 10 to open and operate a savings bank account independently. Minors are also issued a debit card which they may use for cash withdrawal as well as online transactions.[119] Furthermore, minors may also have access to their parents' credit/debit cards. Moreover, the use of this method of verification is limited to paid services. One way to circumvent this issue is by forbidding the use of payment methods that do not require a user's minimum age to be 18 years. For instance, BBFC as an age-verification regulator under the DEA, will not regard confirmation of ownership of any other card where the cardholder is not required to be 18 or over to be verification that a user is aged 18 or over.[120]

[114] Background Report on Cross Media Rating and Classification of Age Verification Solutions, Safer Internet Forum, European Commission, 2008.

[115] More than 80% of children lie about their age to use sites like Facebook, The Guardian, available at https://www.theguardian.com/media/2013/jul/26/children-lie-age-facebook-asa, (last accessed on 2 June 2019).

[116] Complying with COPPA: Frequently Asked Questions, available at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions, (last accessed on 2 June 2019).

[117] Francoise Gilbert, Age Verification as a Shield for Minors on the Internet: A Quixotic Search?, 5 SHIDLER J. L. Com. & Tech. 6 (2008), available at https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/420/vol5_no2_art6.pdf?sequence=1, (last accessed on 2 June 2019).

[118] Background Report on Cross Media Rating and Classification of Age Verification Solutions, Safer Internet Forum, European Commission, 2008.

[119] RBI, Opening of Bank Accounts in the Names of Minors, 2014, available at https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=8866&Mode=0 , (last accessed on 2 June 2019).

[120] Guidance on Age Verification Arrangements, BBFC, October 2018, available at https://www.ageverificationregulator.com/assets/bbfc-guidance-on-age-verification-arrangements-october-2018-v2.pdf, (last accessed on 2 June 2019)

According to data released by the RBI, 47.9 million credit cards and 884.7 million debit cards were operational in India during April 2019.[121] If service providers insist on using credit cards as a method of age-verification in India, as opposed to both credit and debit cards, then a significant population of this country will be excluded from accessing services that mandate prior age-verification.

Advantages	Disadvantages
• Ubiquitous. • Credit cards are issued only to people over the age of 18, making it an effective method to ascertain a user's age.	• Many minors may have a debit card which they operate independently. • Minors may also have access to their parents' cards, and the online service provider will have no way of verifying whether a minor is accessing the site or an adult. • Solely using credit cards as a method of verification will exclude a sizeable population in India.

Table 3: An overview of verification methods using credit / debit cards.

III. Government-Issued Identity Cards (IDs)

Identity cards issued by the government of any nationality are a credible and trustworthy data source for age verification. Another way in which government IDs can be employed from preventing minors from accessing age-restricted content is by relying on information about adults contained in databases of government to verify whether the visitor qualifies as an adult or not.[122]

In this method, a user enters a website, and his/her ID information is sought by the service provider to ensure that the user is permitted to view the website's content. Once the user enters the government issued ID number, the information is verified against the government database. This is usually done through a third-party verification system, that is, a third party verifies the user's age for the website. Third party providers may include mobile phone operators, credit card companies and databases containing information on IDs such as passport and driver's license.

In many countries, national ID cards are used for age verification. Some age verification tools verify a user's age by checking it against a valid driver's license or other government-issued ID cards.[123] In some countries, a user's Social Security Number (SSN) or other such data which can be verified against a government database is used. An example of a country employing this method is South Korea, wherein, all search engines in South Korea are required by law to carry

[121] RBI, ATM & Card Statistics for April 2019, available at https://www.rbi.org.in/Scripts/ATMView.aspx, (last accessed on 9 June 2019).

[122] Self-Regulation in the Alcohol Industry, Report of the Federal Trade Commission, June 2008.

[123] Online Age Verification for Our Children, A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives, The Future of Privacy Forum.

out age verification for viewing adult content.[124] However, SSNs qualifies as sensitive information and users may not be comfortable in disclosing this information to third parties. Furthermore, if the third parties do not employ adequate safeguards preventing a breach of data, it could cause severe losses to the user.

Advantages	Disadvantages
• A credible source of information.	• In cases of national IDs, the functionality may be an issue in a different jurisdiction. • Sensitive information (more than a user's age) that has significant data protection and privacy concerns. • Every citizen may not have a government-issued ID card, and this may exclude a portion of the population.

Table 4: An overview of age verification using National IDs.

IV. Semantic Analysis

Semantic analysis works on the principle that people of a certain age are more likely to employ different and identifiable levels of sophistication when constructing, for example, a social networking profile.[125] Companies use search algorithms which parse information and look for terms/words that are commonly used by underage users. Tinder has stated that it uses tools including "automatic scans of profiles for red flag language and images" to identify underage users.[126] This method is usually employed in tandem with some other method of age-verification.[127]

[124] Online Age Verification for Our Children, A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives, The Future of Privacy Forum.

[125] Online Age Verification for Our Children, A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives, The Future of Privacy Forum.

[126] Tinder, Grindr questioned over age verification requirements after several child abuse cases, available at https://economictimes.indiatimes.com/magazines/panache/tinder-grindr-questioned-over-age-verification-requirements-after-several-child-abuse-cases/articleshow/67957367.cms, (last accessed on 2 June 2019).

[127] Background Report on Cross Media Rating and Classification of Age Verification Solutions, Safer Internet Forum, European Commission, 2008.

Advantages	Disadvantages
• In cases of self-certification, can be used as an additional layer for verification of a user's age. • It can be used to monitor discrepancies even after signup.	• Technology is still being developed, and therefore, this method is imprecise. • People may have different levels of maturity. For instance, a precocious 11-year-old child may not necessarily sound or behave like one. • Can identify the age range and not the exact age. • Challenging to implement in multilingual societies. • Highly intrusive.

Table 5: An overview of semantic analysis for age verification.

V. Biometrics

Biometric data means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural characteristics (such as walking gait or typing style)[128] of a data principal, which allow or confirm the unique identification of that natural person.[129] In this form of age-verification, a user's age may be ascertained by capturing fingerprints, measuring bone density, iris scans, or capturing facial images. It is stated to accurately predict the age of the users, at least within a specific range.[130] Some providers of age-verification technology also use biometrics to determine a user's age. For instance, Yoti, a London based technology company uses a person's facial images to determine whether an individual is old enough to access the content. In this method, once the user uploads his/her image, the human face is detected, and only the relevant portion of the face or pixel data is fed into the neural network to get an age estimate. Once the user's age is verified, the image is deleted from the server.[131] Since it is an emerging technology, its age estimates are subject to a margin of error, and it, therefore, provides an age range and not the exact age.[132]

The following image provides an overview of biometric-based age verification solution:

[128] Online Age Verification for Our Children, A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives, The Future of Privacy Forum.

[129] Section 3(8), The Personal Data Protection Bill, 2018.

[130] Background Report on Cross Media Rating and Classification of Age Verification Solutions, Safer Internet Forum, European Commission, 2008.

[131] Description of the method employed by Yoti. Other companies may choose to retain the image.

[132] Yoti Age Scan – Public Version, April 2019, available at https://s3-eu-west-1.amazonaws.com/prod.marketing.asset.imgs/yoti-website/Yoti-Age-Scan_Digital.pdf, (last accessed on 3 June 2019).

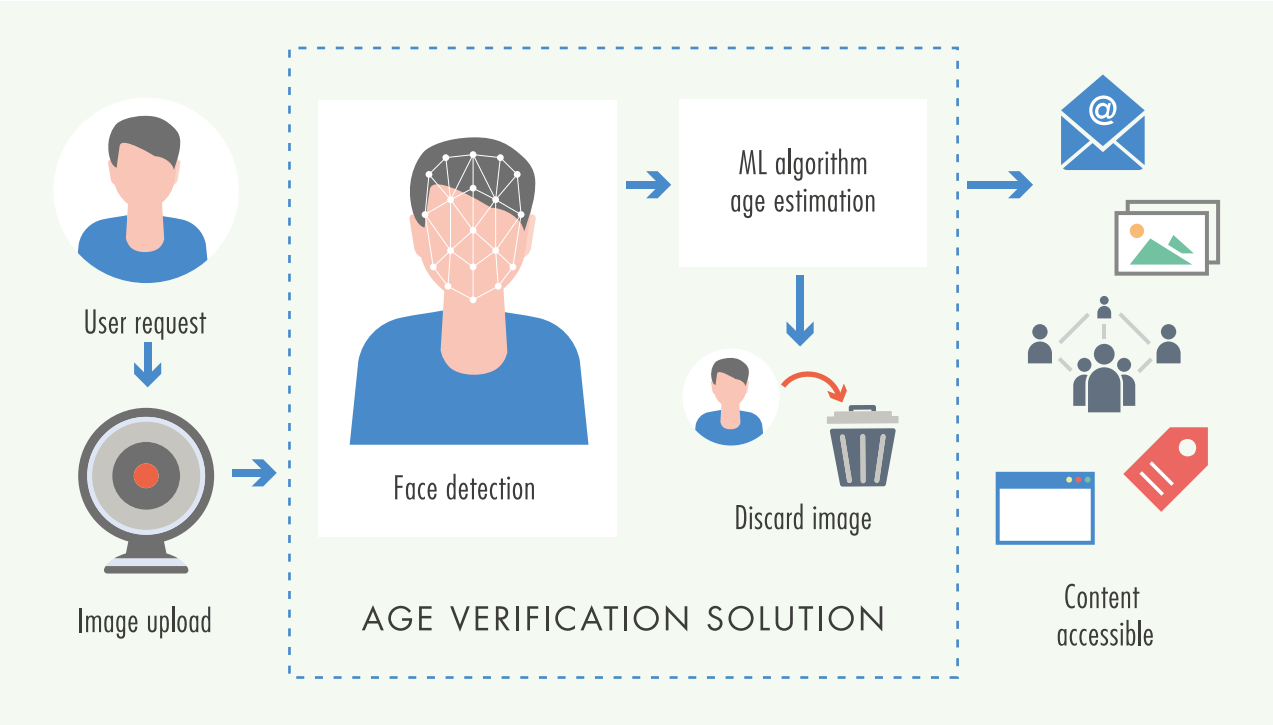

Figure 3: A representational image of age verification using biometrics.

Advantages	Disadvantages
• Unique identification and difficult to evade.	• Does not give an exact age. • The margin of error is high at this point. • Costly to implement. • Users may not be comfortable sharing their biometric information with a third party.

Table 6: An overview of biometrics for age verification.

VI. Offline Verification

A one-time face to face verification method is employed in this form of age verification. A user's age is then supported through traditional IDs such as driver's license, voter ID, or passport. Mobile operators use this method at the point of sale of mobile devices.[133] This method may also be implemented through the purchase of vouchers from a local shop, where face to face ID and age verification may take place at the point of sale. This system will be used by AgeID to comply with the age verification requirements under the DEA. A user will be able to buy a voucher, known as PortesCard, from a

[133] Background Report on Cross Media Rating and Classification of Age Verification Solutions, Safer Internet Forum, European Commission, 2008.

local shop and use its unique validation code to verify their age.[134] However, since this method relies on a validation code, a minor may obtain this information and gain access.

Advantages	Disadvantages
• Offline identification methods are reliable since it facilitates a face to face identification and verification.	• Service providers are required to incur additional costs. • Minors may obtain a known adult's offline verification code.

Table 7: An overview of offline age verification.

4.1 Challenges

I. Effectiveness of Age Verification[135]

Even though age verification methods appear to be a robust mechanism for the protection of minors in the digital economy, it is challenging to employ them successfully. Methods which rely on users to enter their age are mostly ineffective due to users falsifying age data. While methods relying on remote verification also have loopholes since it is difficult to identify whether the user is providing his/her actual identity or using somebody else's information to circumvent verification methods. Therefore, relying solely on age verification methods may be insufficient to protect minors.

A significant implementation challenge with any of the verification methods discussed in the preceding section is that a single step mechanism is highly prone to failure. In order to minimise the risks of minors accessing restricted service, it is, therefore, necessary to have at least a two-step process.[136] An authentication process must follow the identification of the individual.[137] Identification may be performed by entering any Government ID number including PAN card, driver's license, social security number or even a mobile phone number. Once the user has entered this information, the service provider must verify that the person trying to access the system is who they claim to be in the first step.[138] This may be done through sending a One Time Password (OTP) to the user's mobile phone number, or by running real-time checks across multiple government databases or by using algorithms to ensure that the user has not forged his/her documents.[139]

[134] This is how Age Verification will Work Under the UK'S Porn Law, available at https://www.wired.co.uk/article/uk-porn-age-verification, (last accessed on 3 June 2019).

[135] Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Taskforce to the Multi-State Working Group on Social Networking of State Attorneys General of the United States, 2008.

[136] Jamie Tolentino, Are your users who they say they are? How do you know? Future of Communications (online, 30 March 2015), available at: https://thenextweb.com/future-of-communications/2015/03/30/are-your-users-who-they-say-they-are-how-do-you-know/, (last accessed on 29 June 2019).

[137] Inputs received from a stakeholder.

[138] Thomas J. Smedinghoff and David A. Wheeler, Addressing the Legal Challenges of Federated Identity Management, Privacy and Security Law, 2008, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1121127, (last accessed on 9 June 2019).

[139] Inputs received from a stakeholder.

However, the issue with OTPs is that a minor may have access to an adult's phone, which he/she may use to circumvent the age-verification requirement.

II. Implementation Costs and Barriers to Entry

While a two-step process may be more practical in terms of preventing minors from accessing age-restricted services, it may also increase the cost of complying with age verification requirements. On an average, a basic authentication mechanism costs INR1 – 2 per transaction in India (approximately USD0.014 – USD0.028),[140] while a more sophisticated method may cost up to INR 5 per transaction (USD0.072).[141] Even though the cost per transaction may seem low, it is vital to keep in mind that these costs may vary significantly based on a website's user base and the frequency of age-verification implemented by the service. If a website gets 10,000 users in a day, then the cost becomes INR10,000-20,000 (USD144.1-USD288.3)[142] and, some websites get almost 50,000 users in a day (costing approximately INR 1,00,000 – INR2,00,000; an estimated USD1441.9 – USD2,883.9).[143] Moreover, it is not uncommon for websites to have 50,000 users a day. The costs also increase depending on the number of times a website authenticates a user.[144] Therefore, while a single transaction cost for a basic authentication method may not be high, it increases significantly depending on the number of users. Therefore, the costs involved in implementing a more stringent verification method may discourage service providers from undertaking watertight age-verification methods. Thus, high costs associated with age verification may also prove to be a major deterrent for new entrants to the market.

III. Absence of Standard Age-Verification Mechanisms

Age verification technology is dynamic, and as such, there exist no standards within the industry. For instance, the Personal Data Protection Bill, 2018 requires data fiduciaries to incorporate appropriate age verification mechanisms but does not provide any guidance on what methods data fiduciaries may incorporate.[145] However, IEEE is currently in the process of developing standards that seek to establish a framework for age-appropriate digital services wherein end users are children and thereby customises the services to be age appropriate. Tailoring services based on age of the user is crucial to creating a digitally safe environment for children incorporating principles of safety by design and delivery, privacy by design, autonomy by design and safety by design and delivery.[146] In addition to this, IEEE is also developing a standard for child and student data governance which seeks to define specific methodologies for accessing, collecting, storing, utilizing, sharing and destroying child and student data.[147]

---

[140] Rate of exchange as on 9 June 2019.

[141] Rate of exchange as on 9 June 2019.

[142] Rate of exchange as on 9 June 2019.

[143] Rate of exchange as on 9 June 2019.

[144] Inputs received from a stakeholder.

[145] Section 23(2), The Personal Data Protection Bill, 2018.

[146] P2089 - Standard for Age Appropriate Digital Services Framework - Based on the 5Rights Principles for Children, IEEE Standards Association, available at: https://standards.ieee.org/project/2089.html, (last accessed on 29 July 2019).

[147] P7004 – Standard for Child and Student Data Governance, IEEE Standards Association, available at: https://standards.ieee.org/project/7004.html, (last accessed on 30 July 2019).

IV. Impact on Minor's Rights

Discussion on children's rights in the online space has focused mainly on preventing them from harm, and this has reduced children to vulnerable users, thereby neglecting their agency and right to access and participation.[148] As discussed in Section 2, most regulatory approaches have been based on the principles of parental consent. In some cases, the need for prior parental consent may increase barriers to access. For instance, only 29% of total internet users in India are females, and many girls in rural areas are forbidden or discouraged from accessing the internet.[149] Mandating parental consent is likely to increase this gender-divide. Also, this approach presupposes a healthy relationship between the minor and his/her family which may not be the case, for children from abusive households or facing restrictions at home, such a scenario of obtaining prior parental consent may not be feasible.

V. Privacy Concerns

Age verification methods collect personal information, such as mobile phone numbers or credit/debit card information or information from government databases. Since most of these databases only store adult information, age verification providers verify a minor's age by prompting parents to submit a minor's personal information such as date of birth, address, name of the school or gender.[150] Consequently, age verification companies gain access to a large amount of personal data that may be misused or compromised due to inadequate safeguards.

[148] Sonia Livingstone et al., 'One in Three: Internet Governance and Children's Rights', Global Commission on Internet Governance Paper Series No. 22 (November 2015), available at: https://www.cigionline.org/sites/default/files/no22_2.pdf, (last accessed on 29 June 2019).

[149] UNICEF, 'Children in a Digital World, available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf, (last accessed on 29 June 2019).

[150] Brad Stone, Online Age Verification for Children Brings Privacy Worries, The New York Times (online, 15 November, 2008), available at: https://www.nytimes.com/2008/11/16/business/16ping.html, (last accessed on 28 June 2019).

5. CONCLUSION AND RECOMMENDATIONS

Age verification is a necessity for the safe participation of minors in the digital economy. However, as discussed earlier, it is not without its challenges. Thinking ahead on this subject requires us to consider the complexity of the problem. Much like achieving security in online spaces without compromising on privacy and achieving that fine balance, age verification also requires a balance between protecting minors from harm in the online spaces without impeding their right to expression or infringement of their privacy. Some age verification solutions open new concerns with the privacy of users and the protection of their data. While in some cases, the absence of these would potentially result in the infringement of the privacy of minors and put them at risk. As discussed in Section 4, every age-verification method has its share of drawbacks, while some such as biometrics may be too intrusive others such as self-certification are prone to errors. Keeping in mind these challenges following are some suggestions for forward thinking on this subject:

1. Age verification requirement needs to vary across different online services since a homogenous age-verification method is neither feasible nor required. For instance, the same degree of protection is not necessary for opening an email account or signing up for a dating website or participating in real money gaming. Even in the offline world, some films may be open to viewing by a 13-year-old with parental guidance; however, the sale of alcohol to a 13-year-old would be illegal irrespective of parental consent.[151]

   Digital economy relies on monetisation of data and service providers vary significantly in how they treat their users. It has been observed that verification methods in unregulated sectors (such as online gaming or matrimonial/ dating websites) are weaker than regulated sectors (such as banking and finance).[152] Even though, teenagers form a significant user base for some of these apparently unregulated sectors such as online gaming. While, gambling is banned in most States in India, some websites allowing sports betting or card games such as blackjack or poker are currently permitted as being games of 'skill' rather than games of pure 'chance'.[153] It is imperative to understand that a single model of age-verification method will not cater to the needs of all sectors. Therefore, there is a need for sector-specific guidelines wherein stricter restrictions are imposed on service providers that render services having a higher risk of harm, such as access to inappropriate content or online dating websites. As such, age verification requirements must be proportional to the potential risks that a minor may encounter and should not impose an unnecessary compliance burden on the service provider.

   The current legal regime in India does not mandate online service providers to employ any age verification methods. However, some service providers have incorporated voluntary measures such as self-certification or seeking payment information at the time of sign-up to prevent underage users. The following table provides an overview of the existing measures undertaken by companies in India:

[151] Victoria Nash, *et al*. Effective Age Verification Techniques: Lessons to be learnt from the online gambling industry, Final report December 2012-13, Oxford Internet Institute.

[152] Based on stakeholder inputs.

[153] A petition (WP(C)5661/2019) was filed in the Delhi High Court in 2019 demanding a ban on online gaming websites arguing that they are a game of pure chance rather than skill.

Sectors	Relevant Players	Current Measures Comments[154]
E-Mail Accounts	Google, Microsoft, Yahoo	Self-Certification along with semantic analysis.
Online Content[155]	Video-On-Demand: YouTube, Hotstar, Netflix, Amazon Prime Educational Technology: BYJU's, and Khan Academy	None Financial information is sought during sign-up and registration.
Social Networks	Facebook, Snapchat, Twitter	Self-Certification
Online Gaming	Tencent Games, Electronic Arts, Linden Labs	No standard method in place.
Retail & E-Commerce	Amazon, Flipkart	None
Dating Websites	Tinder, Grindr, Happen	Self-Certification along with semantic analysis.
Banking and Finance	Mobile Wallets - Paytm, Mobikwik, Freecharge Unified Payment Interface (UPI): Google Pay[156]	Government IDs
Wearables & IoT Devices	Google Home, Amazon Alexa, Fitbit	None
Online Gambling	–	Not Permitted in India
Pornography	–	Not Permitted in India[157]

Table 8: An overview of voluntary age-verification methods undertaken by companies in India.

As stated in the table above, currently there are no standards in place for protecting children from harm in the online gaming environment. Furthermore, companies engaged in the online gaming industry do not have any standard age-verification methods in place in India apart from requiring users to self-certify their age in some instances. Acknowledging a lack of consistent and effective protection of minors in the online gaming, a standards project has been approved by the IEEE to establish a Guide for Minor Guardianship System for Online Mobile Gaming (IEEE

[154] Based on publicly available information.

[155] 6 out of 10 Parents Do Not Monitor the Content Kids View Online, available at: https://indianexpress.com/article/parenting/family/parents-do-not-monitor-content-kids-view-online-study-5572394/, (last accessed on 29 July 2019).

[156] Minimum age for Google pay is 16; however, users between the ages of 16-18 require parental consent.

[157] Kamlesh Vaswani v Union of India, WP (C) 177/2013, Supreme Court.

2812).[158] This standards project seeks to describe safeguards that strengthen the ability of a parent to monitor their child's participation in online mobile games and also to guide minors participation in online mobile games. The standard currently being developed would be applicable to the design and development of services for a game monitoring system for minors as well as selection of services by the end user.

2. Threshold age for providing consent varies across jurisdictions. For instance, it is 13 in the US, 13-16 in the EU and 18 in South Africa. Lack of harmonisation leads to uncertainty for service providers; therefore, the age of consent must be consistent across legal regimes. Furthermore, setting the age limit at 18 does not take into account the digital realities of our time. An alternative could be having separate categories for children under the age of 13 (requires parental consent), children between 13-18 (consent with parental guidance) and users above the age of 18. In some cases, depending on the service being offered, children between the age of 13-18 may have the option to provide consent. However, the onus must be on the service provider to seek consent in a child-friendly manner by using simple and easy to understand language. Service providers must use age-appropriate and easy to use tools to communicate with children. These tools may include audio prompts, informative graphics, interactive videos and simple language among other things. As such, rather than treating all children under the age of 18 as a homogenous group, more thought needs to be put on their digital behaviour and formulate policies around it. Also, while seeking consent service providers must communicate to the parents as well as children about what personal data is being collected, whether it would be shared with any third party and duration for which the data would be stored.

3. Service providers must adhere to the principles of data minimisation and ensure that only minimum amount of personal data necessary for delivering an individual element of service is collected from the child and it should not exceed the elements of a service that the child requires. This would also require identifying which type of personal data is necessary for rendering a particular service. For instance, in case of an app offering music download service, one element of service could be allowing users to search for tracks they wish to download, while another aspect of service may be to share what individual listeners are hearing to with other users. Since the individual elements of each service vary, the personal data required by the service provider for enabling these services would also vary. Therefore, service providers must only collect personal data which is necessary for delivering specific services.[159] Additionally, upon verification of a user's age, data trail should not be saved and once the purpose for data collection has been fulfilled, the data must be deleted.

4. Age verification methods must be used in addition to educating children and parents about perils of the internet: Age verification methods will not work in isolation since children will find ways to exploit loopholes. Therefore, there is a need to educate children about the risks lurking in the online space and create awareness that these safeguards, in fact, benefit them. Furthermore, parents must also be apprised of the dangers and made aware of the tools available for parental supervision.

5. Parents may be educated about the use of parental controls and how they can utilise a variety of available

[158] P2812 – Guide for Minor Guardianship System for Online Mobile Gaming, IEEE Standards Association, available at: https://standards.ieee.org/project/2812.html, (last accessed on 30 July 2019).

[159] Age Appropriate Design: A Code of Practice for Online Services (Consultation Document), Information Commissioner's Office, available at: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/age-appropriate-design-a-code-of-practice-for-online-services/, (last accessed on 29 July 2019).

tools to monitor screen times, limit internet access to websites safe for children, set passwords which restrict minors' accounts or require passwords to watch content, restrict in app purchases or track their child's location. However, while providing tools enabling parental oversight can be an effective way to mitigate risks faced by children in the online space, children must also be apprised if their online activities are being monitored by their parents. Informing children is necessary to ensure that children's right to privacy is not violated.

6. Age verification methods will aggregate a large amount of user data, and it must be ensured that user privacy is not infringed in the development of solutions, especially in case of children's data. Age verification solutions must, therefore, address issues revolving around data security and ensure that only information necessary to accomplish a purpose is collected from the user. Thus, age verification methods must ensure that the user's right to privacy is not infringed or compromised. Whenever, a service provider contemplates sharing a 'child's data', it must always be in the best interests of the child and due diligence must be undertaken to ensure that such sharing does not put children at a heightened risk of harm. As such, this should mean that children's data should not be shared with third parties unless the service provider has a compelling reason to do so and sufficient regard has been given to the best interests of the child.

7. Service providers must develop apps keeping in mind the age-range of their users and content must be customised keeping in mind the evolving capacity of children belonging to that age group. As such, it is imperative that service providers implement robust age-verification methods which prevent children from accessing age-inappropriate content. However, in case service providers catering primarily to children or more specifically to users under the age of 18 are unable to have effective age-verification tools to identify children from adults or ascertain different age ranges, then additional safeguards must be applied to all users of the services.

8. In addition to creating effective age verification solutions, service providers must also ensure that their app does not 'nudge' children towards a low privacy setting. This could be in the form of a lower privacy setting being more prominent on the user interface or framing the language for a lower privacy setting in a more positive manner or creating additional steps for selecting the lower privacy setting option which effectively means that the service provider is 'nudging' the user to give more personal data. On the contrary service providers can employ 'nudge' techniques to encourage children to make better privacy decisions such as nudges towards high privacy options or wellbeing enhancing behaviour such as limiting screen time or encouraging parental involvement.[160]

9. Age verification measures must not be exclusionary in nature, and due consideration should also be given to creating solutions that are accessible to most of the population. The internet is touted to be the great equaliser of our times and incorporating highly expensive age verification methods or mandating the use of credit cards may trigger users to move to unsafe spaces which have minimal safeguards in place for protecting user data. Therefore, there is a need to develop cost-effective age verification solutions.

[160] Age Appropriate Design: A Code of Practice for Online Services (Consultation Document), Information Commissioner's Office, available at: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/age-appropriate-design-a-code-of-practice-for-online-services/, (last accessed on 30 July 2019).

Children born in the current times are anticipated to lead their lives online. With ever increasing access to the internet and different services and products to choose from minor internet users are likely to be exposed to harm and therefore, acknowledging the need for creating a safer space for children in the digital economy is a step in the right direction. However, due consideration must also be given to minors' internet habits, their digital realities and their right to access the internet. Age-verification methods have the potential to prevent minors from accessing restricted services, but the development of age-verification solutions is still ongoing. Furthermore, in an online world where services span geographical boundaries, the variation in threshold age across countries and identification methods built around local IDs pose significant challenges to age verification solution providers. Age verification as a requirement is inevitable, but the need of the hour is to design clear and common framework that is practical and effective in a digital world sans boundaries.

REFERENCES

Age Appropriate Design: A Code of Practice for Online Services (Consultation Document), Information Commissioner's Office, available at: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/age-appropriate-design-a-code-of-practice-for-online-services/

BBFC, Guidance on Age Verification Arrangements, October 2018, available at https://www.ageverificationregulator.com/assets/bbfc-guidance-on-age-verification-arrangements-october-2018-v2.pdf

Brad Stone, Online Age Verification for Children Brings Privacy Worries, The New York Times (online, 15 November, 2008), available at: https://www.nytimes.com/2008/11/16/business/16ping.html

Central Board of Film Certification Guidelines, available at: https://www.cbfcindia.gov.in/main/guidelines.html

Ceylan Yeginsu, To View Online Porn, First Show Your Papers: U.K. Will Begin Age Checks, The New York Times (online, 19 April, 2019), available at: https://www.nytimes.com/2019/04/19/world/europe/britain-age-checks-pornography.html

Children's Online Privacy Protection Act (COPPA).

DataQuest, 'Almost 50% of Indian Children Admit to Meeting a Stranger they First Met Online, reveals Intel Security study', available at: https://www.dqindia.com/almost-50-of-indian-children-admit-to-meeting-a-stranger-they-first-met-online-reveals-intel-security-study/

Deborah Lupton and Ben Williamson, The Datafied Child: The Dataveillance of Children and Implications for Their Rights, 19(5) New Media & Society (2017).

Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Taskforce to the Multi-State Working Group on Social Networking of State Attorneys General of the United States, 2008.

European Commission, Background Report on Cross Media Rating and Classification of Age Verification Solutions, Safer Internet Forum, 2008.

European Commission - Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/67.

Explained Snippets | Legal drinking age: Mostly 21; 25 in Delhi and four other states, The Indian Express (online, 30 May, 2018), available at: https://indianexpress.com/article/explained/explained-snippets-legal-drinking-age-mostly-21-25-in-delhi-and-four-other-states-5196264/

Federal Trade Commission, 'Self-Regulation in the Alcohol Industry', June 2008.

Francoise Gilbert, Age Verification as a Shield for Minors on the Internet: A Quixotic Search?', 5(2), J. L. Com. & Tech., 2008.

Guidance on Age Verification Arrangements, BBFC, October 2018, available at https://www.ageverificationregulator.com/assets/bbfc-guidance-on-age-verification-arrangements-october-2018-v2.pdf

Holloway, Donell, Green, Lelia and Livingstone, Sonia (2013) Zero to Eight: Young Children and their Internet Use, EU Kids Online, LSE London, available at: http://eprints.lse.ac.uk/52630/

Indian Court Orders Facebook, Google to Offer Plans for Protecting Children, 12 August, 2013, available at: https://www.orfonline.org/article/indian-court-orders-facebook-google-to-offer-plans-for-protecting-children/

Interstate Treaty for the Protection of Minors in the Media.

Jamie Tolentino, Are Your Users Who They Say They Are? How do you know? Future of Communications (online, 30 March, 2015), available at: https://thenextweb.com/future-of-communications/2015/03/30/are-your-users-who-they-say-they-are-how-do-you-know/

Juvenile Justice Act, 2015.

Ley Orgánica de Protección de Datos (LOPD).

More than 80% of Children Lie about their Age to use Sites like Facebook, The Guardian, available at https://www.theguardian.com/media/2013/jul/26/children-lie-age-facebook-asa

Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US footsteps?', 26(2) Information & Communications Technology Law Journal (2017), available at: http://www.tandfonline.com/doi/full/10.1080/13600834. 2017.1321096

Online Age Verification for Our Children, A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives, The Future of Privacy Forum.

Programme and Advertising Codes prescribed under The Cable Television Network Rules, 1994.

Protection of Personal Information (POPI) Act, 2013.

Reserve Bank of India, 'RBI, Opening of Bank Accounts in the Names of Minors', 2014, available at https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=8866&Mode=0

Reserve Bank of India, 'RBI, ATM & Card Statistics for April 2019', 2019 available at https://www.rbi.org.in/Scripts/ATMView.aspx

Sheri Bauman and Tanisha Tatum, Web Sites for Young Children: Gateway to Online Social Networking? 13(1) Professional School Counselling (2009).

Shruti Dhapola, More Kids are Online, but Indian Parents are Finally Taking Stock: Intel Study, The Indian Express (online, 25 December, 2015), available at: https://indianexpress.com/article/technology/tech-news-technology/more-kids-are-online-but-indian-parents-are-finally-taking-stock-intel-study/

6 out of 10 Parents Do Not Monitor the Content Kids View Online, available at: https://indianexpress.com/article/parenting/family/parents-do-not-monitor-content-kids-view-online-study-5572394/

Sonia Livingstone et al., 'One in Three: Internet Governance and Children's Rights', Global Commission on Internet Governance Paper Series No. 22 (November 2015.

Srikrishna Committee Data Protection Report, A Free and Fair Digital Economy, 2018.

Summary of the Digital Economy Act, available at https://services.parliament.uk/bills/2016-17/digitaleconomy.html

The Cigarettes and Other Tobacco Products (Prohibition Of Advertisement And Regulation Of Trade And Commerce, Production, Supply And Distribution) Act, 2003.

The Digital Economy Act, 2017.

The EU General Data Protection Rules (GDPR), 2018.

The Indian Majority Act, 1875.

The Motor Vehicles Act, 1988.

The Personal Data Protection Bill, 2018.

The Protection of Children Online, OECD, 2012.

The United Nations Convention on the Rights of the Child.

This is how Age Verification will Work Under the UK'S Porn Law, available at https://www.wired.co.uk/article/uk-porn-age-verification

Thomas J. Smedinghoff and David A. Wheeler, Addressing the Legal Challenges of Federated Identity Management, Privacy and Security Law, 2008, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1121127

Tinder, Grindr questioned Over Age Verification Requirements after Several Child Abuse Cases, available at https://economictimes.indiatimes.com/magazines/panache/tinder-grindr-questioned-over-age-verification-requirements-after-several-child-abuse-cases/articleshow/67957367.cms

UNICEF, 'Guidelines for Industry on Child Online Protection', 2015.

UNICEF, 'Child Online Protection in India', 2016.

UNICEF, 'Children in a Digital World, 2017.

UNICEF, 'Child Online Protection in India, available at: http://unicef.in/PressReleases/418/UNICEF-India-launches-the-first-comprehensive-report-on-Child-Onl

Victoria Nash, et al. Effective Age Verification Techniques: Lessons to be Learnt from the Online Gambling Industry, Final report December 2012-13, Oxford Internet Institute.

White Paper on Data Protection in India, available at: https://www.meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited

Yoti Age Scan – Public Version, April 2019, available at https://s3-eu-west-1.amazonaws.com/prod.marketing.asset.imgs/yoti-website/Yoti-Age-Scan_Digital.pdf