



Digital Age Assurance Tools and Children's Rights Online across the Globe:

A Discussion Paper



AUTHORS

The discussion paper series on children's rights and business in a digital world is managed by the UNICEF Child Rights and Business Unit. This paper was written by Emma Day.

This paper has benefited from the invaluable contributions of several UNICEF colleagues, including Josianne Galea Baron, Andrew Mawson, Afroz Kaviani Johnson, Daniel Kardefelt-Winther, Erik Nyman, Gabrielle Berman, Keith Woo, Miles Hastie, Sigrun Kaland and Sarah Jacobstein.

Many stakeholders contributed to the discussion paper, including reviewers from the private sector, research institutions and civil society organizations. A special thank-you goes to Dieter Carstensen, Duncan McCann, Fausto Morales, Heather Burns, Iain Corby, Iain Drennan, John Carr, Julie Dawson, Laura Higgins, Megan Langley Grainger, Melissa Stroebel, Milka Pietikainen, Olivier Alais, Sonia Livingstone, Svetlana Smirnova and Victoria Nash for sharing their expertise and inputs.

DISCLAIMER AND COPYRIGHT

This discussion paper is a UNICEF publication. Acknowledgements of company representatives do not imply a company's approval or endorsement of the discussion paper. Any reference made to a specific company does not imply endorsement by UNICEF of the company's policies and practices. This paper does not represent an official UNICEF position on the topic of age assurance tools.

The views expressed in this publication do not necessarily represent the views of UNICEF, and UNICEF makes no representation concerning the source,

originality, accuracy, completeness or reliability of any statement, information, data, finding, interpretation, advice or opinion contained herein.

© United Nations Children's Fund (UNICEF), April 2021

All rights to this publication remain with the United Nations Children's Fund (UNICEF). Any part of the report may be freely reproduced with the appropriate acknowledgement.

ABOUT THIS DISCUSSION PAPER SERIES

As more children around the world spend more time on the Internet in more ways, it becomes increasingly essential to appreciate what children's rights mean in a digital environment. While there is now a widely accepted public imperative to protect children from harm, abuse and violence online, there has been comparatively little consideration of how to empower children as active digital rights-holders. At the same time, the rapidly expanding power and reach of the ICT sector have thrust communications and technology companies into key policy debates on the risks and opportunities children encounter online. This series of discussion papers seeks to explore the relationship between children's rights, business and the Internet in greater detail. The discussion papers address central themes, including children's rights to privacy, freedom of expression, information, education and non-discrimination. While the issues presented are by no means exhaustive, it is hoped that these discussion papers will contribute to broadening the conversation on children's rights and business in a digital world.



Click on section bars to navigate publication

Contents

1	Introduction	5
2	Scope, methodology and limitations	9
3	Approaches to the use of age restrictions to manage exposure to risk	12
4	What age assurance tools are available, and what are their strengths and weaknesses?	15
	4.1 Data sources for age assurance.....	15
	4.2 Automatically generated data	27
	4.3 Tokenized systems.....	30
5	What are the risks to children that age assurance tools might help to mitigate online, and what is the evidence for the harms caused by those risks?	32
	5.1 Gambling	33
	5.2 Pornography	35
	5.3 Online gaming	39
	5.4 Social media	41
	5.5 Child sex abuse materials	43
6	What does the existing regulatory landscape look like with respect to age assurance online?	46
7	Alternatives and complements to age assurance	49
	7.1 Safety by design and privacy by design.....	49
	7.2 Parental controls and supervision.....	50
	7.3 Educational initiatives	50
	7.4 Removing convicted child sex offenders from online spaces.....	51
	7.5 Targeting behaviour rather than age.....	51
8	Summary	52
	8.1 Questions for further discussion and remaining barriers	52
	8.2 Proposed principles for the development and use of age assurance in the context of children’s rights	53

Abbreviations

AADC	Age Appropriate Design Code (of the UK)
AVMSD	Audiovisual Media Services Directive (of the EU)
COPPA	Children’s Online Privacy Protection Act (of the USA)
CRA	credit rating agency
CRC	UN Convention on the Rights of the Child
DPIA	data protection impact assessment
eID	electronic identification
EU	European Union
FTC	Federal Trade Commission (of the US)
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
IWF	Internet Watch Foundation
KYC	know your customer

1. Introduction

1.1 ONLINE PROTECTION AND AGE ASSURANCE

Digital technology has changed the world, and as more and more children go online, it is increasingly changing childhood.¹ As an open space that does not distinguish between its users on any basis, not least their age, the Internet presents risks to which children are especially vulnerable, related to contact, conduct, content and contracts (see Table 1).^{2,3} In recognition of this, and in order to comply with regulations, some websites and apps include age recommendations or restrictions, sometimes as guidance for parents and caregivers regarding the suitability of content or platforms for different age bands, and sometimes as a definitive prohibition on access by children below a specified age.

Age assurance tools draw on diverse data sources to estimate an individual user's age (to varying degrees of accuracy).

Age verification tools are a subset of age assurance tools. They establish a user's age, and even exact date of birth, often by verifying their identity against officially held data.⁴

Policymakers, businesses and advocates around the world are becoming increasingly concerned about online harms against children. One of the solutions being proposed to keep children safer online is the deployment of age assurance tools capable of estimating or verifying the ages of individual users. For example, General Comment No. 25 (2021) of the Committee on the Rights of the Child states that, in order to protect children from economic, sexual and other forms of exploitation in the digital environment, "robust age verification systems should be used to prevent children from acquiring access to products and services that are *illegal* for them to own or use. Such systems should be consistent with data protection and safeguarding requirements" (emphasis added).⁵ As this paper explores, the deployment of age assurance tools is also considered in the context of preventing children from interacting with legal but potentially harmful content or experiences online.

Discussions around the application of age assurance tools are also closely intertwined with industry's responsibility to respect human rights, as outlined in the United Nations Guiding Principles on Business and Human Rights.⁶

- 1 United Nations Children's Fund, *State of the World's Children 2017: Children in a Digital World*, UNICEF, New York, 2017.
- 2 World Wide Web Foundation, *History of the Web*, <www.webfoundation.org> (undated).
- 3 Livingstone, Sonia, E. Lievens and J. Carr, *Handbook for policy makers on the rights of the child in the digital environment*, Council of Europe, Strasbourg, 2020.
- 4 Government Communications Headquarters (GCHQ), Department for Digital, Culture, Media & Sport (DDCMS) and Home Office, *VoCO (Verification of Children Online) Phase 2 Report*, UK Government, London, 2019.
- 5 United Nations Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25.
- 6 United Nations, *Guiding Principles on Business & Human Rights*, <www.business-humanrights.org/en/big-issues/un-guiding-principles-on-business-human-rights/>.

The Children's Rights and Business Principles call on businesses to "meet their responsibility to respect children's rights and to commit to supporting the human rights of children".⁷ Furthermore, following General Comment No. 16 from the Committee on the Rights of the Child, States have obligations regarding the impact of business activities and operations on children's rights.⁸ Increasingly, governments have become interested in the use of technological solutions, including in the form of age assurance tools by companies to better ascertain the age of their users.

Age assurance tools can be applied to prevent child users attempting to access

sites or apps considered unsuitable for their age, or to limit what features or content they are able to access within different platforms on the basis of their age. The use of age assurance tools has also been proposed as a means of ensuring that platforms can comply with data protection laws that require platforms to limit the amount of data collected from children. However, privacy advocates have raised concerns that age assurance tools themselves introduce requirements of data collection from children, thereby generating additional risk.⁹ Table 1 indicates some of the links between categories of risk and how age assurance tools may be relevant to their mitigation or prevention.¹⁰



- 7 United Nations Children's Fund, The Children's Rights and Business Principles, <www.unicef.org/corporate_partners/index_25078.html>.
- 8 United Nations Committee on the Rights of the Child (CRC), General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, 17 April 2013, CRC/C/GC/16.
- 9 Allison, P., 'Politics, privacy and porn: the challenges of age verification technology', *Computer Weekly*, 17 April 2019.
- 10 Definitions are adapted from Livingstone, Sonia and M. Stoilova, *The 4Cs: Classifying Online Risk to Children, (CO:RE Short Report Series on Key Topics)*, Leibniz-Institut für Medienforschung und Hans-Bredow-Institut, Hamburg, 2021.

TABLE 1: Risk categories and relevance of age assurance tools

RISK	DEFINITION	RELEVANCE OF AGE ASSURANCE TOOLS
Content	The child engages with or is exposed to potentially harmful content. This can be violent, gory content, hateful or extremist content, as well as pornographic or sexualized content that may be illegal or harmful, including by being age inappropriate.	Age verification tools can be used to require users to demonstrate that they are 18 or over, to block child users from content that is illegal, and to restrict access to content that is deemed harmful for their viewing.
Contact	The child experiences contact, or is targeted, in a potentially harmful adult-initiated interaction (the adult may or may not be known to the child). This can be related to harassment (including sexual), stalking, hateful behaviour, sexual grooming, sextortion, or the generation or sharing of child sexual abuse material.	Age assurance tools can be used to flag adult users who are interacting with children in a mixed-audience environment, to keep adults out of online environments designed for children, or to keep children out of online environments designed for adults.
Conduct	The child witnesses, participates in, or is a victim of potentially harmful conduct, such as bullying, hateful peer activity, trolling, sexual messaging, pressure or harassment, or is exposed to potentially harmful user communities (e.g. self-harm or eating disorder forums). Typically, conduct risks arise from interactions among peers, although not necessarily of equal status.	Age assurance tools cannot prevent or mitigate harms that occur as a result of interactions between users of the same age groups, but can potentially reduce the risk of younger children being harmed by interactions with much older children.
Contract	The child is party to and/or exploited by potentially harmful contract or commercial interests (gambling, exploitative or age-inappropriate marketing, etc.). This can be mediated by the automated (algorithmic) processing of data.	Data protection legislation in many countries requires companies to ensure they do not collect data from children under the age of 13 (or up to 16, depending on the jurisdiction), without parental consent. Age assurance tools could allow companies to be more certain about the age of their users, putting them in a better position to comply with the law. However, beyond this, the focus on age to determine how well prepared or suited a child is to enter into such contracts could be somewhat arbitrary. Further, the use of age 13 as an upper limit (as in the US and the UK) leaves children aged between 13 and 18 without any special protections. Age assurance may also be relevant in preventing children from exposure to certain forms of digital marketing (e.g. marketing of unhealthy food products).



© UNICEF/JUN040221

While the terms and conditions of online games, social media platforms and dating apps do state that children must be a certain age to use their platforms, these usually only require users to self-declare their age. It has become evident that young children are easily able to pass self-declaration systems, allowing them to access online environments designed for adults or older children.¹¹ Recognizing this challenge, industry and other stakeholders have made efforts to identify best practice and self-regulate.¹²

1.2 THE DEVELOPMENT OF A SAFETY TECH SECTOR

Proposals to make age assurance tools mandatory have come primarily from the UK, the European Union (EU), Australia and China. For example, age verification tools are referenced in the EU Audio Visual Media Services Directive (AVMSD)¹³ and the UK Age Appropriate

Design Code (AADC).¹⁴ In addition, the emerging safety tech sector, within which age assurance tools are developed to assist companies in complying with legislation, is located primarily in these same countries.^{15,16}

Even so, the proposed laws and emerging technologies are likely to have far-reaching effects on children all around the world. While the major apps and platforms used by children globally come predominantly from the US and China, US companies tend to 'level up' their privacy and protection policies to meet European standards, particularly the requirements of the EU General Data Protection Regulation (GDPR).¹⁷ The decisions made by governments in these countries, as well as the age assurance tools developed for these markets, may have far-reaching impacts on children globally, particularly in contexts where identity credentials may be more difficult to prove.

11 Cooney, A., 'The digital age of consent, one year on', LSE Blog, 23 May 2019.

12 For example, see the Safer Social Networking Principles for the EU, 2009. <https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/sn_principles.pdf>

13 European Commission, Protection of minors, Audio-visual Media Services Directive, <<https://ec.europa.eu/digital-single-market/en/protection-minors-avmsd>>.

14 Information Commissioner's Office, *Age Appropriate Design Code: 3. Age appropriate application*, ICO, Wilmslow, Cheshire, 2020.

15 Perspective Economics and University of London, *Safer technology, safer users: The UK as a world-leader in safety tech*, UK Department for Digital, Culture, Media and Sport, London, 2020.

16 UK Department for Digital, Culture, Media & Sport, UK Online Safety Technology Sectoral Analysis and University of East London (undated). <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology_safer_users-The_UK_as_a_world-leader_in_Safety_Tech.pdf>

17 United Nations Children's Fund, 'Towards a global data governance manifesto for children' (forthcoming 2021).

2. Scope, methodology and limitations

The new and emerging subsector of age assurance providers that has sprung up in response to demand from policymakers and companies offers a variety of ways of determining the age of potential users of online platforms. This paper reviews the reasoning behind the restriction of children's access to certain platforms (or features and content within platforms) on the basis of age from a rights-based perspective, and assesses the current capacity of existing age assurance solutions to meet the challenges identified.

This paper focuses primarily on commercial (and predominantly social) platforms that have been the subject of the most attention in respect of child rights and online protection: platforms concerned with gambling, pornography, online gaming and social media. Discussion of more official online platforms (such as those for public health, education and legal services) has been excluded since these platforms generally also ascertain the identity of users, in addition to their age.¹⁸ Other online environments have also been discussed as candidates for the deployment of age assurance tools (e.g. online dating apps),¹⁹ and these merit additional analysis.

The paper begins by describing some of the main age assurance tools that are currently available and considers the data sources they use. It goes on to consider what is known about the online risks to children that age assurance tools are intended to mitigate, and explores the evidence for the harms such risks can cause. The existing regulatory landscape is then reviewed with respect to the use of age assurance tools, including a consideration of alternatives and complements to current age assurance approaches. The paper concludes by posing some remaining questions for further discussion, along with a set of proposed principles for the development of age assurance tools and techniques in the context of children's rights.

While some of the experts interviewed for this paper expressed concerns that age assurance tools could become mandated by governments for use across the entire Internet, consideration of the application of age assurance systems across the worldwide web is beyond the scope of this paper, as is a detailed discussion of proposed standards for age assurance, such as those emerging in the UK²⁰ and the EU.²¹

¹⁸ Social networks do not generally require their users to prove their identity and may become less popular if they did so, and could even be found to breach the public's right to privacy if they required users to provide personal data in order to access communication services.

¹⁹ Lomas, N. 'Dating apps face questions over age checks after report exposes child abuse', *TechCrunch*, 11 February 2019.

²⁰ PAS1296:2018, Online age checking. Provision and use of online age check services. Code of Practice (UK)

²¹ European Union, EU Consent: Electronic identification and trust services for children in Europe: Creating a safer digital world for children throughout the European Union, 2021, <<https://euconsent.eu>>.

2.1 METHODOLOGY

This paper is based on a rapid desk review of available grey literature sourced through Google searches, supplemented by interviews with experts from academia, the private sector and civil society organisations.

It aims to consider the implications of age assurance tools for child users

of platforms around the world, with a significant limitation being that most of the available evidence and research on this topic come from Western countries, with a great deal of the policy debate originating in the UK. It is therefore presented as an initial review of the age assurance system, designed to stimulate discussion from a child rights perspective (see *Table 2*). It does not represent an official UNICEF position on the topic.

TABLE 2: Children’s rights and age assurance tools

CHILDREN’S RIGHTS AND AGE ASSURANCE TOOLS	
Age assurance tools relate to a number of children’s rights under the UN Convention on the Rights of the Child (CRC), including those listed below. This section presents some key principles for applying the CRC to age assurance tools:	
Article 1 age of a child	The CRC defines children as every human being under the age of 18 years unless, under the law applicable to the child, majority is attained earlier. The CRC does not distinguish between ages of children, but does recognize the principle of the child’s evolving capacities (see Article 5 below).
Article 2 non-discrimination	It is important that age assurance processes do not inadvertently discriminate against children who do not have access to official documents, children with developmental delays, children whose ethnicity is not recognized by algorithms used to assess age, or children who do not have parents or caregivers who are able to engage with verification processes that require parental input.
Article 3 best interests of the child	The best interests of the child should be the primary consideration when making decisions regarding the application of age assurance tools.
Article 4 age of a child	The CRC defines children as every human being under the age of 18 years unless, under the law applicable to the child, majority is attained earlier. The CRC does not distinguish between ages of children, but does recognize the principle of the child’s evolving capacities (see Article 5 below).
Article 5 parental guidance and a child’s evolving capacities	Age assurance processes need to respect the rights of parents and caregivers to provide guidance to children on engaging with online platforms, in accordance with the evolving capacity of the child. There is a balance to be met between the parent’s right to decide what is age appropriate for their individual child, and the government’s duty to protect children’s rights. In general, more protective laws should be set at a higher age to ensure maximum protection for children under the law, whereas laws that relate to children gaining autonomy should be set in line with their evolving capacities (see further below). It may be difficult to reconcile age-based restrictions with the concept of the evolving capacities of the child.

CHILDREN'S RIGHTS AND AGE ASSURANCE TOOLS

Age assurance tools relate to a number of children's rights under the UN Convention on the Rights of the Child (CRC), including those listed below.

This section presents some key principles for applying the CRC to age assurance tools:

<p>Article 7 & 8 birth registration, and protection and preservation of identity</p>	<p>Age is an identity attribute, and as national birth registration systems are increasingly digitized, children's date of birth will be recorded in national systems. There is a balance to be struck between promoting children's rights to birth registration and to an identity, and ensuring that the use of this data is regulated effectively to protect children's privacy.</p>
<p>Article 12 respect for the views of the child</p>	<p>Children should be consulted on their views about which platforms are appropriate for them to access, and should have their views taken into account before being denied access to online spaces or content on the basis of their age.</p>
<p>Article 13, 14, 15 & 17 freedom of expression, freedom of thought, freedom of association and access to information</p>	<p>As much of children's lives has moved online, their rights to express themselves, to access information, and to meet with others and join groups should not be unduly restricted on the basis of their age.</p>
<p>Article 16 right to privacy</p>	<p>Most age assurance tools with a high degree of accuracy rely on official data that can easily identify a child. It is important that children's right to privacy is respected as they continue to engage in online spaces, and that they are only identified where strictly necessary to prevent serious harm, and with their consent or the consent of their parents or caregivers.</p>
<p>Article 19 protection from violence, abuse and neglect.</p>	<p>Children have the right to protection from violence online as well as offline, including from cyberbullying and harassment. Because age assurance methods can detect adults who contact children online, they can play a role in tackling harms that are perpetrated by adults against children (or harms perpetrated by older children against much younger children).</p>
<p>Article 28 right to education</p>	<p>Many platforms, including online gaming platforms, provide children with opportunities for learning that should not be unduly restricted on the basis of age, recognizing that the capacity for learning does not always correspond with age, and nor does the ability to cope with risk.</p>
<p>Article 34 sexual exploitation</p>	<p>Children have the right to protection from sexual exploitation online, and governments and platforms must take all measures to mitigate these risks, which may be easier to do if they know the age or age range of their users.</p>
<p>Article 36 other forms of exploitation</p>	<p>Governments must protect children from exploitation of their data by companies. Requiring platforms to take steps to ascertain the age of their user base in order to comply with special data protection laws for children may be one method of accomplishing this. However, it is also important to ensure that age assurance processes respect the data minimization principle, and children's right to privacy.</p>

3. Approaches to the use of age restrictions to manage exposure to risk

3.1 INTRODUCTION

Using age to determine children's exposure to risk online requires a balancing of children's rights against an assessment of the different risks to which they are exposed. All platforms and websites must take into account the ages set by data protection laws and industry age ratings, as well as the implications of age for other risks, such as sexual exploitation or exposure to harmful content.

Article 1 of the CRC defines a child as every human being below the age of 18, unless in a particular State, majority is reached earlier. Setting an age for the acquisition of certain rights or for the loss of certain protections requires a balancing of the concept of the evolving capacities of the child with the State's duty to provide protection.²² Commentators have observed that, across a series of comments, the Committee on the Rights of the Child has advised that minimum ages that are protective should be set "as high as possible", whereas those that relate to the child gaining autonomy demand a more flexible system, sensitive

to the individual needs of the child.²³ In addition, when setting minimum ages, States must take into account the basic principles of the CRC, which include non-discrimination, the best interests of the child, the right to life and maximum survival and development, and respect for the child's evolving capacities.²⁴

3.2 DIGITAL AGE OF CONSENT

Many platforms have set the minimum age of their users in line with data protection laws. Because most of the platforms that are used by children globally are based in either the US or Europe, the minimum ages of consent (i.e., the digital age of consent) to data collection set by US and EU laws have come to dominate globally. The first data protection law to set a digital age of consent for users was the Children's Online Privacy Protection Act (COPPA) in the US, which set the minimum age at 13. The Federal Trade Commission explains that age 13 was chosen in recognition that younger children are particularly vulnerable to targeting by marketers and may not understand the safety and privacy issues

²² United Nations Children's Fund, *Implementation Handbook for the Convention on the Rights of the Child: Fully Revised Third Edition*. UNICEF, New York, 2007. See also Lansdown, G., *Innocenti Insight: The Evolving Capacities of the Child*, UNICEF Innocenti Research Centre and Save the Children Sweden, 2005.

²³ Ibid.

²⁴ Ibid.



created by the online collection of personal information.²⁵ More recently, in Europe, the GDPR set the digital age of consent at 16, with an option for States to lower this to age 13. The EU requires any company doing business in the EU or using EU data subjects to comply with the GDPR, which has meant that its principles have been adopted far beyond Europe.

Given that data protection laws are designed to protect children from commercial exploitation, it can be argued that age 13 is not, in the words of the Committee on the Rights of the Child, “as high as possible”. This is partly because, in most countries, the minimum age for entering into a contract is 18. Moreover, even many adults have difficulty in understanding the implications of sharing their personal data digitally. General Comment 25 states that ‘States parties should prohibit by law the profiling or targeting of children *of any age* for commercial purposes’ (emphasis added).²⁶

Social media companies, for example, usually set their terms of service in relation to data protection laws, such that they may collect all users’ data without parental consent. Consequently, minimum ages are usually set at between 13 and 16, although users are not generally required to provide proof of their age. One reason given for keeping the minimum age for access to platforms (including social media platforms) at 13 is that if the age were set higher, for example 16 or 18, companies would simply exclude children from accessing their

platforms until they reach the age of consent in order to avoid the cost of differentiating between users with regard to data collection. However, the high market value of child users of technology could mean that these costs may not result in exclusion.²⁷ While it is difficult to predict how individual platforms would respond to changes in minimum age requirements, there have been recent moves by platforms to invest in systems to differentiate the ages of their users.²⁸

3.3 AGE RATINGS

Age ratings are also used for online games and online films, usually on the basis of their containing sexual or violent content that is not illegal, but considered inappropriate for younger age groups. Ratings are generally provided as guidance for parents, rather than enforced. Accessing content that is not illegal yet is possibly harmful to children arguably relates to the child’s evolving capacity. Therefore, following the reasoning of the Committee on the Rights of the Child referenced above, this would call for a more flexible system that is sensitive to the individual needs of the child, as opposed to pre-determined cut-off ages.

Age ratings for online games vary globally: individual game developers usually define age limits within their terms of service. However, Google and Apple app stores may apply a different rating to the same games. The PEGI age-rating system is used in over 30 countries across Europe as a guide for parents, and companies selling offline games in the UK are required

25 Federal Trade Commission, ‘Complying with COPPA: Frequently asked questions’, <www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0>.

26 United Nations Committee on the Rights of the Child, General Comment No. 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25.

27 SuperAwesome, ‘Kids Digital Media Report: Kids digital advertising market will be \$1.7bn by 2021’, 11 June 2019.

28 The YouTube Team, Using Technology to More Consistently Apply Age Restrictions, YouTube Official Blog, 22 September, 2020.

by law to abide by the PEGI ratings.²⁹ The International Age Rating Coalition offers a service to game developers to help them assess the applicable age ratings for their games in different countries.³⁰

Most platforms have a general idea of the age range of users for whom they designed their services, and because advertising is integrated into so many platforms and games, they have a business interest in knowing as much as possible about their

users, including their age, for marketing purposes. Platforms can ascertain the age and other characteristics of their user base through market research, or by drawing inferences from user behaviour. However, difficulties may arise when services designed with adults in mind are in practice attractive to and used by children. The following sections explore the different age assurance tools that are currently available, and examine the data sources they rely on.

Determining the likely age of a platform's user base: the UK government VoCO study

In 2020, the Verification of Children Online (VoCO) research study was carried out by the UK government. The study included consultations with children, parents and industry. It proposed that online platforms should adopt a risk-based approach to age verification, in which companies would establish the likelihood of children accessing their platform and the risks associated with that access, before choosing an age assurance method that would provide a sufficient level of certainty proportionate to the identified risk.

The study proposed that the level of risk to children could be assessed according to the:

- platform architecture and design (including processing of personal data)
- platform operation (including moderation)
- nature of content shared on the platform
- makeup and behaviour of its user base.

The VoCO study emphasized that platforms' intended user base is likely to be different from its actual user base, because self-declaration of age by users leads to many children claiming to be older than they are in order to obtain access. The authors proposed that this risk could be assessed through a combination of self-assessment and external independent assessments, with the latter based on the UK AADC, which applies to information society services directed at children in the UK and which involves:

- conducting independent surveys of platform users (although the study does not say how accurate responses from children would be collected, in respect of whether they are truthful about giving their age online)
- assessing common platform features against likely target audience. (It is not clear from the study whether these would include internal platform-specific measures or more typical, platform-agnostic market research).
- transparency reporting from the platform, including advertising metrics where age is a factor.

29 VSC Rating Board, <<https://videostandards.org.uk/RatingBoard/about-history>>.

30 International Age Rating Coalition <www.globalratings.com/>.

31 Government Communications Headquarters, Department for Digital, Culture, Media & Sport and Home Office, *VoCO (Verification of Children Online) Phase 2 Report*, UK Government, London, 2019.

32 The AADC defines 'information society services' as "apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news or educational websites and websites offering other goods or services to users over the internet." Information Commissioner's Office, Age appropriate design code: services covered by this code, <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/>>.

4. What age assurance tools are available, and what are their strengths and weaknesses?

There are many different types of age assurance tools available, some of which determine that the user is not an adult (i.e. is under 18), and some of which attempt to identify either the age range within which the child falls, or the exact age of the child. This section reviews the different data sources used by age assurance tools, and the implications of each for both their effectiveness in addressing some of the risks to children online identified above, and their implications for children's rights.

4.1 DATA SOURCES FOR AGE ASSURANCE

One of the main concerns with age assurance tools from a child rights perspective is that they all in one way or another process data in order to verify or estimate the age of users. Privacy experts have expressed concerns that beyond children's rights, age assurance tools require data collection from all users, including adults, in order to determine which users are children,

and may therefore infringe the privacy rights of adults as well. To varying degrees, many such tools also leave a trail of data or metadata behind them, including of children's online activity.³³ In an era in which data protection laws now discourage data collection from children wherever possible, some age assurance tools may go against this principle. This tension is especially relevant where such tools are used to assist platforms in complying with data protection laws.

The main potential sources of data for age assurance tools are: State- or government-provided (either centralized or decentralized) data; user-provided; and automatically generated data.³⁴ Tokenized systems can be used with all of these data sources to provide details about the child's age, while protecting the child's identity. Using this categorization by data source, the following section reviews the different technology tools available, the data sources on which they rely, and the potential child rights issues each one raises.

³³ Interview with expert for this paper.

³⁴ Government Communications Headquarters, Department for Digital, Culture, Media & Sport and Home Office, *VoCO (Verification of Children Online) Phase 2 Report*, UK Government, London, 2019.

State- or government-provided data sources

TOOLS THAT PROVE A USER IS AN ADULT AND NOT A CHILD

Strengths	Weaknesses
No data collection needed from children	Requires adults to provide potentially sensitive data
High degree of certainty	Adult users who do not have access to an official ID to prove they are not a child may be excluded from platforms
	Child could obtain and use an adult's ID to circumvent certain methods of age assurance
	Can prove an adult is over 18, but cannot distinguish between ages of children (i.e. only applicable for enforcement of a cut-off at 18)

Age verification tools³⁵ that draw on official data are used to determine whether a user is over the age of 18 and thus to exclude children from platforms designed for adults. These tools usually rely on data sources such as passports and credit rating agencies. Age verification provides a high level of certainty about people for whom this official data is available. 'Within-record' age verification (such as a passport) reflects the age of the person in the document. However, certainty as to whether the user attempting to access the platform is the same individual as the ID holder varies widely depending on whether biometrics have been used, or whether the child has access to an adult's credit card details or other official documents.

Relying solely on this kind of data risks excluding an estimated 1 billion people globally who do not have any legally recognized form of ID, for example adults who do not have passports, a drivers' licences or bank account.³⁶ This is a concern for platforms based in more developed

countries that also have users worldwide, some of whom live in jurisdictions where they cannot easily access any official ID, leading to their exclusion.

In a study of effective age verification techniques in the gambling industry, it was found that Denmark and Spain operate age verification systems that work well in the context of gambling because their regulators allow gambling operators to access the national electronic identity (eID) database to verify identity details. By contrast, many countries do not have a national eID database and so cannot provide the same level of accuracy. There would need to be strong privacy and security measures in place before allowing private companies access to information from a national identity database. It has also been noted that Denmark's reliance on a single centralized database of information may make it more vulnerable to attack than eID systems that are backed by decentralized and more diverse data sources.³⁷

³⁵ Age verification tools are a subset of age assurance tools. They establish a user's age, and even exact date of birth, often by verifying their identity against officially held data.

³⁶ McKinsey Global Institute, *Digital identification: a key to inclusive growth*, McKinsey Report, 17 April 2019.

³⁷ Nash, Victoria, R. O'Connell, B. Zevenbergen and A. Mishkin, *Effective age verification techniques: Lessons to be learnt from the online gambling industry*, Oxford Internet Institute, Oxford, 2013.

TOOLS THAT PROVE THE EXACT AGE OR DATE OF BIRTH OF THE CHILD USER

Strengths	Weaknesses
Where digital identities exist, it is possible for age attributes to be tokenized, providing a high degree of certainty regarding the child's age without exposing their identity	The long-term implications of digital identities being provided to children are not yet known
	Caution is required in relation to eID schemes that rely on biometric information

Age verification tools are relatively effective at excluding children from platforms designed for adults aged 18 or over where they use data obtained from official datasets that reflect the exact age of the user.³⁸ The official datasets used by age verification tools are not, however, very good at determining the specific age of most children under 18 because children are less likely to be featured in these kinds of datasets.³⁹ This indicates that they would likely not be suited, for example, for ascertaining the age of children under the age of 13 using social media platforms, or for ascertaining the age of children under the age of 15 or 16 using certain video games.

Most governments around the world collect official data in relation to children's health, education and welfare. However, there are important ethical and legal considerations in relation to access to and reuse of children's data that was provided with their consent or with parental consent for one purpose such as education, if that is then to be accessed for the purposes of age verification. In Europe, because sensitive education and health data from children is likely to be collected in most

countries on the basis of either consent or a legal requirement, no further processing is permitted beyond the original consent or provisions of the law under the GDPR. This means that new consent would likely be required from the child or a parent to use this data for age verification purposes, or there would need to be a new legal basis that authorized its reuse.⁴⁰

The European Commission recently proposed a new EU Data Governance Act,⁴¹ which sets out rules related to the reuse of public-sector data, and imposes obligations on data intermediary services. While this law applies to the EU, it is important for companies providing age verification services outside the EU to maintain the highest standards of data protection for all of their users, even where they are not legally required to do so, to ensure that children living in countries with less developed legal systems are not afforded a lower standard of rights protection.

Data collected as part of a national eID system could perhaps be more easily used for age verification. This is because the

³⁸ Ibid.

³⁹ Ibid.

⁴⁰ European Commission, *Can we use data for another purpose?* European Union (undated).

⁴¹ European Commission, Proposal for a Regulation on European data governance (Data Governance Act), 25 November 2020.



© UNICEF/UN0143516/PRINSLOO

consent would have been given to collect data for identification purposes, and date of birth is an identity attribute. The digital identity market is predicted to be worth US\$33 billion globally by 2025.⁴² The EU is reportedly planning to announce the establishment of an EU-wide interoperable digital ID system in 2021,⁴³ designed to give people control over their online identity and data and to enable access to cross-border digital services. It is not yet clear whether this will include children's data. The European Commission is also funding a project beginning in March 2021, EU Consent, "to demonstrate an interoperable technical infrastructure dedicated to the implementation of child protection mechanisms (such as age verification) and parental consent mechanisms as required by relevant Union legislation (such as the AVMSD and the

GDPR".⁴⁴ Alongside age verification, the technical implementation of verified parental consent is also challenging for many companies, especially for those with global reach.

Increasingly, governments are digitizing birth registration, giving babies a digital identity from the moment of birth. In Uganda, birth registration rates have increased due to increasing birth registration by mobile phone, and in Uruguay newborns have received birth certificates before they even leave the hospital due to web-enabled birth registration.⁴⁵ Malawi has developed a national eID system with the help of the United Nations Development Programme. The project registered 9.1 million citizens in 180 days with their biometric attributes.⁴⁶

42 Burt, C., 'Digital identity market to reach \$33B in 2025, Malaysia plans biometric national online ID system', Biometric Update.Com, 27 July 2020.

43 Burt, C., 'EU leaders to propose regional digital ID system rules and funding by mid-2021', Biometric Update.Com, 10 September 2020.

44 European Union, EU Consent: Electronic Identification and Trust Services for Children in Europe, <www.euCONSENT.eu>.

45 Plan International, Identifying and addressing risks to children in digitised birth registration systems: a step-by-step guide', Plan International UK, Woking, Surrey, 2015.

46 Hersey, F., 'How Malawi established a biometric national ID system at breakneck speed', Biometric Update.Com, 12 October 2020.

Biometric data

Although it is possible to be given a digital proof of age from the attributes held by a government eID system without applying any biometrics, governments are increasingly using biometrics as part of their national ID systems.⁴⁷ Biometrics collected include fingerprints, iris scans, palm prints and DNA.⁴⁸ Some researchers report that biometric ID cards have been linked to increased government surveillance of citizens in many countries around the world.⁴⁹ Because biometric data is based on data generated from the unique characteristics of humans, it can be used to track and profile people across their lives, which carries unknown in the long term.⁵⁰ Without strict safeguards in place and strong legal frameworks (such as the GDPR which bans profiling of children), biometric IDs can be used to facilitate discrimination, profiling and mass surveillance.⁵¹ Biometric technologies pose specific risks to children because although

they have the potential to strengthen identity management systems, they can also potentially disrupt and lock in the identities of children from a much younger age, including aspects of their identity such as gender.⁵² The implications of tracking and surveillance are heightened for children, given their greater exposure over the life course.

In addition, there are significant risks of exclusion in relation to the use of biometrics for identification of children. Children may have difficulties in accessing the initial ID needed to secure their biometric ID, and there are limitations to the capability of biometrics to register people with certain characteristics due to algorithms being less accurate for certain skin tones, ethnicities, genders and children with certain disabilities. Biometric IDs may also need to be reissued periodically according to physiological changes in the child as they get older.⁵³

Centralized data sources

TOOLS THAT PROVE A USER IS AN ADULT AND NOT A CHILD

Strengths	Weaknesses
No data collection is needed from children	Requires adults to provide potentially sensitive data
Good degree of certainty	Exposes adults to the risk of potentially catastrophic data breaches, exposing many kinds of their personal data

47 Electronic Frontier Foundation, Mandatory National IDs and Biometric Databases (undated).

48 Ibid.

49 Pascu, L., 'Comparitech analyzes government use of biometrics, surveillance and data sharing', Biometric Update.Com, 17 October 2019.

50 Privacy International, *Biometrics* (undated), <<https://privacyinternational.org/learn/biometrics>>.

51 Ibid.

52 United Nations Children's Fund, *Faces, Fingerprints & Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes*, UNICEF, New York, July 2019.

53 Ibid.

Centralized data sources collect different datasets from different sources and put them together in one location. Age verification tools that use centralized data sources often connect to large data aggregators and credit rating agencies such as Experian and Equifax.⁵⁴ According to the Electronic Privacy Information Center, such aggregators pose privacy and security concerns to users who (i) may not want their data and identity associated with the sites they visit online, such as pornography or medical and personal services platforms, and (ii) are distrustful about the security of their personal information.⁵⁵ For example, Equifax was the subject of a data breach in 2017, resulting in the theft of personally identifying data of hundreds of millions of Americans.⁵⁶

It is technically possible to create a firewall between personal identity and age verification, and platforms do not need to know any identity details when verifying age. This can also be achieved using age assurance tools, which can discard

personal data or disconnect it from their age verification records. For example, age attributes can be tokenized anonymously. However, there would need to be robust oversight mechanisms in place to ensure this kind of system was properly implemented.

In comparison with decentralized systems, centralized data systems carry a greater risk of catastrophic population-level security breaches, and of several different data points being part of a single breach. As such, they carry more profound data privacy risks for children. However, centralized data systems are less likely to contain children’s data (due to the type of data collected on adults that is stored centrally and the uses to which it is put). They are also more likely to benefit from more resources to address security risks than smaller decentralized systems. As such, they may be less likely to experience a breach. Trusted safety frameworks and oversight mechanisms are important whether the data is stored in a centralized or decentralized system.⁵⁷

Decentralized data sources

TOOLS THAT PROVE A USER IS AN ADULT AND NOT A CHILD

Strengths	Weaknesses
No data collection is needed from children	Requires adults to provide potentially sensitive data
Good degree of certainty	Exposes adults to potential data breaches, albeit not as large scale as centralized data systems might

54 Nash, Victoria and O’Connell, Rachel and Zevenbergen, Bendert and Mishkin, Allison, *Effective Age Verification Techniques: Lessons to Be Learnt from the Online Gambling Industry* (December 2012-December 2013). Available at SSRN: <https://ssrn.com/abstract=2658038>

55 Electronic Privacy Information Center, *Equifax Data Breach* (undated), <<https://epic.org/privacy/data-breach/equifax/>>; Information Commissioner’s Office, *ICO takes enforcement action against Experian after data broking investigation*, 27 October 2020 <<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/>>.

56 Fruhlinger, J., *Equifax data breach FAQ: What happened, who was affected, what was the impact?*, CSO Online, 12 February 2020.

57 Australia eSafety Commissioner, *Inquiry into age verification for online wagering and online pornography*, Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs, November 2019.



© UNICEF/UN0368708/AL-SAFADI

Decentralized data sources draw on different datasets that are stored separately. This works better for national identity systems than centralized systems because if there is a data breach of one of the datasets, it will only expose a portion of identifying data rather than complete identifying data for individuals or the entire population. A study of effective age verification techniques in the gambling industry found that the UK provides a good example of an integrated

system of age verification providers because it has the benefit of a range of data aggregators and credit reference agencies (CRAs) that reportedly cover up to 90 per cent of the adult population, and so does not rely on one centralized database.⁵⁸ While the proliferation of data collection agencies may not always be an unmitigated good, it does make it possible to mitigate the risk of catastrophic breaches associated with centralized systems.

BLOCKCHAIN AND SELF-SOVEREIGN IDENTITIES TO PROVE THE EXACT AGE OR AGE RANGE OF THE USER

Strengths	Weaknesses
The user retains control and so the child could divulge their age range or their specific age as needed without exposing any other data	This is still an evolving and contested area and many questions related to governance remain

58 Nash, Victoria et al., Effective age verification techniques, 2013.

Blockchain is a decentralized, distributed and sometimes public digital ledger. Individual records, called blocks, are linked together in a chain, which is used to record transactions. Each transaction added to a blockchain is validated by multiple computers in a decentralized network. Transactions are permanently recorded and are very difficult to alter.⁵⁹

Decentralized data systems based on blockchain or other distributed ledger technologies enable age verification systems that are reportedly outside the control of governments or private companies, and provide the user with

more control over their own data.⁶⁰ Self-sovereign identities (SSIs) are closely linked to blockchain technology and have been proposed as a way of giving individuals control and ownership of their own identity information.⁶¹ In an SSI system, the private keys to identity credentials such as age or date of birth are held by the user – in this case a child or their parent – and not by a centralised issuing authority.⁶² However, SSI is still a contested area, both in terms of what the technology can and should involve, and how it should be governed.⁶³ As such, this remains a relatively theoretical option.

User-provided data: Official documents

TOOLS THAT SCAN OFFICIAL DOCUMENTS	
Strengths	Weaknesses
Because the child provides the copy of their ID themselves, there is no record of their query kept with any government ID offices	Many children do not have an official ID
	Children may use the ID of someone who is old enough to access the platform they wish to use
	Because these tools do not query official databases, it is possible to circumvent the scan using falsified documents
	Scanning official documents presents a security risk in relation to data intercepted in motion or a security breach of the company's data-storage or processing database

59 TechTerms, Blockchain Definition, <<https://techterms.com/definition/blockchain>>.

60 PWC, *Blockchain and Digital Identity: the path to Sovereign Identity, P* (undated presentation), <www.pwc.com/it/it/publications/assets/docs/blockchain-and-digital-identity.pdf>.

61 Cheeseman, M., 'Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity', *Geopolitics*, Taylor & Francis Online, 4 October 2020.

62 Ibid.

63 Ibid.

Copies of official documents (such as a passport, driving licence or other form of official ID) can be provided by the user and uploaded to the age verification provider's platform. Depending on the technology used, this can provide a similar level of proof as a customer showing their ID in a shop. It can also be almost as certain as a system that checks the ID provided against an official database to ensure its authenticity⁶⁴.

User-provided documents for the purposes of age verification fall into a system of low-, medium- or high levels of confidence in their accuracy. A low level of confidence would be obtained from showing an image of the ID on a webcam; a medium level of confidence would require the machine-readable zone of data on the ID to be captured and checked to ensure consistency with the claimed date of birth; and a high

level of confidence would require using a smartphone to read the Near Field Communication chip in the document and to confirm that the data is consistent and that the biometric details (facial image) match.⁶⁵ In Belgium, Denmark and Spain, children have national ID cards from the age of 12 and will soon also have electronic identities.⁶⁶ However, many children around the world do not have photo ID documents, or even have their births registered, especially in low income households where children do not have passports, or in countries where photo ID is not widely used.

Similarly, credit card data can be used to verify that a user is over 18, and to the extent that apps are used, app stores make this a very widely used mechanism for parental consent or age verification, although it is possible for a child to obtain an adult's credit card for this purpose.

User-provided data: Self-declared data

AGE ASSURANCE METHODS THAT ASK USERS FOR THEIR AGE	
Strengths	Weaknesses
Child does not have to give away any identifiable data	Quite easy for children to give a different age if they know this is required to access a platform
Less expensive for platforms	May not be sufficient to comply with GDPR requirements of 'reasonable efforts' to verify the age of the users

⁶⁴ Interview with expert for this paper.

⁶⁵ Interview with expert for this paper.

⁶⁶ Nash, Victoria et al., *Effective age verification techniques*, 2013.



© UNICEF/JUN1306750/WILANDER

Rather than requesting official data, many websites and platforms simply require the user to provide their self-declared data such as name, email address and date of birth. The European data protection working party has advised that self-declaration is not sufficient as proof of the age of users of platforms. It advises that it is an implicit requirement of the GDPR that companies should undertake reasonable efforts to verify the age of their users, and that if a child gives consent while not old enough to provide valid consent on their own behalf, this would render data processing unlawful.⁶⁷ They also caution

that age verification should not lead to excessive data processing, and that the mechanism chosen to verify the age of the data subject should be relative to the risk of the proposed processing.⁶⁸

In the US, COPPA allows for self-declaration of age as a sufficient mechanism for assessing the age of users of social media. However, this may be revised, as the Federal Trade Commission (FTC) has recently requested public comment on COPPA, including comments related to age screening.⁶⁹

Biometric data for age verification

TOOLS THAT DETERMINE EXACT AGE ACCORDING TO BIOMETRIC IDENTITY

Strengths	Weaknesses
Biometrics tend to be accurate in relation to adults and so could prove a user is not a child with a relatively high degree of certainty	May be highly privacy invasive for children
Fewer barriers to access than official ID	The use of biometrics for children is still an evolving area and the technology is not yet perfect

67 Article 29 Data Protection Working Party Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017 (17/EN, WP259 rev.01).

68 Ibid.

69 Federal Register, Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule: A Proposed Rule by the Federal Trade Commission on 07/25/2019. <<https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online>>

Some age verification tools are linked to the user's biometric identity and require the user to provide their thumbprint or a face scan to identify them prior to using the platform. Two biometric models are currently being researched for age prediction purposes: unimodal biometrics systems that rely on one biometric feature, and multi-modal biometric systems that combine two or more biometric features.⁷⁰

The use of biometrics is presented as a solution to age verification in countries where children rarely have access to identity documentation,⁷¹ predominantly in the Global South. However, although using biometrics may increase efficiency and allow essential services to be delivered more quickly, there is a need to be mindful of the data security and privacy risks associated with biometrics, especially in countries with, for example, less developed legal systems.⁷² It is imperative that children's access to identity globally is considered holistically, using a rights-based approach that considers all of the children's rights affected. From this perspective, the focus would be on strengthening national ID systems for children and ensuring that

they have access to a data-minimizing and protective ID system for a range of purposes, including access to services.

Set against these concerns is the fact that the capacity to collect biometric information from children is developing rapidly, with innovations now able to capture the fingerprints of newborns.⁷³ UNICEF has produced guidance on assessing the value of including biometric technologies for child rights programmes. Its guidance outlines a need to balance privacy protections against the benefits of data collection, and expresses caution in relation to the accuracy of various models and their implications.⁷⁴ In the EU, the GDPR requires companies to carry out a data protection impact assessment (DPIA) before any data processing that is likely to result in a high risk to the rights and freedoms of individuals – this would apply in the context of collecting biometric information from children. As of March 2020, the Australian government did not recommend using the facial recognition tools being developed by Home Affairs, because the legislation behind the national facial verification database did not include sufficient measures to protect the public's privacy and security.⁷⁵

Biometric data for age assurance

TOOLS THAT USE BIOMETRIC DATA TO ESTIMATE THE AGE OF THE CHILD

Strengths	Weaknesses
The child's biometric data may be deleted once it has been used to estimate their age	Using biometrics to estimate the age of children is associated with a margin of error (which is greater in the case of younger children)
Existing tools are reportedly accurate enough to identify an age band into which the child falls	Algorithms are known to be problematic when used on children whose datasets do not feature in the training data used
	Biometric data is sensitive and carries additional privacy risks

70 Ibid.


71 Ibid.

72 United Nations Children's Fund, *Faces, Fingerprints & Feet*, 2019.

73 KidPrint <<http://kidprint.ucsd.edu>>.

74 United Nations Children's Fund, *Faces, Fingerprints & Feet*, 2019.

75 Taylor, J., 'Porn, public transport and other dubious justifications for using facial recognition software', *The Guardian*, 16 November 2019.



Some age assurance providers collect biometric data from children using technology that scans the child's face and estimates their age based on an algorithm, rather than attempting to identify the child. One provider explained that it does not store biometric data, but uses a hashed numbering system that allows data for a specific user to be deleted, and does not allow a specific user's identity to be recreated from stored data.⁷⁶ This method estimates the child to be within a certain age bracket, with a margin of error that differs depending on the age of the child. Accuracy is lower for children below the age of 13 due to difficulties in obtaining training data to perfect the algorithms for use on younger children. The margin of error is significant because the determination of whether a child is above or below the age at which parental consent for data collection is required has legal consequences.⁷⁷ If the user is incorrectly flagged as being younger, they are provided with the opportunity to correct this by showing an official form of ID. Such approaches may provide a buffer to keep very young children out of online spaces meant for adults. For example, children assessed as being aged under 12 would not be allowed in spaces designed for over-16s. This is a good outcome for those children whose age is correctly estimated, but could risk marginalizing children who do not fit the norms used by the algorithm to determine age, and who also do not have access to official ID.

Ethical questions in relation to algorithm training sets

There are potential ethical issues related to the training of algorithms to assess the age of children, as the only way to improve this technology is to input as many different children's faces as possible, so that the program can become better at assessing age across different ethnicities and contexts. This raises issues related to obtaining consent from children or their parents to use their biometric data for training purposes. The provider Yoti is currently attempting to address some of these issues through the use of volunteers as part of the UK Information Commissioner's Office regulatory sandbox initiative.⁷⁸

Where the composition of algorithm training sets does not fully represent populations, but is nonetheless applied to all, the resulting algorithm is likely to be inaccurate. However, there may be reasons why some excluded groups do not want to provide their data for use in training sets, due to mistrust of governments and companies, for example. If the accuracy of facial recognition technology does not improve, children with darker skin tones could face discrimination as a result of systems that are currently better at recognizing lighter skin.⁷⁹

⁷⁶ Yoti, White paper: Yoti age scan – public version, Yoti, London, 2020.

⁷⁷ Ibid.

⁷⁸ Information Commissioner's Office, Current projects: Yoti <<https://ico.org.uk/for-organisations/regulatory-sandbox/current-projects#yoti>>.

⁷⁹ Holzer, B., 'The Best Algorithms Struggle to Recognize Black Faces Equally', *Wired*, 22 July 2019.

Some age assurance providers request the consent of users (and their parent or caregiver in the case of younger children) to use their biometric data to train their age estimation algorithms. Prominent privacy advocates have argued that ‘legitimate interests’ is not a sufficient basis on which to reuse this kind of highly sensitive biometric data, and argue that users should be invited to expressly opt in to this kind of data reuse, rather than being required to opt out.⁸⁰ Where users are requested to opt in, it is necessary for the terms and conditions to be clear and jargon-free, so that children have a complete understanding of what they are opting into, and what any related risks could be.

Despite significant investment, age estimation of children is an imperfect science, especially in the context of unaccompanied minors seeking asylum, and in forensics.⁸¹ The leading text on the science of age assessment⁸² notes that age is a significant factor in how people are treated in criminal law, by social

services and by asylum and immigration law.⁸³ In 2009, the UK Supreme Court ruled that where the question of a person’s age arises, it is ultimately to be determined by a court, because where official documentation is lacking, professional opinion must be relied upon.⁸⁴ The text goes on to warn that formal age evaluation must never be put in the hands of the inexperienced practitioner, and the expertise of a forensic specialist and a multidisciplinary team is essential.⁸⁵ The best measures, such as radiological examination, are often impractically intrusive, and calculating age osteologically in relation to bone length and dental development can yield different results, which means an examination of multiple bones must be conducted. Even this only generates at best an approximation of age.⁸⁶ This suggests that the application of digital tools to high-stakes situations, including technologies initially developed for online age assurance purposes, may pose additional risks of inaccuracy.

4.2 AUTOMATICALLY GENERATED DATA

AGE ASSURANCE TOOLS BASED ON CHILD’S USAGE

Strengths	Weaknesses
Circumvents the risk of excluding children without access to official documentation	Digital footprints are not always accurate
	Inherently invasive because it profiles a child’s Internet usage, which may not always be lawful, and it could legitimate further data collection

80 Privacy International, *The Identity Gatekeepers and the Future of Digital Identity*, (updated), 7 October 2020.

81 Black, S., A. Aggrawal and J. Payne-Jones, *Age Estimation in the Living: The Practitioners’ Guide*, John Wiley & Sons, 2010.

82 Age assessment is the term used to describe age estimation in asylum and refugee law.

83 Ibid.

84 R(A) v Croydon London Borough Council [2009] UKSC 8, [2009] 1 WLR 2557.

85 Black, S. et al., *Age Estimation in the Living*, 2010.

86 Ortner, Donald J. and W. Putschar, *Identification of Pathological Conditions in Human Skeletal Remains*, Smithsonian Institution Press, 1981; Stewart, T.D, *Essentials of Forensic Anthropology*, Charles C. Thomas, 1979.



© UNICEF/UN046200/KLJAJO

Several large global platforms have become brokers of digital identities based on personal digital footprints, although these identities may not be entirely accurate and hence are referred to as being 'unverified'.⁸⁷ These platforms monitor users' likes, the pages they follow and the friends they interact with over time, so compiling a user profile that indicates the subject's likely political preferences, personal interests and age range. Data brokers also buy information from multiple platforms and collate data related to individual users.

Owing to a general lack of transparency in the industry, the extent of data collected on children by these platforms is unknown, although in some jurisdictions, data cannot legally be collected from children aged under 13 (or up to 16

depending on the country) without parental consent. It is certainly possible that these user profiles can be fairly accurate, including by triangulating data from different sources.⁸⁸ However, one of the largest data brokers in the world reportedly concedes that around 30 per cent of the data it holds on each profile is incorrect, which is a significant margin of error.⁸⁹

There are ethical issues involved in using digital footprints, depending on the sources of information the platform uses, and whether these sources are in the public domain. Where data related to the child's identity does not come from the public domain, it is imperative that the child or their parent has given meaningful consent for the use of their data for the specific purpose of age assurance.

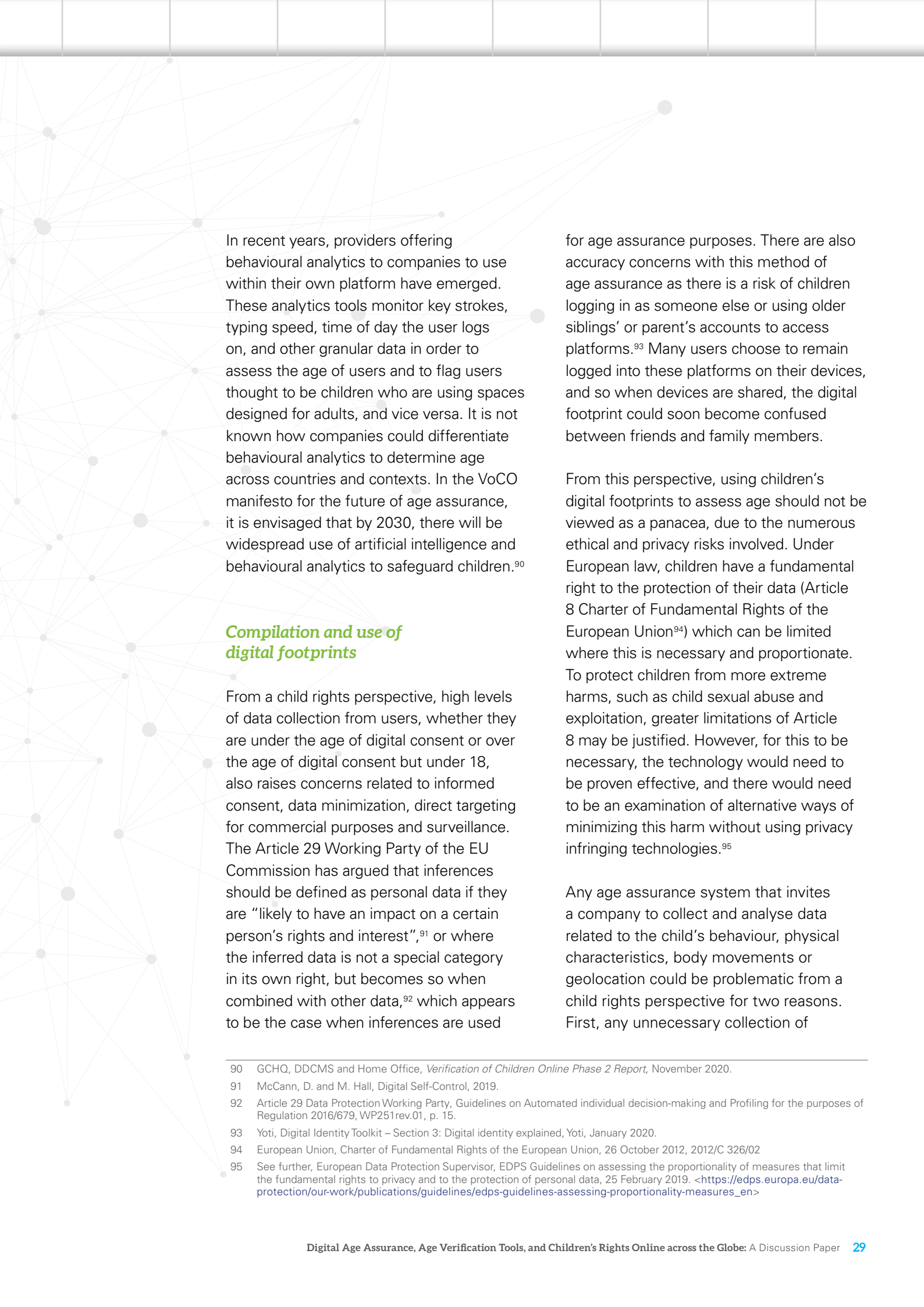
AGE ASSURANCE TOOLS BASED ON BEHAVIOURAL ANALYTICS

Strengths	Weaknesses
Circumvents the risk of excluding children without access to official documentation	Inherently privacy invasive because it profiles the child's Internet usage
	Accuracy of data may be reduced where children share devices with family and friends

⁸⁷ Yoti, Digital Identity Toolkit – Section 3: Digital identity explained, Yoti, London, January 2020.

⁸⁸ Ibid.

⁸⁹ McCann, D. and M. Hall, *Digital Self-Control: Algorithms, Accountability and our Digital Selves*, New Economics Foundation, London, 2019.



In recent years, providers offering behavioural analytics to companies to use within their own platform have emerged. These analytics tools monitor key strokes, typing speed, time of day the user logs on, and other granular data in order to assess the age of users and to flag users thought to be children who are using spaces designed for adults, and vice versa. It is not known how companies could differentiate behavioural analytics to determine age across countries and contexts. In the VoCO manifesto for the future of age assurance, it is envisaged that by 2030, there will be widespread use of artificial intelligence and behavioural analytics to safeguard children.⁹⁰

Compilation and use of digital footprints

From a child rights perspective, high levels of data collection from users, whether they are under the age of digital consent or over the age of digital consent but under 18, also raises concerns related to informed consent, data minimization, direct targeting for commercial purposes and surveillance. The Article 29 Working Party of the EU Commission has argued that inferences should be defined as personal data if they are “likely to have an impact on a certain person’s rights and interest”,⁹¹ or where the inferred data is not a special category in its own right, but becomes so when combined with other data,⁹² which appears to be the case when inferences are used

for age assurance purposes. There are also accuracy concerns with this method of age assurance as there is a risk of children logging in as someone else or using older siblings’ or parent’s accounts to access platforms.⁹³ Many users choose to remain logged into these platforms on their devices, and so when devices are shared, the digital footprint could soon become confused between friends and family members.

From this perspective, using children’s digital footprints to assess age should not be viewed as a panacea, due to the numerous ethical and privacy risks involved. Under European law, children have a fundamental right to the protection of their data (Article 8 Charter of Fundamental Rights of the European Union⁹⁴) which can be limited where this is necessary and proportionate. To protect children from more extreme harms, such as child sexual abuse and exploitation, greater limitations of Article 8 may be justified. However, for this to be necessary, the technology would need to be proven effective, and there would need to be an examination of alternative ways of minimizing this harm without using privacy infringing technologies.⁹⁵

Any age assurance system that invites a company to collect and analyse data related to the child’s behaviour, physical characteristics, body movements or geolocation could be problematic from a child rights perspective for two reasons. First, any unnecessary collection of

90 GCHQ, DDCMS and Home Office, *Verification of Children Online Phase 2 Report*, November 2020.

91 McCann, D. and M. Hall, *Digital Self-Control*, 2019.

92 Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251rev.01, p. 15.

93 Yoti, *Digital Identity Toolkit – Section 3: Digital identity explained*, Yoti, January 2020.

94 European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02

95 See further, European Data Protection Supervisor, *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, 25 February 2019. <https://edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures_en>

personal data from children should be avoided. Second, data collected on a premise of predictive analytics and machine learning may or may not be accurate, and may in fact result in discrimination. Platforms should be encouraged to minimize data collection from children and should arguably not be encouraged to create profiles of their child users based on their behaviour, location and other attributes that may go far beyond simply ascertaining age. This would risk leaving

children vulnerable to surveillance for commercial purposes, and to security risks if there is a data breach.

4.3 TOKENIZED SYSTEMS

Tokenized systems can be used by many different kinds of age assurance tools that use a variety of data sources. They can allow the child to only disclose their age or their age range, without disclosing any other identifying information.

TOOLS THAT ALLOW A CHILD TO DISCLOSE THEIR AGE (OR AGE RANGE) ONLY

Strengths	Weaknesses
The child does not have to disclose their identity and could provide an age range rather than their exact age	Records of the metadata associated with the child's token usage may be kept by the company or on their device, potentially forming a data trail linking back to the child



© UNICEF/JUN245119/KANOBANA



© UNICEF/UN050435/MUKWAZHI

Tokenized systems replace sensitive data with unique identification symbols, which retain the essential information about the data while maintaining its security.⁹⁶ Some tokenized systems only require identity data to be provided once: this is not retained, but used to create an attribute-based ‘token’ that can be shared with any service that needs to check the child’s age without revealing any other aspects of their identity.⁹⁷

A query to such a tokenized system would ask if the user was over the age of 18 and return a ‘yes’ or ‘no’ answer. Or, the query could be ‘what is the age

range of the user?’, to get the response ‘11–14’, or ‘how old is the user?’ to get a more precise age. In either case, the age attribute would not be connected to any other identifying information about the user. However, during the course of interviews for this paper, privacy concerns were raised about age assurance companies keeping records of where tokens have been used in the form of metadata, and potentially associating this with individual users. This further highlights the need for robust governance frameworks (see Section 6) to maintain users’ trust and confidence in the systems deployed.

⁹⁶ Rouse, M., ‘Tokenization definition’, TechTarget Search Security, (undated).

⁹⁷ Nash, Victoria, Gate-crashers? (forthcoming, 2020).

5. What are the risks to children that age assurance tools might help to mitigate online, and what is the evidence for the harms caused by those risks?

It is important to establish the risks to children that age assurance tools might help to mitigate online, in order to assess whether the use of such tools is necessary and justified in order to pursue the legitimate aim of upholding children's rights, as defined in the CRC.⁹⁸

Under the International Covenant on Civil and Political Rights (ICCPR), both children and adults have rights to protection against arbitrary and unlawful interference with their privacy and correspondence, and to freedom of expression. Any encroachment on ICCPR rights must first be to pursue a legitimate aim, and must also be deemed necessary and proportionate to meet that objective. Any restrictions on ICCPR rights must be the least intrusive instrument available among those that might achieve the desired result.⁹⁹ Accordingly, children should not be age-gated out of any online environment, or have their access to content or aspects of an online service limited, without solid evidence that this is necessary.

It is not possible to eliminate risk or harm entirely for children either offline or online. Evidence suggests that children's exposure to a certain degree of risk, according to their evolving capacity, helps them to build resilience and to prepare for the adult world once they reach the age of 18.¹⁰⁰ However, while frameworks for understanding children's online risks exist,¹⁰¹ there is little regulation or consensus regarding what is actually harmful to children online around the world, or any definition of what is and is not appropriate for children in different contexts by way of content, play or social environments online.

In the UK Government's VoCO study, participating platforms said that their efforts to protect children online were limited by the lack of a consistent definition of threats or potential harms to children online, or any agreement on the risk level posed by specific service features. They said they would need agreement on the likelihood

⁹⁸ See further letter from the-then Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, to the UK government, commenting on the UK Digital Economy Bill's mandated use of age verification tools by pornography websites, 9 January 2017.

⁹⁹ Ibid.

¹⁰⁰ Livingstone, S., 'More online risks to children, but not necessarily more harm: EU Kids Online 2020 survey', LSE Blog, 11 February 2020.

¹⁰¹ Livingstone, Sonia and M. Stoilova, *The 4Cs: Classifying Online Risk to Children*, 2021.

of the threat posed to children in given scenarios and on the best options for risk mitigation, to create a level playing field and to be confident that they were using the most appropriate age assurance tool to mitigate risks.¹⁰²

It is difficult to set precise ages in relation to children's general use of the Internet at which content or conduct becomes suitable for individual children because children mature at different rates. Moreover, some children have special educational needs that affect their cognitive skills, yet still wish to socialize online with their peers. Children have the right to be protected online from sexual exploitation and abuse and from violence, but this must be balanced with their rights to privacy, freedom of expression, participation, play and access to information. Any use of age assurance tools must ensure that all of these rights are protected and promoted for children online.

Legislative and technological responses to risks and harms should be proportionate to both their prevalence and impact,¹⁰³ and generally based on evidence. In many countries, offline products and services, such as alcohol, tobacco, gambling and film content, came to be age restricted in law through public and parliamentary debate related to research and evidence and broad public agreement.¹⁰⁴ However, in the online context, age restrictions can currently be applied through decisions made by private companies, often for reasons related to compliance with data protection regulations, rather than on the

basis of robust evidence related to harmful content or conduct.

This paper looks at online gambling and pornography, because these sites are almost universally restricted for children to access, and at social media and gaming apps, because these platforms set out age restrictions for children's access in their terms and conditions. It also considers the use of age assurance tools to address the harms caused by children being depicted in child sex abuse materials online, as a means of flagging content that features children, thereby enabling its removal and the rescue of child victims following human review.

5.1 GAMBLING

What do policymakers say?

According to the International Association of Gaming Regulators, the legal age for participation in gambling activities aligns with the age of majority in most jurisdictions. Therefore, globally, the average (modal) legal age to gamble is 18 across all markets.¹⁰⁵

What is the evidence of risk and harm?

There is evidence to suggest that people who gamble earlier in life are more likely to become problem gamblers in adulthood, and problem gambling is associated with low self-esteem, poor school performance and increased risk of other addictions.¹⁰⁶

¹⁰² GCHQ, DDCMS and Home Office, *Verification of Children Online Phase 2 Report*, November 2020.

¹⁰³ Baines, V., 'On Online Harms and Folk Devils: Careful Now', *Medium*, 24 June 2020.

¹⁰⁴ Nash, Victoria et al., *Effective age verification techniques*, 2013.

¹⁰⁵ International Association of Gaming Regulators, 'Gaming Regulation – Global Developments 2018-19 (Markets)'.

¹⁰⁶ Sellgren, C., 'Child gambling a "growing problem" – study', BBC News, 15 October 2019; Parent Zone, 'Gambling and children – a problem?', (undated).

However, early exposure is clearly not the only cause of gambling addiction. Concerns have been raised in the UK that children from age 11 are increasingly likely to become problem gamblers due to exposure to high volumes of betting ads online.¹⁰⁷ The potential harms related to gambling, for example getting into financial debt, are also evident.

As well as traditional gambling websites, there has been an increase in gambling or gambling-like features becoming integrated into online games and e-sports platforms accessed by children.¹⁰⁸ Gambling regulators from 16 European countries released a statement at the 2018 Gambling Regulators European Forum, expressing concerns regarding the blurring of lines between gambling and gaming. These concerns related to skin betting, loot boxes, social casino gaming and the use of gambling-themed content within video games.¹⁰⁹ However, disagreements still abound on precisely what features amount to gambling within online games.¹¹⁰

Does the evidence warrant age restrictions?

Gambling seems to be quite a straightforward activity to link to age, as the potential to get into debt is also regulated by age in other contexts (such as being able to open a bank account, have a credit card or take out a loan).

Are age assurance tools likely to be effective in this context?

For gambling websites, age verification tools to ensure a user is an adult appear to be the most appropriate. Because gambling is illegal in most countries for anyone under the age of 18, the burden is upon adults to prove they are over 18 to access gambling websites or apps. Gambling websites in many jurisdictions are subject to stringent know-your-customer (KYC) and money-laundering regulations, meaning they need to know the financial identity as well as the age of their customers. In this context, it is relatively straightforward to prevent children from accessing online gambling sites because of the identity credentials required for all users.

Gambling companies use CRAs to verify users' ages, which inspires public confidence because CRAs are heavily regulated and there is clarity in relation to liability issues related to age and identity verification among adults.¹¹¹ Gambling companies have to pay a fee to obtain the data required for age verification, and this is built into their business costs.¹¹² Online gambling is prohibited in Singapore, except for two named exempt operators, under the Remote Gambling Act 2014. Singapore Pools is an exempt operator that allows users to verify their age in person or online using their National Registration Identity Card, followed by a video call.¹¹³

107 Davies, R., 'Children more likely to become gamblers due to high volume of betting ads', *The Guardian*, 27 March 2020.

108 Derevensky, Jeffrey L. and Mark D. Griffiths, *Gaming Law Review*, November 2019, pp. 633–639.

109 Gambling Commission, Declaration of gambling regulators on their concerns related to the blurring of lines between gambling and gaming. 17 September 2018. <www.gamblingcommission.gov.uk/PDF/International-gaming-and-gambling-declaration-2018.pdf>

110 DDCMS, *Loot Boxes in Video Games: Call for Evidence*, UK Government, London, September 2020, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/920393/Loot_Box_Call_for_Evidence_Document_.pdf>.

111 Nash, Victoria et al., *Effective age verification techniques*, 2013.

112 Nash, Victoria, *Gate-crashers?* (forthcoming, 2020).

113 Australia eSafety Commissioner, *Inquiry into age verification for online wagering and online pornography*, November 2019.

When it comes to gambling within games, one approach could be to require users who wish to partake in activities that may be defined as gambling to verify that they are an adult, as with gambling websites. This would place the onus on adults to prove they are eligible to access gambling, thus avoiding placing any additional requirements on children. Alternatively, the gaming platform may choose to establish the age of all of users in order to prevent children's exposure to gambling activities. In such cases, age assurance tools may be called for. What constitutes gambling within a game is not currently defined and is likely to vary across different jurisdictions, which makes it difficult to apply age assurance technology broadly in this context. This has also been difficult to regulate as there is currently no legal definition of virtual currency, and because third-party betting sites may register in jurisdictions with weaker laws or poor legal enforcement related to children and gambling.¹¹⁴

5.2 PORNOGRAPHY

What do policymakers say?

Viewing pornography is illegal for both adults and children in many countries across Asia, Africa and Central Europe. As such, the issue of age assurance in order to gain access to pornography is not applicable in these contexts. The term 'pornography' has many legal definitions within different jurisdictions, so it is not always clear across the literature

that consistent definitions are being used.¹¹⁵ Top-ranked digital sexuality education media worldwide accessed by children include websites, apps and YouTube vloggers, most of which are in the English language and based in the US.¹¹⁶ Some of this content may be classified as 'pornography' in certain contexts: if it were age restricted, this could deny children access to vital sexuality education materials.¹¹⁷

The UK Digital Economy Act 2017 was the first piece of legislation in the world to mandate the use of age verification tools to restrict children's access to pornography online (although the age verification provisions of the Act yet to come into force). It contains provisions mandating age verification for users of commercial pornography websites. In October 2020, the UK Government indicated its intention to repeal certain provisions in this legislation and to replace it with a new Online Harms Bill, anticipated some time in 2021, with Ofcom as the new regulator¹¹⁸.

More recently, in June 2020, the French Government introduced an amendment to a broader law on domestic violence requiring pornography websites to implement an age verification mechanism.¹¹⁹ In the case of companies that do not comply within 15 days with a first warning from the French audio-visual regulator Conseil Superior de l'Audiovisuel, the Paris Court of Justice could send an order to telecoms operators to block access to the website from France.

114 Livingstone, Sonia, 'The rise of skin gambling: how outdated legislation allows thousands of UK children to gamble online', *LSE Blog*, 17 April 2019.

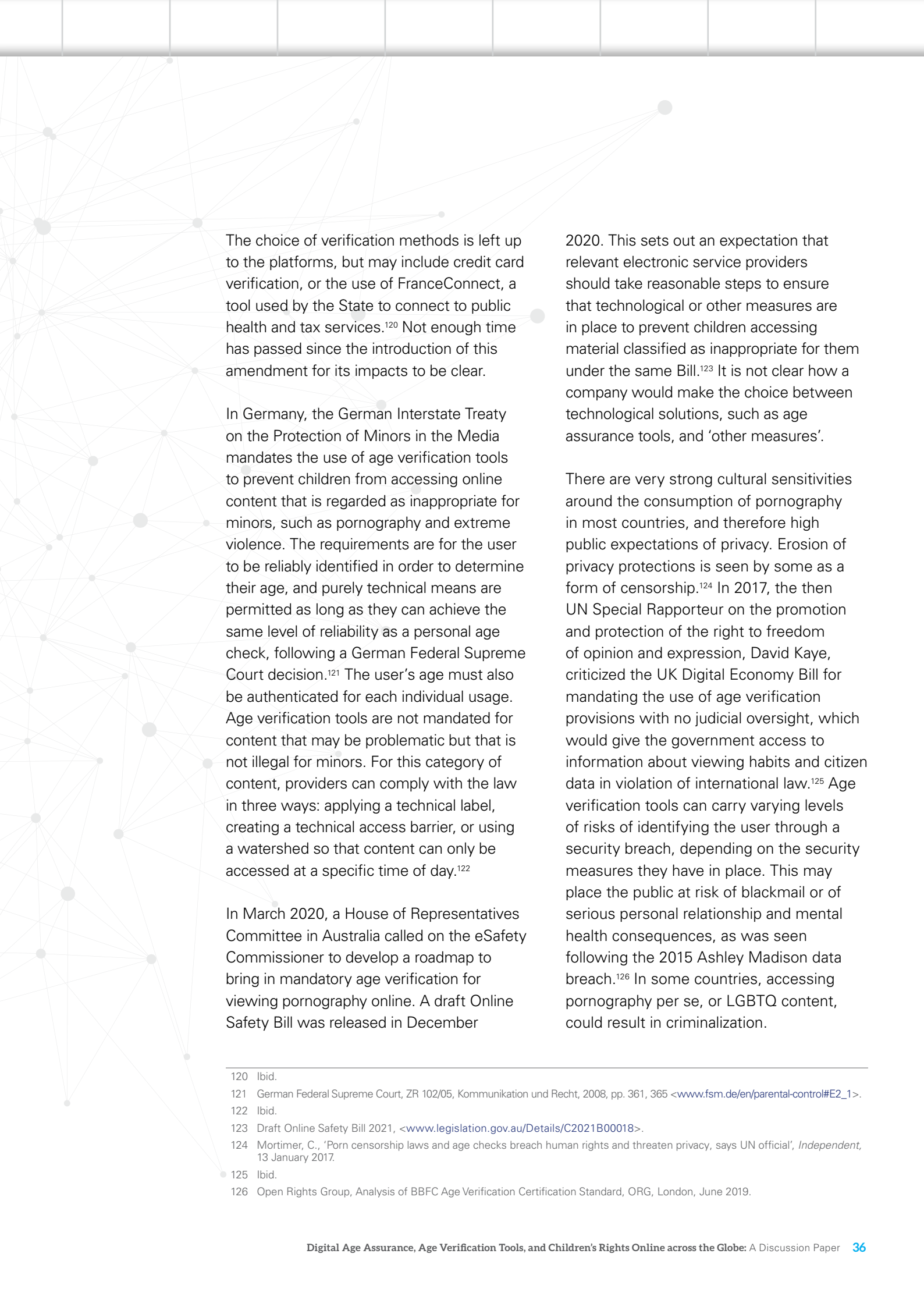
115 Akdeniz, Y., 'Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach', in L. Edwards, and C. Waelde, C. (eds), *Law and the Internet: Regulating Cyberspace*. Hart Publishing, Oxford, 1997.

116 United Nations Children's Fund, *The Opportunity for Digital Sexuality Education in East Asia and the Pacific*, UNICEF East Asia and Pacific, Bangkok, 2019.

117 Ibid.

118 Ofcom, *Ofcom to regulate harmful content online*. 15 December 2020. <<https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/ofcom-to-regulate-harmful-content-online>>

119 Braun, E. and L. Kayali, 'France to introduce controversial age verification system for adult websites', *Politico*, 9 July 2020.



The choice of verification methods is left up to the platforms, but may include credit card verification, or the use of FranceConnect, a tool used by the State to connect to public health and tax services.¹²⁰ Not enough time has passed since the introduction of this amendment for its impacts to be clear.

In Germany, the German Interstate Treaty on the Protection of Minors in the Media mandates the use of age verification tools to prevent children from accessing online content that is regarded as inappropriate for minors, such as pornography and extreme violence. The requirements are for the user to be reliably identified in order to determine their age, and purely technical means are permitted as long as they can achieve the same level of reliability as a personal age check, following a German Federal Supreme Court decision.¹²¹ The user's age must also be authenticated for each individual usage. Age verification tools are not mandated for content that may be problematic but that is not illegal for minors. For this category of content, providers can comply with the law in three ways: applying a technical label, creating a technical access barrier, or using a watershed so that content can only be accessed at a specific time of day.¹²²

In March 2020, a House of Representatives Committee in Australia called on the eSafety Commissioner to develop a roadmap to bring in mandatory age verification for viewing pornography online. A draft Online Safety Bill was released in December

2020. This sets out an expectation that relevant electronic service providers should take reasonable steps to ensure that technological or other measures are in place to prevent children accessing material classified as inappropriate for them under the same Bill.¹²³ It is not clear how a company would make the choice between technological solutions, such as age assurance tools, and 'other measures'.

There are very strong cultural sensitivities around the consumption of pornography in most countries, and therefore high public expectations of privacy. Erosion of privacy protections is seen by some as a form of censorship.¹²⁴ In 2017, the then UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, criticized the UK Digital Economy Bill for mandating the use of age verification provisions with no judicial oversight, which would give the government access to information about viewing habits and citizen data in violation of international law.¹²⁵ Age verification tools can carry varying levels of risks of identifying the user through a security breach, depending on the security measures they have in place. This may place the public at risk of blackmail or of serious personal relationship and mental health consequences, as was seen following the 2015 Ashley Madison data breach.¹²⁶ In some countries, accessing pornography per se, or LGBTQ content, could result in criminalization.

¹²⁰ Ibid.

¹²¹ German Federal Supreme Court, ZR 102/05, Kommunikation und Recht, 2008, pp. 361, 365 <www.fsm.de/en/parental-control#E2_1>.

¹²² Ibid.

¹²³ Draft Online Safety Bill 2021, <www.legislation.gov.au/Details/C2021B00018>.

¹²⁴ Mortimer, C., 'Porn censorship laws and age checks breach human rights and threaten privacy, says UN official', *Independent*, 13 January 2017.

¹²⁵ Ibid.

¹²⁶ Open Rights Group, Analysis of BBFC Age Verification Certification Standard, ORG, London, June 2019.



© UNICEF/UNI232328/NOORANI

What is the evidence of risk and harm?

There are several different kinds of risks and harms that have been linked to children's exposure to pornography, but there is no consensus on the degree to which pornography is harmful to children. Prominent advocates point to research arguing that access to pornography at a young age is linked with poor mental health, sexism and objectification, sexual aggression and other negative outcomes.¹²⁷ The evidence suggests that some children appear to be harmed by exposure to some kinds of pornography at least some of the time, but that the nature and extent of that harm vary.¹²⁸

There is conflicting evidence regarding how many children worldwide are accessing

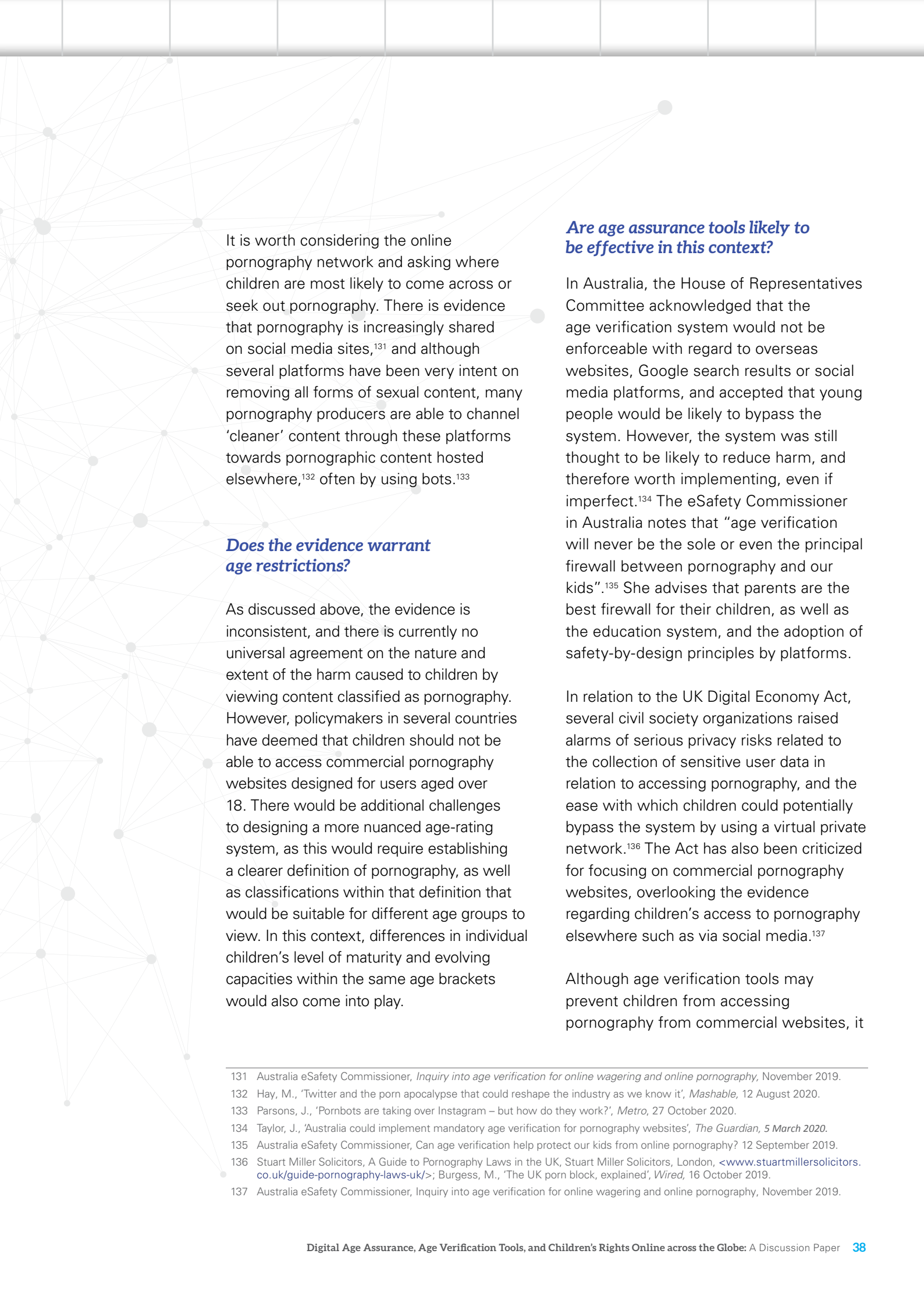
pornography online, and how often. Some studies have found that boys are more likely to experience greater exposure to pornography at an earlier age, and they are more likely to be exposed to violent or abusive images such as rape, whereas girls are more likely to be subject to involuntary or problematic exposure.¹²⁹ The 2020 EU Kids Online study compared survey findings from 19 European countries and found that in most countries, most children who saw sexual images online were neither upset nor happy (ranging from 27 per cent in Switzerland to 72 per cent in Lithuania); between 10 per cent and 4 per cent were fairly or very upset; and between 3 per cent (in Estonia) and 39 per cent (in Spain) reported feeling happy after seeing such images.¹³⁰

¹²⁷ Parliament of Australia, 'Age verification for online pornography', <www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report/section?id=committees%2Freportrep%2F024436%2F72615>.

¹²⁸ Binford, W., 'Viewing Pornography through a Children's Rights Lens', *Sexual Addiction & Compulsivity: The Journal of Treatment & Prevention*, vol. 25, no. 4, 2018; Livingstone, S. and J. Mason, *Sexual Rights and Sexual Risks Among Youth Online: A review of existing knowledge regarding children and young people's developing sexuality in relation to new media environments*, London School of Economics, London, 2015; Oosterhoff, P., C. Muller and K. Shephard, 'Sex Education in the Digital Era', *IDS Bulletin*, vol. 48, no. 1, 2017; Owens, E., R. Behun and J. Manning, et al., 'The Impact of Internet Pornography on Adolescents: A review of the research', *Sex Addict Compulsivity*, vol. 19, 2012, pp. 99–122.

¹²⁹ United Nations Children's Fund, *The Opportunity for Digital Sexuality Education in East Asia and the Pacific*, 2019.

¹³⁰ Smahel, D., H. Machackova, G. Mascheroni, L., Dedkova, E., Staksrud, K., Ólafsson, S. Livingstone and U. Hasebrink, *EU Kids Online 2020: Survey results from 19 countries*, EU Kids Online, London School of Economics, London, 2020.



It is worth considering the online pornography network and asking where children are most likely to come across or seek out pornography. There is evidence that pornography is increasingly shared on social media sites,¹³¹ and although several platforms have been very intent on removing all forms of sexual content, many pornography producers are able to channel 'cleaner' content through these platforms towards pornographic content hosted elsewhere,¹³² often by using bots.¹³³

Does the evidence warrant age restrictions?

As discussed above, the evidence is inconsistent, and there is currently no universal agreement on the nature and extent of the harm caused to children by viewing content classified as pornography. However, policymakers in several countries have deemed that children should not be able to access commercial pornography websites designed for users aged over 18. There would be additional challenges to designing a more nuanced age-rating system, as this would require establishing a clearer definition of pornography, as well as classifications within that definition that would be suitable for different age groups to view. In this context, differences in individual children's level of maturity and evolving capacities within the same age brackets would also come into play.

Are age assurance tools likely to be effective in this context?

In Australia, the House of Representatives Committee acknowledged that the age verification system would not be enforceable with regard to overseas websites, Google search results or social media platforms, and accepted that young people would be likely to bypass the system. However, the system was still thought to be likely to reduce harm, and therefore worth implementing, even if imperfect.¹³⁴ The eSafety Commissioner in Australia notes that "age verification will never be the sole or even the principal firewall between pornography and our kids".¹³⁵ She advises that parents are the best firewall for their children, as well as the education system, and the adoption of safety-by-design principles by platforms.

In relation to the UK Digital Economy Act, several civil society organizations raised alarms of serious privacy risks related to the collection of sensitive user data in relation to accessing pornography, and the ease with which children could potentially bypass the system by using a virtual private network.¹³⁶ The Act has also been criticized for focusing on commercial pornography websites, overlooking the evidence regarding children's access to pornography elsewhere such as via social media.¹³⁷

Although age verification tools may prevent children from accessing pornography from commercial websites, it

¹³¹ Australia eSafety Commissioner, *Inquiry into age verification for online wagering and online pornography*, November 2019.

¹³² Hay, M., 'Twitter and the porn apocalypse that could reshape the industry as we know it', *Mashable*, 12 August 2020.

¹³³ Parsons, J., 'Pornbots are taking over Instagram – but how do they work?', *Metro*, 27 October 2020.

¹³⁴ Taylor, J., 'Australia could implement mandatory age verification for pornography websites', *The Guardian*, 5 March 2020.

¹³⁵ Australia eSafety Commissioner, *Can age verification help protect our kids from online pornography?* 12 September 2019.

¹³⁶ Stuart Miller Solicitors, *A Guide to Pornography Laws in the UK*, Stuart Miller Solicitors, London, <www.stuartmillersolicitors.co.uk/guide-pornography-laws-uk/>; Burgess, M., 'The UK porn block, explained', *Wired*, 16 October 2019.

¹³⁷ Australia eSafety Commissioner, *Inquiry into age verification for online wagering and online pornography*, November 2019.

is unlikely that they would prevent children from accessing pornography completely. Therefore, if the goal is to prevent children from viewing pornography online in any form, it is not clear that preventing children from visiting commercial pornography websites through age verification would be a successful strategy.

At a baseline, age assurance tools could be more suited to ensure that younger children are not able to access commercial websites intended for adults, while mitigating broader privacy concerns. This could be done by checking whether the child in question appears to be within a range of 14–18, which could be effective in excluding young children. However, it is possible that this would cause children to seek out pornography elsewhere, such as on social media and to share it with friends on messaging apps, than preventing them from accessing it altogether. However, there is still an argument to be made that mandating the use of age verification or assurance in law could contribute to changing social norms around children accessing pornography, and hold the companies producing pornography more accountable for deploying the same restrictions online as is the norm offline in many contexts.

In the case of pornography accessed via social media, even if the platforms employed age assurance tools to tailor the user experience to the age of the user, it is unclear whether age assurance would protect child users of social media from bots designed to direct them to pornography sites.

From a rights perspective, extreme care would be needed to avoid excluding children from sexual and reproductive health information online: sexuality education, including resources for LGBTQ education, may be categorized as pornography in some contexts. Finally, it is questionable whether age assurance tools are an appropriate response to pornography that depicts extreme violence or violence against women, both of which can arguably be considered harmful for viewers of all ages.

5.3 ONLINE GAMING

What do policymakers say?

Age assurance tools to access games are only mandated by law in China. In 2011, the US Supreme Court struck down a law requiring ratings for video games and making it illegal to sell certain games to people aged under 18.¹³⁸ The Court found that video games deserve the same level of protection of freedom of speech as exists for books and films. It compared the violence depicted in games to Grimm’s Fairy Tales, which are broadly thought of as acceptable to children despite containing lots of violence.

What is the evidence of risk and harm?

There has not been any conclusive research connecting games that contain significant violent content with aggressive responses in players either in general,¹³⁹ or specifically in relation to under-18s.¹⁴⁰ Games can also include adult themes or semi-pornographic

¹³⁸ *Brown v. Entertainment Merchants Association*, 564 U.S. 786 (2011).

¹³⁹ Pinsent Masons, *Video games and age restrictions – the US and UK*, 1 April 2018.

¹⁴⁰ Nash, Victoria et al., *Effective age verification techniques*, 2013.

material.¹⁴¹ However, evidence as to adverse impacts of such exposure to children is so far inconclusive.¹⁴²

Participating in online, multiplayer games with other people, both friends and strangers, has become increasingly popular among children, as has watching live streams of others playing games. The vocal and written chat functions that allow players and viewers to interact could put children at risk of various online harms, such as grooming by sexual predators or exposure to explicit content.¹⁴³ It is particularly difficult to moderate high volumes of voice chat in real time to prevent this from happening, although algorithmic tools have been developed to filter inappropriate and hateful content or even to track signs of grooming.¹⁴⁴ It is possible to deploy these tools for all users, without needing to restrict children's access or ascertain the ages of individuals. It is also possible to apply stricter filters for younger users as they participate in the game. However, age assurance tools alone should be used with caution to address grooming, as interactions between adults and children are often not inherently problematic (for example, children may wish to interact with older relatives online).

Gaming companies may collect data on children's behaviour, on their interactions with others and on their behaviour across multiple devices and apps linked to their gaming device.¹⁴⁵

There has been widespread media concern in many countries about the possibility of children becoming 'addicted' to video games, or using them excessively. However, the evidence available showing major negative effects on children's well-being from gaming is contested.¹⁴⁶

Does the evidence warrant age restrictions?

The gaming sector is rapidly evolving, and is a space shared by children and adults. Gaming is reportedly the fastest growing segment of the media and entertainment industry globally, with companies focusing on Internet streaming and free-to-play games.¹⁴⁷ China is the world's fastest growing video game market and home to TenCent, the largest gaming company in the world. Global industry leaders can also be found throughout the US, Europe and Asia.¹⁴⁸ Outside China, gaming companies generally only require children to self-declare their age to sign in. The majority of streaming services do not require anyone to sign in to view gaming content, or to participate in chat streams, even where they contain adult themes.¹⁴⁹

In the context of gaming, and also in relation to children's general use of the Internet, it is difficult to set precise ages at which content or features become suitable for children. This is partly because children mature at

141 TransUnion, Risk-Based Authentication Solutions, (undated), <www.iovation.com/topics/age-verification>.

142 Kardefelt-Winther, D., How does the time children spend using digital technology impact their mental well-being, social relationships and physical activity? An evidence-focused literature review, UNICEF Innocenti Discussion Paper 2017-02, UNICEF, New York, 2017.

143 United Nations Children's Fund, *Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry*, UNICEF Discussion Paper Series: Children's Rights and Business in a Digital World, UNICEF, New York, 2019.

144 Lyons, K., 'Microsoft tries to improve child abuse detection by opening its Xbox chat tool to other companies', *The Verge*, 14 January 2020.

145 United Nations Children's Fund, *Child Rights and Online Gaming*, 2019.

146 Ibid.

147 Capital Ideas, Video game industry goes for the win, 12 September 2019, <www.capitalgroup.com/europe/capitalideas/article/video-game-industry.html>.

148 Ibid.

149 United Nations Children's Fund, *Child Rights and Online Gaming*, 2019.

different rates. Age ratings provided by game developers can still be a useful guide for children and their parents, similar to age ratings for films. Moreover, carrying out research to ascertain the age range of the user base (rather than verifying the age of every individual user) can also go some way towards enabling platforms to create environments that are safe by design.

Are age assurance tools likely to be effective in this context?

Because age ratings for games are generally designed as guidance for parents and their children to follow, the most appropriate form of age assurance tool could be one that checks whether the child falls within a rather wide age band.

While age assurance tools have been deployed to limit gaming time, there are concerns that the collection and retention of children's personal and behavioural data may segue into surveillance for commercial or political purposes.¹⁵⁰ For example, the use of facial recognition to curb children's game time would likely not comply with the GDPR, under which the use of facial recognition technology requires legal grounds such as explicit consent, a legal obligation or the public interest. In order for facial recognition to be compliant with the GDPR for age assurance purposes, it would have to be demonstrated that this was a proportionate approach, and that less intrusive options were not available.¹⁵¹

5.4 SOCIAL MEDIA

What do policymakers say?

There are no laws that limit the age at which children can use social media. However, most social media companies require their users to be aged 13 before they can use their platforms, in order to comply with COPPA in the US and the GDPR in the EU. The GDPR sets the age at which children can consent to data collection at 16, but allows states to choose a lower age, with the minimum being 13. In a June 2020 Communication on the GDPR, the EU Commission proposed possible targeted amendments to the GDPR regarding the "the possible harmonisation of the age of children's consent in relation to information society services".¹⁵² It is important to note that this relates to data protection and the digital age of consent to data collection, rather than to protecting children from harmful content or contact online. Many companies have chosen to set the minimum age at 13 in their terms of service, arguably to avoid needing to obtain parental consent from their younger users (although self-declaration of age is usually used, which is not difficult for children to circumvent). Using age assurance to prevent under-13s from joining social media platforms may unduly restrict access by younger users who could benefit from access, with safeguards in place to restrict collection of their data.¹⁵³

¹⁵⁰ Ibid.

¹⁵¹ Oy, Berggren, '3 Key Considerations for GDPR Compliance With Facial Recognition Technology', Lexology, no. 20, July 2020.

¹⁵² European Commission, Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, Brussels, 24.6. 2020 COM(2020) 264.

¹⁵³ Nash, Victoria, Gate-crashers? (forthcoming, 2020).

What is the evidence of risk and harm?

Children face different risks of data exploitation in social media environments at different ages. Children aged under 13 (and up to 16 in some jurisdictions) are protected from data exploitation by law. Children may also expect additional layers of data protection, such as prohibition of commercial exploitation through data profiling.¹⁵⁴

However, there is significant evidence to suggest that children much younger than 13 can easily bypass the age restrictions on social media platforms, leaving them open to data exploitation, and the use of their data for profiling and targeted advertising. For example, CyberSafe Ireland found through its regular survey of 8- to 12-year-olds that 48 per cent of children under 8 years use social media.¹⁵⁵ In a case lodged with the UK High Court against YouTube in 2020, it was alleged that YouTube has breached the privacy and data rights of under-13s under both UK law and the GDPR by collecting and using their data.¹⁵⁶ Similarly, in the US, the FTC brought a suit against Google in which evidence was produced where Google described YouTube as “the number one website visited regularly by kids”, “today’s leader in reaching children age 6–11 against top TV channels” and “unanimously voted as the favorite website of kids 2–12”.¹⁵⁷ The FTC also took action against TikTok in 2019 for knowingly allowing children aged under 13 to use its app and continuing to collect their personal information, and subsequently fined the company US\$5.7 million.¹⁵⁸

Does the evidence warrant age restrictions?

There are very sound rights-based reasons for restricting companies from collecting data from children. However, age-gating children’s access to social media on the basis of the age of digital consent appears to be a crude way of protecting children from data exploitation, because it bars access prior to the age of 13 or 16 (depending on the digital age of consent), and then provides no protections for children between the ages of 13 and 18. Restricting access to platforms prior to the age of digital consent has the unintended consequence of restricting children’s participation, freedom of expression and other potential opportunities offered by social media. For example, critics such as Naomi Klein have advised children to move away from corporate platforms because of the difficulties with age-based access, which can restrict younger children’s rights to freedom of expression and to protest online.¹⁵⁹

Just as chat functions within games may expose children to risks of harms related to sexual or violent content or conduct (see above), the same can be said for social media messaging apps. Restricting access to platforms, or to features and content within them, on the basis of age may not be sufficient to fully mitigate such risks. However, if policymakers or companies do decide to restrict children’s access on the basis of age, similar age ratings as those

154 Macenaite, M. and E. Kosta, ‘Consent for processing children’s personal data in the EU: following in US footsteps?’, *Information & Communications Technology Law*, vol. 26, no. 2, 2017, pp. 146–197.

155 Cybersafe Kids <<https://cybersafeireland.org/blog/posts/2020/may/the-digital-age-of-consent-2-years-later/>>.

156 BBC, ‘YouTube faces legal battle over British children’s privacy’, 13 September 2020, <www.bbc.co.uk/news/business-54140676>.

157 Federal Trade Commission, Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children’s Privacy Law, 4 September 2019. <<https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>>

158 Perez, S., ‘The FTC looks to change children’s privacy law following complaints about YouTube’, *TechCrunch*, 18 July 2019.

159 Gheorghiu, Diana, *How coronavirus makes us rethink youth protests*, Global Child Forum, Stockholm, (undated), <www.globalchildforum.org/blog/how-coronavirus-makes-us-rethink-youth-protests/>.

used by the gaming industry will be required for children under the age of digital consent, because currently, age restrictions on access to social media generally relate to data protection laws rather than online safety.

Are age assurance tools likely to be effective in this context?

The main method of age assurance used by social media companies is self-declaration by children. This has been shown to be ineffective in preventing under-13s from accessing social media: it is easy for children to misrepresent their age, and they are incentivized to do so to gain access. This also makes self-declaration ineffective as a method of protecting children from data exploitation, because after they input an adult birth date, companies may take their response at face value and collect their data.

Alternatives to self-declaration have been implemented on certain platforms. For example, an age assurance provider has worked with a social networking app designed for young people which has a separate community for 13- to 17-year-olds, to scan the user profiles using facial analysis technology.¹⁶⁰ This technology allows the platform to flag users who seem younger than 13 or older than 17, and to request further proof of age from those users. This makes it possible to remove users found to be of an inappropriate age, which would not be possible to do through a manual review of millions of users.¹⁶¹ However, this is still an emerging technology. Although it can flag users who are likely to be underage, it still

relies on processing children's biometric data, even if this data does not need to be retained. It also raises issues for those children who are flagged inaccurately, who then face the hurdle of proving their age.

An alternative approach suggested by a number of stakeholders, including CyberSafe Ireland and 5Rights, is to provide technical measures and tools that allow users to manage their own safety adequately, and that are set to the most secure privacy and safety levels by default, so that children are not incentivized to misrepresent their age.¹⁶² Separately to data protection issues, there may still be reasons to age-rate some social media apps to protect children from inappropriate content or contact.

5.5 CHILD SEX ABUSE MATERIALS

Distinct from the contexts discussed above, there is another use for age assurance tools, namely the detection of child sex abuse materials online.

There have been some recent promising cases of age assurance tools being used to combat child sex abuse materials online. First, age assurance tools are already in use to help children have sexual content depicting themselves removed from the Internet in the UK. Second, a number of organizations have been experimenting with the deployment of age assurance tools on pornography websites or other platforms that contain pornography, to flag images that appear to be of children aged under 18 for removal, subject to human review.

¹⁶⁰ Yoti, 'Making the Yubo App Safer for Users', Yoti Blog, 5 February 2019.

¹⁶¹ Ibid.

¹⁶² 5Rights Foundation, Let's make it easy for online services to protect children's data, <<https://5rightsfoundation.com/in-action/lets-make-it-easy-for-online-services-to-protect-childrens-data.html>>; Curley, C., *A Review of Age Verification Mechanisms for 10 Social Media Apps*, CyberSafe Ireland, Dublin, May 2020.



© UNICEF/JUN040656/

In the UK, age assurance tools are being used by the Internet Watch Foundation (IWF) in partnership with the NSPCC and Childline, to help children to report naked or sexual photos of themselves posted online. To do so, they have to confirm they are under 18, which they can do either by i) confirming their identity by uploading a UK passport, driver's licence, CitizenCard or a young person's ID card, or ii) sharing an estimate of their age based on a facial scan using an app, which makes it possible for victims to report the materials and have them removed anonymously.


Experts interviewed for this study noted that in many countries where abuse materials involving children after the age of puberty exist, they are very often presumed to be adults. This means that post-pubescent children need to prove that they are under 18 in order to have their images or videos classified as child sex abuse material. The age assurance

is required to enable the IWF to remove the materials, as its mandate is only to remove content featuring children aged under 18.¹⁶³ Given that pre-pubescent children's images would likely be removed without the need for age assurance, the tools would be most suited to assess post-pubescent children whose age was in doubt. It is possible that the algorithms used would be more accurate in identifying children in this age group.

There are significant concerns about the involvement of under-18s in the pornography industry, as this content constitutes child sexual exploitation under the CRC, whether the child consents to its production or not. There are also well-documented links between children featured in pornography, the sale of children for sexual purposes, and human and child trafficking for sexual purposes,¹⁶⁴ which makes flagging and investigating underage sexual images online particularly important.

¹⁶³ Childline: Report a nude image online <www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online/>.

¹⁶⁴ Beck, J. 'The Link Between Pornography and Human Trafficking', *Ever Accountable*, (undated), <<https://everaccountable.com/blog/the-link-between-pornography-and-human-trafficking/>>.



PornHub and XVideos have recently been criticized by a New York Times investigative journalist for not doing enough about child sex abuse on their platforms.¹⁶⁵ A week after the New York Times piece, and in response to Visa and Mastercard consequently withdrawing their payment services, PornHub announced changes to its platform to i) require anyone uploading a video to verify their identity; ii) improve moderation; and iii) prevent the downloading of videos, which allows illegal materials such as child sex abuse materials to proliferate.¹⁶⁶ This is a positive move, and pressure is now being put on XVideos and XNXX to follow suit, as they are reportedly among the 10 most visited websites worldwide.¹⁶⁷

There are also concerns that leading pornography websites allow categories of searches that clearly suggest the people depicted are under the age of 18, such as “less than 18”, “training bra” and “pre teens”.¹⁶⁸ A proposed solution is that a targeted approach be taken to review the age of people depicted in pornographic content categorized with headings such as “teen” as a minimum. A counterargument for this approach is that adults of a youthful appearance would need to verify their

age in order to continue being featured in legal pornography.¹⁶⁹ On balance, it seems arguably proportionate to place the burden on adults rather than children in this regard.

Interviewees for this paper also proposed that there is a need for an infrastructure allowing more people in the academic world to build models of age assurance for social purposes, such as detecting minors on pornography or escort websites, and identifying child sex abuse victims from images and videos online. This could help to address the current situation in which non-governmental and civil society organizations do not have the expertise to develop the technology, and industry has access to the data but has a proprietary interest in it. Academics could be well positioned to ensure that models of age assurance are built and applied on the basis of robust evidence, and are reviewed by recognized ethical standards bodies, while still collaborating with civil society and the private sector. For this to work, it would be necessary to devise a very secure yet transparent method of data-sharing between industry and academia, for example through the use of regulatory sandboxes, and substantial and sustainable funding.

¹⁶⁵ Kristof, N., ‘The Children of Pornhub: why does Canada allow this company to profit off videos of exploitation and assault?’, *New York Times*, 4 December 2020.

¹⁶⁶ Kristof, N., ‘Opinion: An Uplifting Update, on the Terrible World of Pornhub’, *New York Times*, 9 December 2020.

¹⁶⁷ Ibid.

¹⁶⁸ Ibid.

¹⁶⁹ Ibid.

6. What does the existing regulatory landscape look like with respect to age assurance online?

When age assurance tools are used to restrict children's access, they inherently involve restrictions to children's rights to access information, freedom of expression and protection of personal data, and so different child rights must be balanced. Where age assurance tools are required for adults to access certain regulated content, they may also involve restrictions on adults' rights to privacy and protection of personal data, which must also be taken into account. The test for balancing rights under international human rights law (the proportionality test) involves three criteria: i) any interference with a human right must be set out in a clear legal provision detailing the restriction; ii) it must be in pursuit of a legitimate aim; and iii) the response should be proportionate and necessary.¹⁷⁰

This proportionality test is also reflected at a European level in the revised AVMSD, which notes that following the Court of Justice of the EU, access to content

online can be restricted for public interest reasons such as obtaining a high level of consumer protection, provided that such restrictions are justified, proportionate and necessary.¹⁷¹ Specific legal measures for the protection of minors online are laid out in the AVMSD and in the GDPR. The premise of the AVMSD is that the less control a viewer has and the more harmful a specific content could be, the more restrictions should apply.¹⁷² The AVMSD provides that the most harmful content, which could impair the physical, mental or moral development of children, should be subject to the strictest measures such as encryption and parental controls. Importantly, the AVMSD also provides that personal data of minors processed in the framework of technical child protection measures should not be used for commercial purposes.¹⁷³

When it comes to limiting children's access to platforms and content online through

¹⁷⁰ De Schutter, O., *International Human Rights Law: Cases, Materials, Commentary*, 3rd edition, Cambridge University Press, Cambridge, 2019.

¹⁷¹ European Commission, Protection of minors. Audio-visual Media Services Directive, <<https://ec.europa.eu/digital-single-market/en/protection-minors-avmsd>>.

¹⁷² Ibid.

¹⁷³ Ibid.



the use of age assurance tools, it is clear that governments across the world hold different views on what a 'legitimate aim' is in this context, and on what constitutes a 'proportionate and necessary response'. The use of age verification tools to protect children is mandatory in Germany and France to prevent children from viewing illegal content (primarily pornography), and in China to prevent overuse of gaming. In the UK, the AADC provides guidance to companies in implementing UK data protection laws and the GDPR, and approaches age assurance from a risk-based perspective, requiring the robustness of age assurance to match the level of risk.¹⁷⁴ In China, restricting children's gaming time is considered of primary importance by the Chinese Government,¹⁷⁵ whereas this is not the predominant view taken by Western countries. In Europe, restricting children's access to certain kinds of pornography online is generally considered a legitimate aim by governments, whereas in the US, this is seen by the courts as an infringement of constitutional rights to freedom of speech, while in many other countries, pornography is entirely illegal. There is unlikely to be global agreement on what constitutes a proportionate and necessary response, particularly when it comes to the use of facial analytics, facial recognition and behavioural analytics.

While global consensus in these matters is unlikely, regional governance frameworks may ultimately have global impact, as has been seen with the GDPR. This is because companies generally prefer to operate to

one set of rules globally, so that they do not have to create different systems for different countries or regions. Because Europe is a significant market power in the technology sector, any decisions made there are likely to have an impact globally on technology companies wishing to sell their products in the European market.

There is currently very little regulation globally that is specifically related to age assurance tools, and outside the gambling and financial sector, the age assurance sector appears to be primarily self-regulated. There are arguments for both government regulation and private sector self-regulation for these types of technology. One study found that white-listed gambling companies regard themselves and each other as maintaining high standards in relation to both identity verification and age verification processes because they are subject to licence.¹⁷⁶ However, gambling companies located in jurisdictions that are less regulated were identified as examples of poor practice.¹⁷⁷ This points to the role of government regulation in improving practice. The need for a level playing field through the mandated use of age assurance tools was supported by industry stakeholders consulted for the UK VoCO study.¹⁷⁸

Standards also play an important role in the age assurance landscape, such as the UK PAS 1296 age-checking code of practice, which is overseen by a trade association. An in-depth analysis of these is beyond the scope of this paper, but

¹⁷⁴ Information Commissioner's Office, *Age appropriate design code: a code of practice for online services*, ICO, Wilmslow, Cheshire, 2020.

¹⁷⁵ Expert interview for this paper.

¹⁷⁶ Nash, Victoria et al., *Effective age verification techniques*, 2013.

¹⁷⁷ Ibid.

¹⁷⁸ GCHQ, DDCMS and Home Office, *Verification of Children Online Phase 2 Report*, November 2020.



© UNICEF/JUN157764/MAWA

the eSafety Commissioner has noted that the development of robust technical standards and requirements for age assurance is essential, as well as a better understanding of the effectiveness and impact of age assurance solutions in addressing distinct policy concerns.¹⁷⁹ In a report on age assurance tools published by 5Rights in March 2021, the creation of common standards on privacy, security and proportionality, as well as a regulatory framework with oversight and accountability, is recommended.¹⁸⁰

The AVMSD recognizes that both self- and co-regulatory instruments can play an important role in delivering a high level of consumer protection, and that public interest objectives are more easily met with the active support of service providers themselves.¹⁸¹ Different jurisdictions differ in terms of the public's preference for government regulation or private sector self-regulation, but

fundamental to any age assurance system is a high degree of trust from the general public, which is arguably lacking in both sectors currently.¹⁸²

The adoption of age assurance systems at scale across the Internet would be associated with both technical and governance challenges that must be addressed by stakeholders across the private sector, government and civil society. It is important that any standards or regulations set for the private sector are written from a child rights-based perspective, rather than simply from a compliance perspective, and strike an appropriate balance between privacy, security and safety. If companies are required to meet certain standards, they should be audited by an independent body, with provisions to review both compliance with regulations and technical testing of their products to ensure these meet the standards in practice.

179 Australia eSafety Commissioner, Inquiry into age verification for online wagering and online pornography, November 2019.

180 5Rights, But how do they know it's a child? Age Assurance in the Digital World, March 2021.

181 European Commission, Protection of minors. Audio-visual Media Services Directive, <<https://ec.europa.eu/digital-single-market/en/protection-minors-avmsd>>.

182 Confessore, N.m 'Cambridge Analytica and Facebook: The Scandal and the Fallout So Far', *The New York Times*, 4 April 2018; Simon, M. 'Investing in Immigrant Surveillance: Palantir And The #NoTechForICE Campaign', *Forbes*, 15 January 2020; Franco, M., 'Palantir filed to go public. The firm's unethical technology should horrify us', *The Guardian*, 4 September 2020.

7. Alternatives and complements to age assurance

Part of the assessment of whether or not age assurance tools are a proportionate response to mitigating the potential harms children are exposed to online involves asking what alternatives are available. There are many ways to protect children online, and none of these alone constitutes a complete solution. As concluded by the Australian eSafety Commissioner, there is a need for a suite of tools to keep children safe online. Age assurance tools may be one of these, but likely not the most important or effective one¹⁸³. Some alternative approaches are described briefly below.

7.1 SAFETY BY DESIGN AND PRIVACY BY DESIGN

Platforms should be encouraged to employ safety-by-design principles, as well as the related principles of privacy by design, security by design and inclusive design. This approach seems to have a broad base of support. For example, one expert interviewed for this paper argued that this is likely the only way to protect children with no negative impacts on them.

The Australian eSafety Commissioner Safety by Design principles encourage platforms to build safety features into their products and services for everybody.¹⁸⁴ This includes developing ground rules, providing tools for users to block and report problematic people and content, implementing technical solutions to minimize exposure to content risks, ensuring strong privacy settings by default and promoting user empowerment. It includes taking preventative steps to ensure that known and anticipated harms have been evaluated in the design and provision of an online service; that user empowerment and autonomy are secured as part of the in-service experience; and that organizations take ownership and responsibility for users' safety and well-being, and are clear about the steps required to address any issues.

The UK AADC incorporates privacy-by-design principles.¹⁸⁵ Several child rights organizations have called for privacy by default, which differs from privacy by design, especially for users who declare themselves to be under the age of 18,

¹⁸³ Australia eSafety Commissioner, Inquiry into age verification for online wagering and online pornography, November 2019.

¹⁸⁴ Australia eSafety Commissioner, Safety by Design <https://www.esafety.gov.au/sites/default/files/2019-10/LOG_per cent20 per cent20-Documents8b.pdf>

¹⁸⁵ UK Information Commissioner's Office, Age Appropriate Design Code <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>>

so that children are not incentivized to misrepresent their age.¹⁸⁶ The AADC requires companies to carry out a risk assessment in relation to children's data protection, and to deliver services in an age-appropriate way.

7.2 PARENTAL CONTROLS AND SUPERVISION

Filters can be installed on home Wi-Fi systems or on individual devices to prevent children from accessing adult content. It is also possible to enable browsing in 'safe mode' and with 'safe search' filters. Many consoles such as Xbox One, PS4 and Nintendo Switch feature parental controls. This approach is likely most suitable for younger children, because it may infringe children's rights to access information and to freedom of expression where their Internet access is censored at an older age. Practically speaking, it is also likely that older children will be able to circumvent parental controls.

There is a clear role for parents in supervising their children's use of the Internet. It has been argued that, in most cases, there should be no need for children to prove how old they are, and that parents and educators should be responsible for keeping them safe both online and offline (apart from where goods and services are legally restricted, in which case providers should employ a proportionate means of checking age).¹⁸⁷ The problem is that the children who are most vulnerable online are likely to be those who are also more vulnerable offline.¹⁸⁸ These children are less

likely to have parents or educators who have the capacity to engage with them in relation to their Internet use.

There is also a clear generational gap in digital literacy, further exacerbated in countries where children who are engaging with online environments through mobile devices have parents who do not speak English, or have low levels of general literacy as well as low levels of digital literacy, or where harmful content may be in languages undetected by foreign apps. For children who do not live with their parents, it can be hard for already overstretched carers in institutions to take on the role of supervising children's Internet use, along with all their other responsibilities. It therefore becomes necessary to define what the responsibility of platforms operating in such countries and contexts is to ensure a basic level of protection for children using their online spaces. A default position of 'safety by design' and 'privacy by design' promises to be an important part of the solution here, rather than relying exclusively on age assurance.

7.3 EDUCATIONAL INITIATIVES

Educational initiatives were highlighted by many of the experts interviewed for this paper as being essential to keep children safe, and to allow children to build the resilience they need to navigate risks they will inevitably come across online. The important role that can be played by schools to channel online safety messages was also highlighted.

¹⁸⁶ 5Rights Foundation, Let's make it easy for online services to protect children's data <<https://5rightsfoundation.com/in-action/lets-make-it-easy-for-online-services-to-protect-childrens-data.html>>; Curley, C., 'A Review of Age Verification Mechanisms for 10 Social Media Apps', 2020.

¹⁸⁷ Nash, Victoria et al., *Effective age verification techniques*, 2013.

¹⁸⁸ Livingstone, S., 'Vulnerable offline and at risk online: tackling children's safety', LSE Blog, 20 February 2019.



© UNICEF/JUN245119/KANOBANA

7.4 REMOVING CONVICTED CHILD SEX OFFENDERS FROM ONLINE SPACES

In order to protect children from sexual exploitation online, an alternative to restricting children's access to online spaces is more proactively removing convicted child sex offenders. It was reported that in New York State, several leading companies including Microsoft, Apple, Blizzard Entertainment, Electronic Arts, Disney Interactive Media Group, Warner Brothers and Sony collaborated to work with the attorney general to remove thousands of registered sex offenders from their online game platforms.¹⁸⁹ It would seem to make sense that convicted child sex offenders who are restricted by law from spaces frequented by children such as schools should be similarly restricted online. However, clear limits would need to be set, given the necessity of participating in online spaces for many essential social functions. One study found that restricting sex offenders from accessing social media may increase their

social exclusion and undermine efforts to reintegrate them into society, thereby also increasing their chances of reoffending.¹⁹⁰ Another weakness of this approach is that it would likely only address a small subset of online child sex offenders, as those who have been convicted are likely to make up a small portion of online predators.

7.5 TARGETING BEHAVIOUR RATHER THAN AGE

Some contact and conduct risks to children online such as bullying and harassment may relate more to individual personality than age, and therefore may be better addressed by moderation practices aimed at intervening when negative behaviour is detected, rather than applying age restrictions that may be somewhat arbitrary. However, this approach is not without its challenges. For example, it would be very difficult in practice to decide who should moderate behaviours in all the different contexts in which they may play out around the world.

189 Crime Victims Center, 'A. G. Schneiderman's "Operation Game Over" Purges Thousands of Sex Offenders from Online Video Game Networks', Ronkonkoma, N. J., 2012, <www.parentsformeganslaw.org/prevention-safer-online-gaming>.

190 Wilcox, A., and C. Najdowski, 'Should registered sex offenders be banned from social media?' *American Psychological Association. Judicial Notebook*, vol. 48, no. 4, 2017.

8. Summary

Some leading experts in child online safety have indicated that the age assurance system is not yet mature enough to be fully implemented,¹⁹¹ although the Australian eSafety Commissioner takes the view that age assurance has global and local momentum behind it as a potential solution.¹⁹² The Australian eSafety Commissioner has noted that age verification is a nascent field, and the effectiveness of age verification as a mechanism for preventing and addressing different risks and harms depends on a wide variety of technical, legal, policy and cultural factors, so there is a need to leverage other solutions to address online harms in a holistic and multifaceted way¹⁹³. The UK VoCO study noted that in order to gain public confidence in age assurance tools, there is still a need for further research into how age assurance may disproportionately affect some children.¹⁹⁴ It is imperative that this kind of research is undertaken before age assurance tools are rolled out at scale, to prevent discrimination, as well as further research into the effectiveness of specific age assurance tools. The UK VoCO study involved a small-scale user acceptance testing trial using a start-up specializing in age checking. The end-to-end proof of concept demonstrated that age assurance could work on platforms and devices with which children and their parents

were familiar. However, it was noted that further work was needed with a larger group to understand how this would operate at scale.¹⁹⁵

It seems likely that as significant investments are made in technologies and underlying governance frameworks, the age assurance system may mature and become a more viable option in the near future. In the meantime, some questions for further discussion remain, including those set out below, followed by proposed principles for guiding the development and use of age assurance tools in the future.

8.1 QUESTIONS FOR FURTHER DISCUSSION AND REMAINING BARRIERS

- ✓ Are age assurance tools a good way to ensure that platforms implement their data protection obligations? If so, should the age of digital consent be raised to 18 and decoupled from the age of access to social media platforms?
- ✓ Should there be hard rules related to the ages at which children can be permitted access to different games? If so, who should set the criteria for different ages and should they be consistent throughout the world? Is the


¹⁹¹ Nash, V., *Gate-crashers?* (forthcoming, 2020).

¹⁹² Australia eSafety Commissioner, *Inquiry into age verification for online wagering and online pornography*, November 2019.

¹⁹³ *Ibid.*

¹⁹⁴ GCHQ, DDCMS and Home Office, *Verification of Children Online Phase 2 Report*, November 2020.

¹⁹⁵ *Ibid.*



International Age Rating Coalition age-classification system an appropriate one for use globally?

- ✓ Could more robust forms of verified parental consent be used in place of age assurance for children? What about children who do not have parents equipped to monitor their Internet usage?
- ✓ What are the implications of age assurance tools for children with special educational needs and/or disabilities?
- ✓ What are the implications of age assurance tools for groups of children who may be at greater risk of surveillance, such as minority ethnic and religious groups, and undocumented children?
- ✓ Are there any kinds of data such as biometric data, behavioural analytics or social media digital footprints that should not be used for age assurance purposes on ethical grounds?
- ✓ Should age assurance systems be regulated by governments, co-regulated or self-regulated by the private sector?
- ✓ How can age assurance requirements be implemented in countries where the underlying data sources required to prove the child's age are not available? Is the use of facial recognition for age estimation a good solution for this?
- ✓ What are the risks for children in the Global South of age assurance regimes designed for use by dominant platforms from the US, the EU and China?

- ✓ Are standards required for the collection, use and destruction of children's personal data and metadata collected for age assurance purposes?
- ✓ Should age assurance be applied on individual platforms or more broadly across the Internet? What are the pros and cons of each?

8.2 PROPOSED PRINCIPLES FOR THE DEVELOPMENT AND USE OF AGE ASSURANCE IN THE CONTEXT OF CHILDREN'S RIGHTS

Proportionate usage


- ✓ Age assurance tools should only be used where there is evidence that they will mitigate a recognized harm to children, and where a less intrusive solution is not available. Where this is the case, the least intrusive form of age assurance possible (proportionate to the risk of harm) should be used.

Transparency

- ✓ When age assurance tools are used, children should have the right to know exactly how and when they are working, and what specific data sources have been drawn on to ascertain their age.

Access

- ✓ Children's rights to access information, to participation and to freedom of expression should be protected at all times, as well as their rights to privacy and data protection. Children's access to spaces and content should not



be restricted unless it is truly necessary to do so to prevent harm, on the basis of evidence. Safety and privacy by design should be prioritized over blocking children's access.

- ✓ Children should be provided with a remedy where their age is wrongly estimated by an age assurance tool, and a means of appealing against the decision to deny them access.
- ✓ Children's access should not be prevented wholesale where there are opportunities to provide a safer experience by tailoring the content and features made available to them within platforms.

Inclusion

- ✓ Any use of age assurance tools must ensure that marginalized groups of children are not excluded or discriminated against by requiring them to produce more or more sensitive data to prove their age, such as children on the move, undocumented children, children with disabilities, or children from minority ethnic groups.

Technical

- ✓ It is likely that as countries and regions move towards implementing national eID systems, and as the private sector continues to innovate in this space, a more mature ecosystem will emerge that includes greater potential for age assurance tools to be used. Care should be taken before encouraging children to share their eID widely online, if proof of identity is not required.

Governance

- ✓ There is a need for clarity on what – if anything – should be age-gated, and why, in different global contexts. Where age-gating is to be used, a clear rationale should be given for the chosen ages, together with evidence of the potential harm that is to be mitigated by preventing underage access, accompanied by a DPIA.
- ✓ There is a need for an international, consistent regulatory framework for age assurance that prioritizes children's rights, and balances safety, protection, security, privacy, freedom of expression and access to information. Any such regulatory framework must include effective oversight and enforcement mechanisms.

