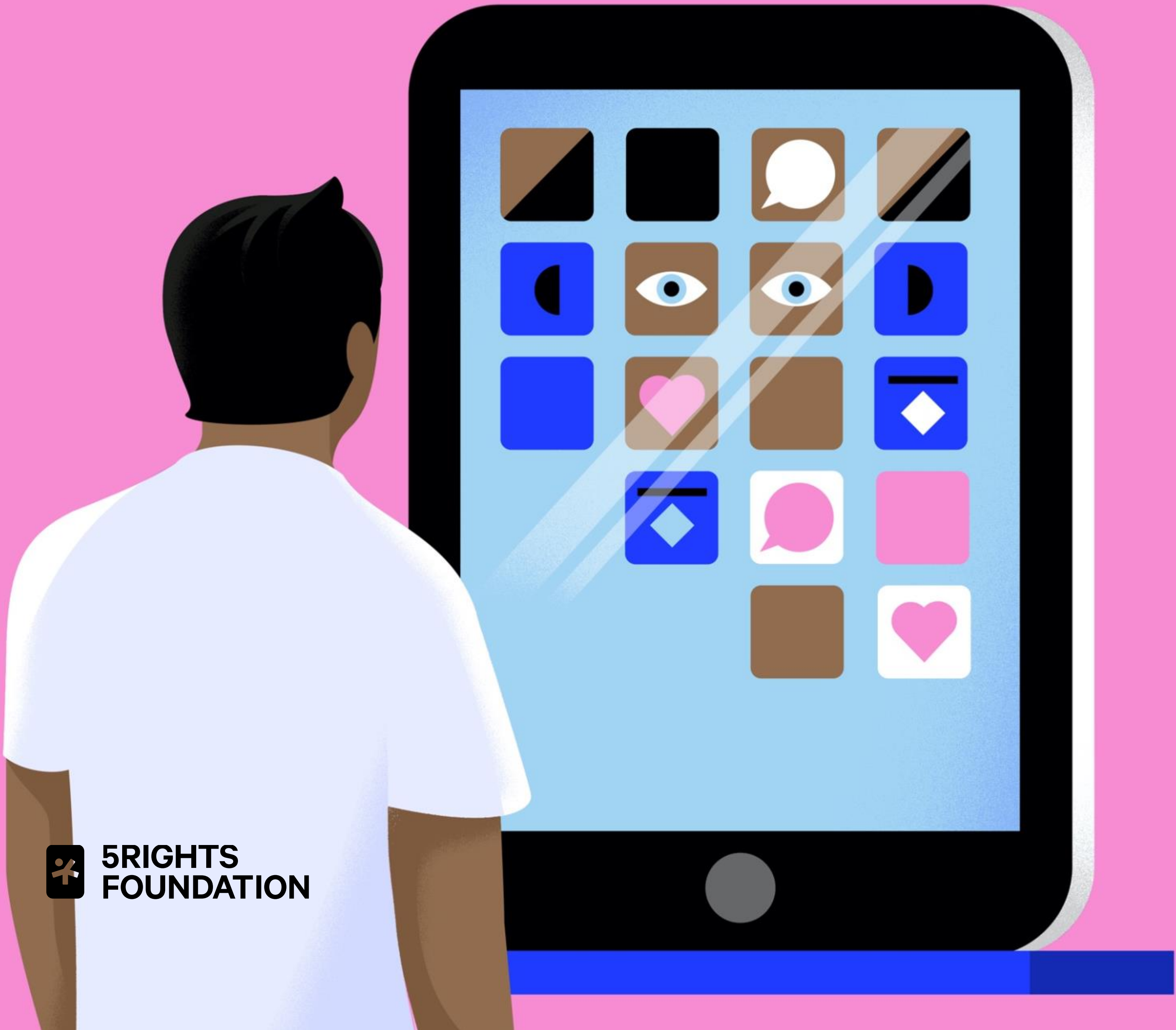
October 2021

But how do they know it is a child?

Age Assurance in the Digital World



5RIGHTS FOUNDATION

> **“We want to be on the internet to learn and to share, but we are not ready for the whole adult world.”**[1]
>
> Young person, UK

About 5Rights Foundation
Building the digital world that young people deserve

5Rights develops new policy, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives and ensures that children's rights and needs are recognised and prioritised in the digital world.

Our focus is on implementable change and our work is cited and used widely around the world. We work with governments, inter-governmental institutions, professional associations, academics, businesses, and children so that digital products and services can impact positively on the lived experiences of young people.

A child or a young person is anyone under the age of 18, as defined by the UN Convention on the Rights of the Child.[2] Rights language refers specifically to “children”, however, children themselves often prefer to be called “young people.” In this report we use the terms children and young people interchangeably, but in either case it means a person under the age of 18, who is entitled to the privileges and protections set out in the UNCRC.

[1] 5Rights focus group, September 2016.

[2] Article 1 of the United Nations Convention on the Rights of the Child states “a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.”

Contents

Preface

The digital world is not optional for most children. It is where they access education, health services and entertainment, build and maintain their relationships, and engage in civic and social activities. Digital technologies are built into the physical environments children inhabit and the systems that govern their lives, from the bus pass that gets them to school to the algorithms that grade their exam results. If the digital world is not optional for children, then it follows that it should be designed to meet their rights and needs.

Few disagree in principle, but before long the question is asked, how do we know if they are a child? In a time of mass surveillance, this is a curious question. Many companies have a detailed picture of their users' interests, location, relationships, family status, income, sexuality and so on.[3] Understanding users (profiling) and tailoring user journeys (personalisation) are the bread and butter of the tech sector, so it is perplexing that companies claim it is difficult, impossible or intrusive to identify children by age. This has undermined the faith of policy makers and civil society in the validity and possibility of recognising children in the digital environment.

As a result, the concept of age assurance carries the weight of firmly held ideological preconceptions, technical doubts and a lack of public trust in both digital service providers and the state. Governments and regulators increasingly demand special provision for children and with those demands has come a market for age assurance solutions. However, there remains a yawning gap between our desire to tackle the asymmetries of power between children and the technology they are using and our commitment to introducing rights-respecting age assurance.

This report starts by answering why and when we need to establish age and moves toward the practicalities of how that might be done, before setting out common standards by which we should measure age assurance systems. It brings clarity to what we mean by age assurance, what the risks and benefits of the current approaches are, and as we move forward, what the rules of the game should be. Above all, it points out that age assurance should not be mistaken for a silver bullet or a short cut to making the digital world fit for children. All age assurance does is let a service provider know that a child is there, or perhaps more accurately, ensures that the sector does not continue to pretend that children are not there. Its value lies not simply in the act of verifying or estimating age but in the enormous opportunity it brings once children have been recognised.

What age assurance looks like in 2021 will be unrecognisable a decade from now, but as government and regulators increasingly demand a better deal for children they must also provide minimum standards for assurance and a measurable criteria against which

[3] LGBTQ children online: Why digital platforms must design with them in mind, *5Rights Foundation*, June 2020.

solutions can be assessed. While there are multiple technological approaches, each is undermined by a lack of common standards and regulatory oversight. As we move to a more regulated and responsible digital environment, considering the age of a user should simply become a price of doing business.

This report focuses specifically on the UK, but the basic themes and conclusions are relevant to countries across the globe. Aimed at the general reader, it does not gloss over the complexities associated with establishing age, but it does take the view that age assurance is simply a gateway to the bigger prize of building the digital world that young people deserve.

Beeban Kidron

Baroness Beeban Kidron
Chair, 5Rights Foundation

Definitions

Age
The period of time someone has been alive or something has existed.

Verification
The act of verifying something (proving or checking that it exists, or is true or correct).

Estimation
A guess or calculation about the cost, size, value or extent of something.

Assurance
A positive declaration or promise intended to give confidence.

Age assurance
An umbrella term for both age verification and age estimation solutions. The word 'assurance' refers to the varying levels of certainty that different solutions offer in establishing an age or age range.

Age verification (AV)
A system that relies on hard (physical) identifiers and/or verified sources of identification, which provide a high degree of certainty in determining the age of a user. It can establish the identity of a user but can also be used to establish age only.

Age estimation (AE)
A process that establishes a user is *likely* to be of a certain age, fall within an age range, or is over or under a certain age. Age estimation methods include automated analysis of behavioural and environmental data; comparing the way a user interacts with a device or with other users of the same age; metrics derived from motion analysis; or testing the user's capacity or knowledge.

Age gate
A technical measure used to restrict or block access for users that do not meet an age requirement.

Identification (ID)
Establishes the identity of a unique person, and is likely to include some form of age verification.

Child or young person
A person under the age of 18.[4]

[4] Article 1 of the United Nations Convention on the Rights of the Child states "a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier."

Executive Summary

The UK's forthcoming Online Safety Bill has set the stage for a digital world that delivers more for children. Now is the key moment to introduce better age assurance, not as an end in itself, but as part of a wider programme of product development and market diversification that allows a child to be a child online. Below we summarise the key issues relating to the debate around age assurance, and how they might be addressed:

- Age assurance is not a silver bullet for keeping children safe online. It is simply a tool to identify that a service is dealing with a child.
- We must develop a mixed economy of age assurance solutions. Not all situations require the same level of assurance and many products and services need a combination of age assurance tools.
- Many technical solutions for age assurance exist, but their application is often co-opted by companies to maximise data collection.
- Children should not be routinely asked to disclose more information than is necessary to prove their age.
- At the heart of concerns about age assurance is a reluctance on the part of service providers to take on the responsibilities they would have to children once their age is known.
- Many of the changes necessary to make a service age appropriate do not need additional or new age assurance technologies, but rather require services to disable some of their more intrusive or risky design features such as geolocation data tracking, private messaging or targeted advertising.
- In many cases, the alternative to age assurance is to make a product or service appropriate for a mixed audience that includes children.
- Many age assurance solutions have great potential, but all are undermined by the lack of common definitions, agreed standards and regulatory oversight. These must be set out in legislation to give confidence to children, parents and businesses in their use.
- Pressures for better services and treatment for children will lead to greater investment and further innovation, but what 'good' looks like will be determined as much by developing standards and accountability as technical innovation.
- Statutory codes for age assurance will drive the development of new products and services and create a richer and more diverse digital ecosystem in which children are an acknowledged user group.
- Government should set out a statutory code of practice for age assurance in anticipation of the Online Safety Bill. It should include the following 11 common standards:

- Age assurance must be privacy preserving
- Age assurance should be proportionate to risk and purpose
- Age assurance should be easy for children to use
- Age assurance must enhance children's experiences, not merely restrict them
- Age assurance providers must offer a high level of security
- Age assurance providers must offer routes to challenge and redress
- Age assurance must be accessible and inclusive
- Age assurance must be transparent and accountable
- Age assurance should anticipate that children don't always tell the truth
- Age assurance must adhere to agreed standards
- Age assurance must be rights-respecting

Age assurance is a necessary part of broader action to build the digital world that young people deserve, and to do its job well it must be flexible and multifaceted to meet the myriad circumstances for which it will be used. A regulatory framework that offers certainty to businesses and can be trusted by parents and children will drive the innovations and redesigns that we need to see across the tech sector to support children's participation in the digital world.

Context

There is as yet no singular regulatory or statutory code in the UK that sets out exactly when age assurance is needed online and how it should be deployed. There are laws for the purchasing of age-restricted goods and services which apply to online retailers and service providers and there are pockets of regulation that require age assurance, but in the absence of codified standards set out in regulation, companies either do not know what is adequate or are able to turn a blind eye to their obligations to ascertain the age of their users.

In the UK, debates about age assurance have largely centred on restricting access to 'adult' content, such as pornography, with the unhappy outcome that age assurance is seen primarily as a way of *restricting* children in the digital world. Preventing inappropriate access to adult material is important, but characterising age assurance as simply a way of preventing children entering 'adult' spaces fails to recognise the full gamut of possibilities that age assurance offers, and simultaneously threatens to push children out of the digital world.

At its best, age assurance offers children the prospect of being invited into a digital world that offers them greater privacy, freedom from commercial pressures, content and information in formats and language that they like, protection from misinformation or material that promotes harmful activities (such as suicide, self-harm or disordered eating), as well as supporting digital services in their legal duty not to provide children with age restricted contact and content. Rather than being the route to keeping children out of the digital world, age assurance can drive the development of new products and services to create a richer and more diverse digital ecosystem in which children (one in three internet users) are a recognised user group.

Ignoring children online is in part a consequence of the US legislation, the Child Online Protection Privacy Act (COPPA) 2000, which defines a child as any person under the age of 13 and requires companies to obtain parental consent to process the data of children under 13.[5] Originally conceived as a marketing code at a time when the digital world was neither as pervasive nor persuasive as it is now, COPPA sought to restrict advertisers accessing children under 13. Over the last two decades, COPPA has defined children's online experience around the globe and COPPA-like provisions have been exported into all digital markets, including the UK's.

COPPA is restricted to services 'directed to children under 13 years of age', and children aged 13 to 17 receive no specific protections, creating a de facto age of adulthood online of 13. This means the vast proportion of children, who spend the greatest amount of time online, are treated as if they were adults. This is profoundly out of step

[5] Children's Online Privacy Protection Rule ("COPPA").

with a child's development, their rights and needs, and with almost all other sectors that engage with children. COPPA also only applies if a service has 'actual knowledge' that a user is under 13.[6] In practice, this has driven a 'don't look don't see' attitude to the tens of millions of under 13s who enter an adult world of aggressive data collection, targeting and harmful content. This sanctioned blindness has also disincentivised the development of services and products for children.

Another defining factor in the development of age assurance in the UK has been the contentious debate about the development of government issued identity cards. While many countries have ID card and/or digital IDs, including many European countries, the UK has strongly resisted their introduction, largely due to concerns for privacy and the impact on civil liberties.[7] The privacy implications of age assurance are discussed in detail later, but it is seldom acknowledged that age is just one aspect of identity. While many, if not most services exploit the lack of regulation to take more information than is necessary about users, it is rarely the case that a service needs to know a user's identity to verify their age. Applying the arguments against digital identity systems to the introduction of age assurance overlooks this distinction and fails to recognise that age assurance can be developed in ways that are privacy preserving,

Often heard in the debate around age assurance is the assertion that most solutions are unworkable because children lie about their age. This is unhelpful on at least four different fronts, the most important of which is that children have not been offered any alternative. If age assurance were associated with greater privacy, less aggressive commercial targeting and greater moderation, rather than simply denying children access, there would be less reason to lie. Second, all evidence from child development experts points to the fact that children need boundaries. The friction created by age gates sends the message that what they are doing or seeing is not a norm. Third, when children lie about their age in other circumstances, such as to buy alcohol or cigarettes, the responsibility is on the adult (individual or business) not the child. It leads us to ask, why are we making children responsible for a sector-wide failure to treat them as children? And finally, the sector is one of the most innovative and imaginative in the world and the technology for age assurance is already available. What is lacking is the investment, commitment and the political and commercial will to set regulated standards.

While standards have not yet been set, age assurance has already been referenced in a number of legislative and regulatory provisions, both at national and international level,

[6] Actual knowledge is defined as the direct and clear awareness of a fact or circumstance, as distinct from 'constructive knowledge', which is defined as 'knowledge that a person is deemed to have of facts that he would have discovered had he made the usual and proper inquiries.'

[7] Unlike many of its European neighbours, the UK does not have a national identity scheme or citizen ID cards and therefore does not have the foundations on which to develop national digital identities that citizens can use to prove who they are when they engage with digital services. The Identity Cards Act 2006 was an Act of Parliament in the UK that was repealed in 2011 following widespread public opposition to the scheme.

notably the Digital Economy Act 2017,[8] the Data Protection Act 2018[9] (and the Age Appropriate Design Code[10]), Video-sharing platform (VSP) regulation 2020,[11] the EU's Audio Visual Media Services Directive (AVMSD)[12] and the government's draft Online Safety Bill[13], as well as the UNCRC General Comment No. 25 on children's rights in relation to the digital environment.[14]

When the government passed the Digital Economy Act (DEA) in 2017, requiring commercial providers of pornography "to have robust age verification controls in place to prevent children and young people under 18 from accessing pornographic material"[15] there was outcry from the privacy lobby that this was tantamount to users being asked to give up their privacy and hand over their identities to commercial pornography sites. With public trust in the handling of personal data at an all-time low, this part of the DEA was never implemented, the government instead promising to fulfil its objectives through the forthcoming online harms regime.[16]

The government announced that the unrealised aims of part 3 of the DEA would form part of the new Online Safety Bill, and that pornography would be put out of reach of children through robust age assurance (in this instance age verification mechanisms). However, while the Bill repeals the provisions of the DEA, as currently drafted, it does not guarantee that all pornography sites will be put beyond the reach of children, since the regulation will apply only to user-to-user or search services. It is widely understood that this was not the government's intention but an oversight in the drafting that failed to recognise the critical role age assurance can play in the landscape of regulation.

New legal, regulatory and treaty requirements are pushing the development of age assurance tools, and the commercial opportunity has been recognised by the private sector. Companies have stepped in to develop identity products and services including

[8] Digital Economy Act 2017, UK Public General Acts, 2017.

[9] Data Protection Act 2018, UK Public General Acts, 2018.

[10] Age appropriate design: a code of practice for online services, ICO, September 2020.

[11] Video-sharing platform (VSP) regulation, Ofcom, October 2020.

[12] Audiovisual Media Services Directive (AVMSD), European Commission, date accessed 29 March 2021.

[13] Draft Online Safety Bill, presented to Parliament by the Minister of State for Digital and Culture by Command of Her Majesty, May 2021

[14] General Comment No. 25 (2021) on children's rights in relation to the digital environment, OHCHR, March 2021.

[15] The Digital Economy Act 2017 requires commercial providers of pornography "to have robust age verification controls in place to prevent children and young people under 18 from accessing pornographic material." Although this legislation was passed, the guidance was never laid before Parliament by the appointed regulator (British Board of Film Classification) or implemented in practice.

[16] Online Harms statement made by Nicky Morgan (former Secretary of State for Digital, Culture, Media and Sport) on 16 October 2019.

a whole raft of age assurance products. They too decry the lack of clarity of expectations or regulatory framework.

Some efforts have been made to introduce standards for age assurance. The British Standards Institution produced the Publicly Available Specification (PAS 1296:2018) which sets out the basis for describing the levels of assurance offered by different methods of age checking.[17] The UK government is sponsoring the update of this standard and in 2021 it also produced a prototype of a UK digital identity and attributes trust framework. The framework introduces the concept of a trust mark and certification for the future and goes some way to exploring the kinds of elements that would engender trust in a range of identity products including age assurance products.[18] In May 2021, Baroness Kidron also introduced a Private Members Bill requiring age assurance systems for online or digital services or products to meet certain minimum standards.[19]

There is also a global push for shared standards and greater interoperability between age assurance solutions. The development of an international standard for age verification is underway, to be introduced by the International Standards Organisation (ISO).[20] The European Commission is also funding the euConsent project, which will develop standards for how age verification providers can share the checks they perform. All providers working as part of the scheme will be audited for the accuracy of their checks, as well as the privacy and data security protections they have in place.[21]

These initiatives provide a rich backdrop for any future regulatory action, but they also speak to the urgent need for a coherent intervention by the government. A comprehensive, sector-wide statutory framework for age assurance to ensure consistency, consumer trust and certainty is necessary for businesses to ensure that the tools they are using are fit for purpose.

There can be little exaggeration of the level of confusion that reigns — what are the risks, what is age appropriate, and what does good look like?[22] These questions can

[17] PAS 1296, Online Age Checking. Provision and use of online age check services. Code of Practice, British Standards Institution and EURIM Digital Policy Alliance, March 2018.

[18] The UK digital identity and attributes trust framework, published February 2021.

[19] https://bills.parliament.uk/bills/2879

[20] A working draft of this standard (PWI 7732 – Age Assurance Systems Standards) is due to be presented at the end of 2021.

[21] The euConsent consortium is currently consulting with stakeholders on developing an EU-wide age verification network, and will eventually launch a three-month pilot of the new system that is produced.

[22] During the transition period for the Children's Code, the ICO engaged with industry stakeholders on age assurance, many of whom were seeking clarity around the levels of risk arising from different types of data processing and the required level of age certainty needed to identify child users and mitigate the risks, the varying levels of assurance that different solutions provide, confirmation of which providers or types of solutions comply with data protection requirements and how to collect additional personal data required for age assurance while complying with the data

only by answered by a set of clear expectations with measurable standards that can be properly managed by the regulator. Age assurance without trust will benefit neither industry nor children. A set of clearly articulated standards that give credibility and consistency to the different age assurance tools and solutions will create the conditions under which the industry can recalibrate its relationship with children.

minimisation principle of the Children's Code. (See: Information Commissioner’s opinion: Age Assurance for the Children’s Code, 14 October 2021)

Why is age assurance needed?

Children have recognised needs and vulnerabilities that are specific to their age and development stage. A child is not eligible to vote, there are 'No Parking Zones' outside schools, a competitive track race for a child is shorter than a track designed for an adult and we instinctively shield a young child's eyes if something violent or upsetting happens in their environment. This is not because of their specific circumstances, but because they are a child.

In the digital world, children are routinely presented with information, behaviours and pressures that they do not have the developmental capacity to negotiate, whether pressured to expand their social network by befriending unknown adults, nudged to make in-game purchases, targeted by sexualised content or bombarded with advertising and misinformation. The normalising of services designed by and for adults creates an environment that is beyond a child's development capacity – the demands of which are difficult to navigate, often damaging and sometimes dangerous.

> **"If they're targeting people that are vulnerable, then how is that fair?"[23]**
>
> Young person, UK

> **"Digital play is mainly aimed at young people... and I just feel like they may have less maturity to know when the limit is to play a game."[24]**
>
> Girl, aged 15-17, UK

While the age of an individual child is not itself a perfect metric for capacity, it is widely understood that children develop different skills at certain points as they grow up. This is referred to as the 'evolving capacities of the child'.[25] Knowing the age or age range of a child offers a clear framework for designing with childhood milestones in mind and responding to the particular risks and opportunities for children at different developmental stages.[26]

Age assurance is simply a way for providers of digital products and services to know the age of their users. Age assurance alone will not deliver an age appropriate service but is a first step to ensuring that products and services provide children with the safety, security, privacy and freedoms to which they are entitled.

[23] 5Rights Youth Commission Workshop, 5Rights Foundation, 2019.

[24] Digital Futures Commission: The future of free play in the digital world, 5Rights Foundation, November 2020.

[25] The Principle of Evolving Capacities under the UN Convention on the Rights of the Child, Sheila Varadan, 2019

[26] 'Designing with childhood milestones in mind' from Digital Childhood: Addressing Childhood Development Milestones in the Digital Environment, 5Rights Foundation, December 2017.

When is age assurance needed?

In the UK, childhood takes place seamlessly online and offline. Services and products used in one environment have consequences in others. As children pick up a smart phone, ask Alexa to play a song or log on to a remote learning platform, they are connected to and impacted by digital technologies.

Importantly, children's experiences are not limited to services and products *directed at them.* Most children spend most of their time online using services that are *not directed* at them, for example, social media, streaming services, messaging apps and e-commerce sites.[27] Children also spend time on services from which they are specifically prohibited, for example, gambling services,[28] pornography sites[29] and dating services.[30] Additionally, many of their lived experiences are mediated by technologies that they have not chosen to engage with, for example, facial recognition technology in public places, predictive policing technology or algorithms used for allocating welfare resources. Digital technologies that engage children without their participation often affect them in ways they may not know.

The UK government's Verification of Children Online research project (VoCO)[31] highlights that a service's intended audience is often different from its actual audience, in part because of the ease with which children can claim to be older than they are through 'tick-box' age assurance. VoCO proposes a risk-based approach to age assurance, where services first assess the likelihood of a child gaining access before establishing the level of risk that the service presents.

Given the wide uses of digital technologies and the millions of services and products available, it is more fruitful to consider scenarios in which age assurance is *unlikely* to be needed, rather than attempt to identify those products and services that need to establish a child's age. For example, age assurance is not needed for:

- Products or services that are unlikely to engage with children or be of interest to children, such as a pension service, a hardware supplier, or an estate agent.

[27] Children and parents: Media use and attitudes report 2019, Ofcom, February 2020.

[28] The Gambling Commission survey of 11-16 year olds in England and Scotland found that 9% spent their own money on gambling activities in the seven days prior to taking part in the survey, and 37% had gambled in the last 12 months. 1.9% were classified as 'problem' gamblers and 2.7% were classified as 'at risk'. Young People and Gambling Survey 2020, Gambling Commission, November 2020.

[29] The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches, Neil Thurman & Fabian Obster, May 2021

[30] Apple and Google let underage users on dating apps, says Tinder, Telegraph, April 2021.

[31] VoCO (Verification of Children Online) Phase 2 report, Department for Digital, Culture, Media & Sport, Government Communications Headquarters, and Home Office, November 2020.

- Products or services specifically designed for children that have already met the criteria of child centred design in the development of their service.32
- Products or services specifically designed to be shared by a mixed audience that have already met the criteria for child centred design.
- Products or services that require identification of a unique user, through which they have already established the age of that person, for example, the NHS, a bank, and some (but not all) education services.

News media and online encyclopaedic resources that children have a right to access[33] may be exempt from age restrictions or age assurance, even if children are likely to access them, but should consider age ratings (labelling) and content warnings. Such exemptions should not be used as cover for aggressive marketing or targeting children.

In most other cases, a product or service is likely to need to take one of two routes:

- use an appropriate age assurance method to establish the age or age range of their child users, or
- redesign to meet the criteria appropriate for a mixed audience that includes children.

Sometimes this is a question of choice, but in other circumstances it may be mandatory, for example required by law or required as part of an industry code.

Below are a few of the most common areas where age assurance is likely to be mandated or required. The list is indicative rather than exhaustive, recognising that services are varied and multifaceted and that it may be part of, rather than the entire product or service that requires age assurance.

Age-restricted goods

There are currently 56 types of products spanning 16 sectors that are age restricted in the UK. For example, you must be 16 to buy a lottery ticket or scratch card,[34] and 18 or over to purchase knives[35], cigarettes,[36] or alcohol.[37] In order to sell these age restricted products, age verification will be required.

[32] Those that offer high levels of privacy, safety, security, and are age appropriate for the age or age range of their users as a result of child impact assessment and risk mitigation.

[33] Article 17, UNCRC states that every child has the right to "access to information and material from a diversity of national and international sources."

[34] As of April 2021, the minimum age for National Lottery participation will move from 16 to 18 years old. See more from: National Lottery minimum age will rise to 18 from April 2021, Age Checked, data accessed 16 February 2021.

[35] Selling, buying and carrying knives, GOV.UK, data accessed 16 February 2021.

[36] Rules about tobacco, e-cigarettes and smoking: 1 October 2015, GOV.UK, 9 July 2015.

[37] Alcohol and young people, GOV.UK, date accessed 16 February 2021.

Age-restricted services

There are many age-restricted products and services. Gambling services,[38] commercial pornography sites[39] and dating sites are restricted to over 18, as are some violent interactive games. Social media sites are largely restricted to those above 13, but some have a minimum user age of 16[40] or have particular features, such as direct messaging that can only be used by those over 16.[41]

Age-restricted content

Some content has age restrictions, for example, films with ratings above U and PG, content on video sharing platforms that is violent or sexual in nature, or age-restricted advertising for food and soft drinks high in fat, salt and sugar (HFSS).[42] The UK's Video-sharing platform guidance, produced by Ofcom, requires services to deploy appropriate measures to protect under-18s from harmful material, including anything which might impair their physical, mental or moral development.[43] Ofcom also regulates video on-demand services with statutory requirements to prevent the inclusion of harmful content.[44]

Age-appropriate experiences for particular age-groups

Age assurance can ensure services are delivered to the intended age groups, such as sexual health advice, education products or apprenticeship/training opportunities. It can also be used to tailor information, design features or content to the age of the user. For example, a gaming service may wish to automate 'time outs' or create 'less stickiness' for younger children, or a news media site that usually sits behind a paywall may wish to give free access to teenagers.

Data protection

Data protection is currently one of the biggest drivers of the requirement for age assurance. The EU's General Data Protection Regulation (GDPR) regime states "children merit specific protection with regard to their personal data."[45] Age assurance also forms

[38] The Gambling Act (2005) established the minimum legal age of gambling at 18.

[39] Pornhub recently announced changes requiring anyone uploading content to the site to verify their identity in a move to tackle child sexual abuse on the platform. Pornhub will partner with Yoti – a digital identity platform – using age assurance technology to authenticate users seeking to upload content, or users giving consent for their content to be downloaded. See more from: Pornhub Sets Standards for Safety and Security Policies Across Tech and Social Media; Announces Industry-Leading Measures for Verification, Moderation and Detection, Pornhub press release, 2 February 2021.

[40] Minimum age to use WhatsApp, WhatsApp FAQ.

[41] In April 2020, TikTok announced it would only allow direct messaging for users aged 16 and over.

[42] Age-restricted ads online Advertising Guidance (non-broadcast), CAP, 2021.

[43] Video-sharing platform guidance: Guidance for providers on measures to protect users from harmful material, Ofcom, October 2021.

[44] On-demand programme services: who needs to notify Ofcom?, Ofcom, September 2021.

[45] Recital 38 of the General Data Protection Regulation states that "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."

part of the UK's Age Appropriate Design Code[46] requiring services "likely to be accessed" by children under the age of 18 to have age assurance mechanisms that are proportionate to risk, or design their services to be age appropriate for all users.[47] This is an approach being taken up in other jurisdictions.[48] Strategic litigation focused on the use of data of under 13s is also increasingly being used to force compliance with data protection regimes, including COPPA in the US.[49]

> **"I am... worried about my data being shared because, despite having my privacy settings on, I can see my preferences in ads and often get spam mail due to my email being shared."**[50]
>
> Girl, aged 18, Canada

> **"Stop selling our data, phone numbers, etc. to companies, for advertisements."**[51]
>
> Boy, aged 14, UK

> **"It's a bit scary to think about why free apps have so much money. I also wonder about their motives when they make a free app. Maybe they sell my pictures, data etc."**[52]
>
> Girl, aged 17, Norway

[46] Age appropriate design: a code of practice for online services, ICO, September 2020.

[47] Age appropriate application, ICO, September 2020.

[48] Children Front and Centre: Fundamentals for a child-oriented approach to data processing [Draft Version for Public Consultation], Irish Data Protection Commission, December 2020.

[49] In 2019, The US Federal Trade Commission took action against Music.ly alleging violation of children's privacy law.

[50] Our Rights in a Digital World: A snapshot of children's views from around the world, 5Rights Foundation, March 2021.

[51] UNCRC Young Writers Group, 5Rights Foundation, August 2020.

[52] Our Rights in a Digital World: A snapshot of children's views from around the world, 5Rights Foundation, March 2021.

What level of assurance is needed?

The level of assurance should be proportionate to the nature and level of risk presented by a product or service in relation to the age of the child. The cumulative nature of risk must also be taken into account, as multiple design features or different parts of a user's journey combine to create greater risks. For example, a service that allows public visibility settings for user profiles as well as direct messaging between users will carry more risk than a service that allows only one of these features. The less intrusive and risky a service is, the lower the bar of assurance needed to identify a child user. For example, a charity whose interactions with users are limited to announcing campaigns, distributing a newsletter or promoting fundraising activities, and which does not share user data with third parties or allow comments on their site's blog posts, will need little age assurance. Indeed, if a service is entirely appropriate for all those it impacts on — including children — it does not need to establish the age of its users at all.

The following common factors should be considered:

Legal and regulatory requirements

Regulation may determine the level of age assurance needed. For example, it is required by law that a person prove they are over 18 to gamble or buy alcohol – which requires a high level of assurance.

Age assurance systems should also meet legal requirements for data processing. In the UK, services can process personal data with the consent of the user, or five other lawful bases including processing that is necessary for: fulfilling a contract with the individual; complying with the law; protecting someone's life; performing a task that is in the public interest; the data controller's legitimate interests or the legitimate interests of a third party (except where there is a good reason to protect the individual's personal data which overrides those interests).

The nature and scale of the risks or opportunities that a service presents

Services carry different levels of risk depending on their functionalities and design features. The level of risk is obvious for some services, such as those that facilitate anonymous interaction between unknown users, putting children at risk of grooming, radicalisation or extortion. For others, risks can be less obvious, such as 'sticky' or 'invasive' features which may make it difficult for a child to put their device down and may interrupt their sleep.

By contrast, some services may offer positive age-specific features such as 'time-outs' or opportunities for easy disengagement. For example, a service that adheres to data minimisation principles, has no direct messaging and does not feature 'adult' material may still need to use age assurance to tailor some aspect of its service, but may require a lower level of age assurance given the lower risk overall.

One often forgotten consideration is the cumulative and interconnected nature of risk.[53] A service that encourages public profiles that also promotes or recommends harmful, violent, sexual or body dysmorphic content, enables private messaging, rewards those with large followings and shares user data widely with third parties, has with each feature added to the risk for a child. As the risks add up, so too does the requirement for a higher level or age assurance. Importantly, children most vulnerable offline tend to be those most vulnerable online which may be another factor in assessing risk of a particular service.

Establishing risks

The 4 Cs framework groups risks faced by children in the digital world into four broad categories: content, contact, conduct and contract. They can be used as a way to identify, understand and categorise risks to children online.

Content: A service carries risk when a child or young person can be exposed to harmful material. This includes content that is inappropriate for their age, including pornography, extreme and real-life violence, discriminatory or hateful content, disinformation and content that endorses risky or unhealthy behaviours such as disordered eating or self-harm. If a service has few community rules and little content moderation, it presents greater risk than a service that has well-understood terms of use that are robustly upheld.

Contact: Contact risks are created when a child or young person is able to participate in activity with a malign actor, often, but not always, an adult. These risks can lead to child sexual exploitation, grooming, harassment, stalking, blackmail, unwanted sexual advances or location sharing. Services that allow private messaging, make a child's location visible, or facilitate the introduction of unknown adults to children via friend suggestions are inherently risky.[54]

Conduct: Services can create conduct risk by facilitating or even encouraging behaviours and activities that cause harm to young people, both as victims and perpetrators. These activities include bullying, sexting, revenge porn, trolling, threats and intimidation, peer pressure and loss of control of digital legacy/footprint.

[53] Risky-by-Design, 5Rights Foundation, date accessed 16 February 2021.

[54] 75% of the most popular social media services globally facilitate the introduction of strangers to children. Of the 12 most-used social platforms globally (sourced from Revive.Digital), 9 platforms use automated-decision making systems to recommend profiles of strangers to users.

Contract: Some services expose children to inappropriate commercial and contractual relationships or pressures. These can result in harm from compulsive use, gambling, targeted advertising, hidden costs or loss of control over personal data. Services that are particularly aggressive in their data gathering and/or commercial targeting may need to establish the age of children so as not to break data protection law or put children in overly commercial environments.

The 4 Cs can be used in child impact assessments to assess risk. Child impact assessments are fundamental to designing and developing services that are age-appropriate by default. The output from a child impact assessment allows providers to identify both risky and positive elements of their service, and where necessary, redesign features or operating processes to mitigate risk or increase beneficial outcomes.

There is currently little formal help for services to interpret risk and harm, as illustrated by research from the Verification of Children Online (VoCO) project.

VoCO identified conditions and tools which industry felt would help them to identify and mitigate risks.[55] These include:

- Consistent definitions of threats/potential harms and agreement on the risk level posed by specific service features
- Agreement on the likelihood of the threat posed to children in given scenarios
- Agreement on the best options for risk mitigation
- An agreed risk assessment with risk case studies

Risk assessments

Risk assessments are a norm across all commercial sectors and provide a way of assessing risk. 5Rights is working on a Child Risk Assessment framework specifically for the tech sector, building on the findings of the Digital Futures Commission on Child Rights Impact Assessments in the digital environment.[56] It follows the step-by-step process used by most risk assessments frameworks that support companies to identify, analyse, assess and review their service or product.

- **Know your customer** - who is it that you are impacting (in this case a child or children).
- **Map impact** - interrogate the impact of your service, including the impact on underage children who should not be using it.

[55] VoCO (Verification of Children Online) Phase 2 report, Department for Digital, Culture, Media & Sport, Government Communications Headquarters, and Home Office, November 2020.

[56] Child Rights Impact Assessment: A tool to realise child rights in the digital environment, Mukherjee, S., Pothong, K., Livingstone, S. and 5Rights Foundation, 2021.

- **Gather evidence** - this will be collected on a risk register that should be created through three lenses: risk, rights and safety-by-design.
- **Consult** - in and outside your organisation. Solutions may come from surprising places including children themselves.
- **Assess, analyse and appraise** - what you discover may be surprising or obvious and different risks are likely to require different mitigation strategies.
- **Recommend** - this is your plan of what to do.
- **Publish and report** - transparency gives confidence to users and regulators. It also provides learning for others and sets a bar for your organisation.
- **Monitor and review** - digital products and services are rarely static. Small changes can have big impacts and constant vigilance and iteration is necessary.

These eight steps can be used to create a product, to assess an existing product or to look at the intersection between products that may together create risk. They must reveal known harms, unintended consequences and emerging risks, and take into account not only content but contact, conduct and contract risks, as per the 4 Cs risk framework.

The age or age range of the child user

It is not always the case that younger children need a higher bar of age assurance. Younger children often have greater parental supervision[57] and largely access or are recommended fewer age-inappropriate products and services.[58] Counterintuitively, this means that often *more* support and protections are needed for older children, particularly as many children are given smartphones when starting secondary school, introducing them to a whole world of products and services designed for adults when they are only 11 years old.

Age and age range must be considered *in relation to the nature of the service*, since some content or services may be particularly difficult or damaging to children of different ages. For example, the promotion of unhealthy fast diets or muscle-building routines have a disproportionate impact on teenagers.[59]

[57] For example, younger children are more likely to have technical controls set up by their parents on their gaming devices to control their gaming and online use. Ofcom report that over half of parents of 5- to 7-year-olds and 8- to 11-year-olds whose child play games say they have some sort of controls in place: such as time-limiting software, controls to stop the child playing games above a certain age rating, or controls to prevent them from going online. In contrast, four in ten parents of 12- to 15-year-olds (39%) have these controls in place. See more from: Children and parents: Media use and attitudes report 2019, Ofcom, February 2020.

[58] A third of 12- to 15-year-olds have said they have seen something 'worrying or nasty online', making them almost twice as likely as 8- to 11-year-olds (18%) to see this type of content. See more from: Children and parents: Media use and attitudes report 2019, Ofcom, February 2020.

[59] According to the Good Childhood Report 2021, a greater proportion of girls have been unhappy with appearance than with any other area of life (e.g. school, friends, family) across the years 2009-2021. Social media has been criticised as a

In many cases, the alternative to age assurance is to make a product or service appropriate for a mixed audience that includes children. It is important to note that many of the changes necessary to make a service age appropriate do not require additional or new technology, but rather require services to disable some of their more intrusive design features such as geolocation data tracking, private messaging or targeted advertising.

source of insecurity for teenage girls in particular, and Facebook's own internal research found that “We make body image issues worse for one in three teen girls."

What are the different types of age assurance?

There are many different approaches to ascertaining the age or age range of users. Collectively these should be referred to as **age assurance** but are often collectively referred to as age verification. They vary widely in ambition. Some seek to verify an exact act, **age verification (AV);** others to estimate an age or age range, **age estimation (AE);** and some are designed to identify a specific person, **identification (ID).**

These differing ambitions are set out in the ten approaches below. In trying to understand the risks and benefits of one approach over another, it is important to note that they are often combined, sequenced or repeated within one user journey, or even in a single assessment of age.

Age assurance tools may be introduced at the point of access to a service, or they may be used sequentially in different parts of a product or service. For example, an e-commerce site may have no initial age checks, but may ask to verify a user's age if they wish to purchase a restricted product.

For this reason, there is no absolute line between all of the approaches, but they have been categorised to allow an analysis of their strengths and weaknesses.

Figure 1 maps the ten approaches against those set out by the VoCO project and the standards in the Age Appropriate Design Code. Where concepts are the same or similar but terminology is different, our choice of language is explained.

5Rights Foundation	Verification of Children Online (VoCO)	Age Appropriate Design Code	Type	Notes
1. Self-declaration	Child provided	Self-declaration Technical measures	AE	Technical measures which discourage false declarations of age are referenced in as part of self-declaration.
2. Hard identifiers	Large central databases Distributed information	Hard identifiers	ID/AV	In both cases means accessing existing data bases of previously establish identification data.
3. Biometrics	Body metrics Biometrics	x	ID/AE	Body metrics and biometrics have been combined into one category to encompass data inferred from physical characteristics.
4. Profiling and inference models (AI)	Behavioural	Artificial intelligence	AE	Data that is provided by looking at user behaviour.
5. Capacity testing	x	x	AE	
6. Cross-account authentication	x	x	AE	
7. Third party age assurance provider a. Digital identity b. B2B c. Age tokens	Trusted online provider authentication Age check exchanges	Third party age verification services	ID/AV/ AE	This involves several approaches but is unified by the fact that there is a dedicated third party that provides the assurance.
8. Account holder confirmation	Digital parent provided	Account holder confirmation	AV/AE	
9. Device/ operating system controls	X	Account holder confirmation	AV/AE	
10. Flagging	Peer provided	Technical measures	AE	Flagging is identified as a distinct category and is a subset of technical measures as defined by the ICO.
x	Environmental	x	AE	The use of environmental data is referenced in emerging technologies.

Figure 1: Ten approaches to age assurance

Data used for age assurance

Many different data sources are used for age assurance.[60] In its most rudimentary form, that data source could be a child (or their parent/carer) simply telling a service their age, age range or date of birth. At the other end of the spectrum, the data source might be a hard identifier (official documentation such as a passport or driving licence) or be provided from government held records, for example by checking a user's name, address or national insurance number against existing databases.

A user's age can be checked against publicly held datasets, including medical or school records, credit or tax databases and other national registers. The quality of the data can vary depending on the method of collection, and datasets may well contain errors or omissions. Private databases can also be used, such as those held by banks or by mobile phone providers, who would have conducted initial age or identification checks to allow a user to open a bank account, take out a credit card or purchase a mobile phone.

Many of these official datasets contain more information about adults than children, particularly those relating to government services. While in many cases it is more efficient and more appropriate for a service to confirm a user is an adult rather than a child, this approach presents limitations in contexts where age restrictions are set below 18 or where a product or service is tailored to the age of the child. There are also justified concerns about security risks when centralised databases are used in age assurance.

Data used to assure age can also be derived from contextual information about a person's use of a service, for example, the type of content they frequently interact with, the location they are accessing the service from, the times and frequency they are 'active', the ages of the users they interact with, or they can be put into an age range by their ability to complete a given task or their use of language.

Biometric data relating to the physical or behavioural characteristics of a user, such as their facial features, iris or voice scans, finger and palm print, gait, the speed at which they type (keystroke dynamics) or the way they pinch a screen or scroll, can also be used to estimate age. This data might be given voluntarily to establish age or identity, for example a Touch ID to unlock a device, or it may be gathered in the course of use. Data relating to physical characteristics such as height and gait are commonly collected by devices such as phones or wearable fitness trackers, and can indicate the likely age of a user.

[60] The Verification of Children Online (VoCO) project group the data sources into three categories as user reported, officially provided and automatically generated in their Data Source Type Taxonomy (DSTT). 5Rights has divided biometric data and data relating to capacity testing into separate categories.

Approaches to age assurance

1. Self-declaration (AE)

Self-declaration is often referred to as ‘tick box’ age assurance and is associated with the current failure to truly establish the age of children online. It requires a user only to enter their birthdate, or to tick a box that asks if they meet the minimum age of use. However, when used in conjunction with additional proactive checks and technical measures, it can be much more effective. For example,

- When a child enters a date of birth that indicates they are below the minimum age, the service can deny access and block repeated attempts from the same IP address, even if the birthdate is subsequently changed.
- Language and framing can elicit more truthful age declaration, for example, “enter your date of birth” rather than “confirm that you are over 13.” Then, as above, services can block repeated access attempts if the user is below the minimum age.
- Where a child has submitted a date of birth that indicates they are above the minimum age, their provided age is checked again later in the process, such as when they next log in (“Can you remind us of your date of birth?”). Children who gave a false date of birth on registration may not remember the date of birth they gave when asked at a later stage or on a different day. Any discrepancy can be escalated to a moderator, who may ask for further proof of age.

It may be used in combination with other data sources, such as biometric data or information derived from how a child interacts with a service. Some services use self-declaration as an initial step for age assurance before asking users to provide other information, such as a photo ID or facial image, against which they can compare the declared age.

TikTok asks users to self-declare their date of birth when they create an account. If a child enters their date of birth and they are below the minimum age of use (13), TikTok will bar them from creating an account if they go back and try to enter a different age.

Summary:

- Self-declaration alone offers a relatively low level of assurance.

- Self-declaration puts responsibility on the child to report their age truthfully.[61]
- Generally, services do not reveal if additional steps are being taken, such as blocking repeated access attempts or checking age at different stages in the user journey, meaning the level of assurance is unclear and can be higher *or* lower than imagined.
- Children may not understand the impact that pretending to be older could have on their user experience or on their digital identity/footprint.
- Self-declaration is easy for children to use and convenient for services that may pose little risk to children but may wish to offer additional information or tailored services.

This form of age assurance is only suitable for low risk and low intrusion products and services which do not include features or operate in ways that impact negatively on children.

2. Hard identifiers (AV/ID)

Age assurance using hard identifiers requires users to provide verified sources of identification to prove their age. A user may be asked to upload a copy of a photo ID that displays their date of birth, such as a passport, or they may be asked to provide other identifying information, such as their name, address, school, NHS number or national insurance number that can be checked against official databases. Some identity documents show a user's date of birth 'within-record', such as a passport, while others, such as a credit card, may not provide the user's exact age or date of birth, but can act as a proxy (you must be 18 or over in the UK to have a credit card.)

Hard identifiers, correctly attributed to the user, provide a high level of age assurance, because these documents or credentials have themselves been through a verification process.

As of September 2020, YouTube asks its users to be signed in to their account when viewing age-restricted videos, and in the EU (to comply with the Audio-visual Media Services Directive) they must prove they are 18 or over by providing a valid ID or credit card.[62]

[61] Most social media require users to be 13 or over to use the service, but 42% of 5- to 12-year-olds in the UK use social media. See more from: Children and parents: Media use and attitudes report 2021, Ofcom, April 2021.

[62] Using technology to more consistently apply age restrictions, YouTube Official Blog, 22 September 2020.

Summary:

- Some hard identifiers contain many more attributes than age, such as name and address, or sensitive personal data such as race and gender. The more personal data that is captured to establish the age of users, the higher the standards of security, data retention and storage and accountability need to be.
- It may be that additional information, such as a facial scan or confirmation from another individual (such as a parent) or institution (such as the child's school) is necessary to match the hard identifier with the user.
- If a child uses another person's ID[63] or a falsified document, they may be in danger of committing a crime.[64]
- Widespread use of hard identifiers for age assurance may disadvantage children who do not have access to official documentation, for example due to immigration status, language barriers or lack of funds.[65]
- The information gathered about an individual is commercially valuable, increasing the risk that it will be kept or used for purposes other than identifying the age of users.[66]

The use of hard identifiers offers a high level of assurance but presents risks of privacy violations and potential exclusion. Hard identifiers are most commonly used for age assurance by services that are restricted to users over 18, which puts the emphasis on proving users are adult.

3. Biometrics (ID/AE)

Biometric data such as height, gait, voice, facial features, keystroke dynamics or finger and palm prints can be used to identify a particular person or to estimate their age through techniques such facial scanning, natural language processing and behavioural analysis.

[63] There have been documented cases of children under the age of 18 setting up OnlyFans accounts (an 18+ restricted service) using a 'borrowed adult ID'. A BBC reporter posing as an underage person was also able to set up an account using a photo ID that belonged to their older sibling. See more from: Teenagers breaking law to sell explicit selfies on social media, The Times, April 2020.

[64] See: https://www.safeguardingsheffieldchildren.org/sscb/children-licensed-premises/false-id/print.

[65] The ICO's age assurance opinionstates: "There is a risk of excluding or indirectly discriminating against individuals who lack the necessary documentation or data, such as credit history. Organisations should therefore take a holistic approach to what hard identifiers they accept. Organisations should also take the Equality Act into account and the requirement to ensure reasonable adjustments for those with protected characteristics. For example, they may wish to consider accepting a broad range of hard identifiers such as a GP letter, a utility bill or letter from a social worker or social housing provider, rather than only relying on passports, driving licences or credit cards."

[66] Under the General Data Protection Regulation (GDPR), purpose limitation is a requirement that personal data be collected for specified, explicit, and legitimate purposes, and not be processed further in a manner incompatible with those purposes (Article 5(1)(b), GDPR).

Facial recognition identifies an individual, for example the Face ID used to unlock a mobile device or tablet, whereas facial analysis, one of the most widely used forms of biometric estimation for age, can estimate the age of a face without recognising or identifying the individual. Facial analysis compares the user's facial features against large datasets that have been used to train the technology through machine learning. Facial analysis is inclusive of those who may not be able to present a valid ID document. It can also be used in privacy preserving ways if services discard the facial image once it has estimated a user's age.

Biometric data may be processed in real-time to assure age or may be used in combination with contextual data, for example how long a user spends on a service, to build a long-term picture or 'age profile'. Biometric estimation is sometimes used as an additional layer of assurance after an initial age check using hard identifiers or self-declaration.

GoBubble, a social networking site made for children, uses facial analysis technology to conduct age assurance checks. The service asks for the child's birthday, after which they are asked to take a 'selfie' to prove they are a child. When the selfie has been taken, the child selects "Check My Age" at which point the anonymous age estimation technology determines if the child's face matches the age range of their self-declared age. Once the child's age has been estimated using facial analysis, the technology provider can confirm if the estimated age matches the age range of the child's self-declared age. The 'selfies' obtained for age assurance are then instantly deleted and the child has access to the service.[67]

Summary:

- The process of estimating age using biometric data is often opaque to users and they may have little understanding of the type of data that is collected or how it is used, shared and stored.
- While the technology has advanced, in some cases facial analysis has failed to recognise characteristics of very light or very dark skin.[68] Any variances in accuracy based on gender, skin tone or other characteristics should be clearly identified and mitigated.[69]
- The accuracy of facial analysis varies depending on the age of the user and has been shown to be less accurate for younger children. Additionally, the margin of

[67] This age estimation technology is provided by Yoti. See more from: Developing our anonymous age estimation technology, Yoti, October 2020.

[68] Passport facial recognition checks fail to work with dark skin, BBC News, October 2019.

[69] The ICO states in its opinion on age assurance that "organisations must ensure that any automated decision-making system is sufficiently statistically accurate and avoids unjustifiable discrimination. This includes systems provided or operated by third parties."

error means that children who are close to an age boundary (18) may be at risk of being falsely verified.

- The efficacy and impact of biometric estimation on children with disabilities or craniofacial differences is as yet unclear.[70]
- Increasingly, children are being asked to provide facial images to enter buildings or access devices, creating conditions in which those who don't wish to provide this kind of data could be denied access to places and services.
- Faces can be read for emotion, attention, comprehension and mood, the data from which can be used to affect real world outcomes for children.[71]
- Without formal standards and accountability, biometric data may be misused to build up a child's data profile.

Biometric data can offer varying levels of assurance from very low to very high, but in the absence of standards and accountability, as well as independent audits and transparency requirements, issues of purpose limitation, efficacy, discrimination and security may arise.

4. Profiling and inference models (AE)

> "I didn't know the internet knew that much about you. I thought it's just what you put out there."[72]
>
> Young person, UK

Profiling refers to the processing of data to analyse and infer information about a user, or to predict and determine aspects of user behaviour. Profiling for the purposes of age assurance is widely referred to as using 'AI' or 'inference models' to estimate age. Data used for profiling is made up from information users *choose* to share about themselves, and information that is *inferred* or automatically collected from their engagement with services, for example, how long they spend on a webpage, where their cursor hovers, the times of day they access a service and their interests, location and friends.[73]

Service providers separate users into groups, variously referred to as 'user groups,' 'target markets,' 'audiences' or 'FLoCs' (federated learning of cohorts) based on their

[70] The ICO's age assurance opinionwarns "systems based on biometrics such as hand or facial structure may perform poorly for people of non-white ethnicity, or for those with medical conditions or disabilities that affect physical appearance. There is also a risk from newer techniques that have not been effectively tested or screened for these risks."

[71] This AI reads children's emotions as they learn, CNN Business, February 2021.

[72] Youth Commission Workshop, 5Rights Foundation, 2019.

[73] Also known as 'social proofing' or 'crowd proofing,' where the feasibility of data gathered through this source is being reviewed by the Age Check Certification Scheme. See more from: Social Proofing, Age Check Certification Scheme.

interests, activities and likely behaviours. Primarily used for commercial reasons, group-based profiling allows companies to effectively target users with advertising and promote content to curated audiences. This profiling or 'surveillance'[74] builds highly detailed profiles, for example, a service may determine a child's height, daytime location, interests and best friends, even an understanding of their sexuality, if they live with their parents or carer, have a dog or live in owned or rented accommodation – the information is infinite.

These data points can act as a proxy for estimated age[75] and can be matched against a user's self-declared age or another given data point to provide an additional layer of assurance.

Facebook announced in July 2021 it will be making greater use of AI technology to infer the real age of their users. They will use multiple signals such as the age of users indicated in birthday messages and comparing the self-declared age of users with the age indicated in linked accounts, such as Instagram.[76]

Summary:

- Profiling and inference create a significant tension between data processing and a child's right to privacy.[77]
- Profiling and inference may offer a low level of assurance if the quality of the data is poor or the dataset contains errors or omission.
- Profiling is very likely to result in the collection of data beyond that which is needed for age assurance.[78]
- Data derived from profiling and inference models is often shared with third parties and can be used in ways that has a detrimental impact on children.

Profiling and inference avoid creating the friction in a user journey of an age screen or age gate. It can also help services identify children who have wrongly claimed to be older than they are who can then be asked to provide additional information to

[74] The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Shoshana Zuboff, Jan 2019.

[75] Following the Italian Data Protection Authority's orders against TikTok, Guido Scorza, the official in charge of data protection, suggested TikTok could estimate the ages of users by looking at their content, groups of friends and how they interact with their peers. "It may not be possible to distinguish between a 9 and a 10-year-old user, but it should be possible to distinguish between a 9-year-old and a 13-year-old."

[76] How do we know someone is old enough to use our apps? Facebook press release, July 2021

[77] While inference can seem like a less disruptive or intrusive way for services to assure the age of their users, this approach may constitute further intrusion on children's privacy

[78] The ICO states in its opinion an age assurance that "profiling data gathered for age assurance must not be used for any incompatible purpose" and that "the Commissioner will take action in the event that personal data is misused under the guise of or during processing for age assurance."

verify their age. However, it presents an almost insuperable problem of unwanted data collection and surveillance and risks identifying younger users only after they have been engaging with a service that is not age appropriate.

5. Capacity testing (AE)

Capacity testing allows a service to estimate a user's age based on an assessment of their aptitude or capacity. For example, a child may be asked to complete a language test, solve a puzzle or undertake a task that gives an indication of their age or age range. Services can use capacity testing to assure age without collecting personal data from children.

> The Chinese app 'Baby Bus' can be set to 'go to sleep' after it has been used for a predetermined amount of time. At this point, the user is asked to recognise traditional Chinese characters for numbers – a simple test for adults but a challenging one for young children. This is designed to prevent children from changing the settings on their own.

Summary:

- Game-like language or aptitude tests are a child-friendly method of age estimation but can be completed by an adult or older child on behalf of a younger child.
- Capacity is not equivalent to age, and many children of the same age have different language skills and problem-solving abilities. These variances may preclude access to services for children with lower aptitudes.
- Capacity testing may only indicate that a child is likely to be above or below a certain age, rather than their exact age or age range, making it difficult for services to enforce age restrictions on this basis.
- There is significant scope for innovation in this field since much of what is understood about users from current methods of profiling, such as keystroke dynamics, speed of response, use of emojis etc., has not yet been repurposed for capacity testing.

Capacity testing is a good way of minimising the amount of personal data collected about a child but without further measurable and agreed standards, are not suitable for services where a user's exact age is needed.

6. Cross-account authentication (AE)

Cross-account authentication is where a child uses an existing account to gain access to a new product or service. These accounts are often with large companies such as

Apple, Facebook, Google or Twitter. In this form of authentication, the provider (the company) confirms that the user is who they say they are by asking them to enter the correct username and password for their account.[79] In some cases, additional confirmation is required, for example via a one-time password (OTP).

Having authenticated the user, the provider (original company) allows the new service to access, read or receive user data via an API (Application Programming Interface). This data *could* be limited to a child's age (as a single attribute) but in practice, the data shared usually includes other data such as the user's name, location and email address.[80] Once the accounts are linked through the API, the original provider can gather data from the new service (often a condition of providing the log in), building an even greater picture of the child.

A key issue with this method is the lack of understanding about what is being shared and whether age is being checked at all. Our research has shown that child users can access some 18+ restricted sites using this method,[81] suggesting this approach may be configured to increase data collection rather than assure age. Nonetheless, if the data sharing between services and authentication providers was subject to minimum standards, cross-account authentication has the potential to offer a convenient method of age assurance for both users and services.

Summary:

- The level of assurance is determined by the method used by the original authenticating provider, which could be low or high which can undermine the very act of assurance.
- There is a lack of transparency around the data sharing that takes place in cross-account authentication.
- Data sharing between the authentication provider and the service often results in more data being shared than is necessary to assure the age of user.
- The sharing of data means that both the authentication provider and the service being accessed are creating and owning data profiles of children that can be used for other purposes.
- Widespread use of big tech companies for age assurance may further entrench their market dominance.

[79] How Tokens Work in Using the Graph API, Facebook for Developers.

[80] When signing in to the video-sharing service Triller via an existing Twitter account, users must share their profile information and account settings, email address, accounts they follow, tweets they have posted to their timelines, permission to follow and unfollow accounts, post updates to their profile and account settings, post and delete content, and mute, block and report accounts.

[81] 5Rights was able to sign-up for an OnlyFans (18+ subscription-based digital membership service) account by logging in via Google, using an account created as a 13-year-old. This age was provided to Google through self-declaration.

Cross-account authentication can provide convenience for children by removing the need to prove their age every time they access a service, but as currently deployed it provides an unknown level of assurance. Without transparency around what data is shared, it also risks violating children's privacy and further embedding the market dominance of a handful of companies.

7. Third party age assurance provider (ID/AV/AE)

Third party age assurance providers are companies that offer age assurance or identity confirmation services. They work in multiple ways and offer services direct to users, such as digital IDs, or direct to businesses via API solutions, background checks, or tokenised age checking.

a) Digital Identity (ID/AV)

A digital identity is a digital representation of a person's identity. Digital identities can be made up of a number of attributes or 'credentials', such as a person's name, date of birth, their school or university or address. They provide users with a way to prove their identity when they wish to access a product or service that requires identification or age assurance.

The user first provides a third party digital identity provider with identity documents or credentials, such as a scan of their passport, their national insurance number and a facial image. These can be stored as digital 'wallets' that allow users to share only the attributes required to prove their identity or an aspect of their identity, in order to establish that they are eligible for or entitled to something. This means users can withhold some identifying information or limit the attributes they want to share with a service. Some services allow users to see a record of the credentials they have shared, at what times and with which services, providing greater oversight of their data footprint.

Digital identities are reusable and often free for users. They also have the potential to widen access to those who do not possess a government issued ID document. While most third party digital identities are designed to be data minimising, many services require that a pre-determined set of attributes is shared from a user's digital ID, for example, name, photo and date of birth, instead of simply the user's age. This undermines the enormous potential of digital identities to offer a privacy preserving and data minimising method of age assurance.[82]

[82] The ICO's April 2021 Digital Identity Position Paper states "any digital identity system needs to give special consideration to how it safely accommodates and protects children. Undertaking a data protection by design and default approach, and where relevant conforming to the ICO's Age Appropriate Design Code, helps to mitigate such risks."

Yubo, a social network aimed at 13-25 year olds uses the verification provider Yoti to assure the age of its users. To sign up for a Yubo account, a user must first create an account with Yoti through the 'My Yoti' app, where initial age checks are conducted using facial analysis.[83] If Yoti estimates the user is below the age of 25, they ask for a hard identifier to verify their exact age. When registering for a Yubo account, a user is prompted to grant access to their 'My Yoti' account by entering a password/pin code. The user is then told about the information that will be shared with Yubo from their 'My Yoti' account (their photo, date of birth, gender and a Remember Me ID).[84] The user is granted access once this information has been shared with Yubo and if they meet the age requirements. A record of the data that has been shared with services and the time it was requested is stored on the 'My Yoti' app and can be accessed by the user.

Summary:

- The use of digital identities can reduce the need for users to repeatedly provide documents or other official sources of information. It has the potential to minimise data sharing whilst providing a robust measure of age, though in practice this is undermined by the demands of service providers for additional data.

- Digital identity providers can restrict the shared attributes to only the user's age (sometimes referred to as age token or age check), but as above this is currently rare because of the data sharing practices of services and identity providers.

- If attributes other than age are routinely shared, it means that age restrictions could be used as a proxy for other restrictions and/or demands for data that violate children's rights, for example, making decisions based on gender or location.

- The digital wallet can be expanded to include many attributes or be restricted to one or two, meaning that it could carry other useful information such as exam results or confirmation that the user has completed a training course.

- Amassing huge data sets and holding personal information in centralised or linked databases can present serious security risks,[85] from hacking or fraud to commercial misuse.

[83] Developing our anonymous age estimation technology, Yoti, October 2020.

[84] A Remember Me ID is generated by Yoti so that users do not have to share personal details every time they access a third-party service.

[85] Instagram, TikTok and YouTube user data left unsecured in data breach, Verdict, August 2020.

Digital identities can provide a high level of assurance to services seeking to establish a user's age. They have the potential to minimise the sharing of personal data and give users greater control over individual attributes of their identity, but under current commercial arrangements they tend to reveal more than is necessary about a user to prove their age.

b) Business to Business (B2B) verification (ID/AV)

Many third party age assurance providers offer background identity or age checks. A user may be asked to submit proof of age to a service, such as a hard identifier, which is then given to a third party age assurance provider to be validated. The third party provider performs relevant checks and confirms if the user has passed or failed the age check.

This process is technically no different from other hard identifier methods (approach 2) but the fact that the age verification involves a second, or in some cases, several more businesses, may not be transparent to the user. For example, if a user submits their name and address, they may not know that the service has asked a third party provider to perform checks against one or more private or public databases. Similarly, if a user submits a passport scan or 'selfie' to a service, they may not know that their data is being analysed, shared or stored by a third party. In this scenario, it is more than likely that a child has given permission as part of agreeing to terms and conditions, privacy notices or other published terms, but is entirely unaware of the fact their data is being shared and checked.

OnlyFans is a subscription-based service that allows 'creators' to make money from content they upload. To verify their age, content creators are required to submit a copy of a hard identifier as well as a selfie in which the hard identifier can be seen.

OnlyFans uses third party age assurance providers such as Ondato, Aristotle, and Jumio to conduct age verification.[86] This information is provided in OnlyFans' 13-page privacy policy, but is not made clear when users are going through the age verification process. It is also not clear which one of these three services is used to verify users or on what basis they are chosen, for example, it's not known if age assurance providers are chosen based on jurisdiction, a case-by-case basis, or at random.

Ondato, Aristotle, and Jumio use hard identifiers and biometric facial data to verify a user's age. Biometric data remains with the third party age assurance provider, and does not get stored on OnlyFans servers. The privacy policies of these third party age assurance providers are not made available to the user

[86] Identity Verification, OnlyFans Privacy Policy, December 2020.

unless they visit each provider's website and read their individual published terms. It is unlikely that the user knows the terms under which their biometric facial data is stored. For example, in the case of Jumio, a user's biometric data may be stored for up to 3 years after a user stops using their OnlyFans account or when they close their account, whichever is earlier.[87]

Summary:

- Very often the user does not know a third party is involved in the assurance process.
- If a child is not aware that their data is being sent to a third party age assurance provider, then it is arguable that they did not give informed consent for data processing.
- Using a third party age assurance provider introduces another company or companies into the value chain, resulting in the increased sharing of personal data between services.
- There is little transparency about how a user's information is shared and verified, or why it is stored, creating a concern it may be used for purposes other than age assurance.
- The information gathered about an individual is commercially valuable, increasing the risk that it will be kept or used for purposes other than identifying the age of users.[88]

Age assurance conducted at the level of business-to-business can minimise the level of engagement needed from the user to prove their age, but the process lacks transparency and oversight, which can make users vulnerable to privacy violations. Without agreed standards for data minimisation, this approach can lead to excessive data sharing.

c) Age tokens (AV/AE)

An age token contains only information relating to the specific age or age range of a user. This allows the service to establish if a user meets their age requirements without collecting other personal information. In many cases, an age token may not give a user's actual age and only provide confirmation that a user has passed or failed the

[87] Information for Illinois residents, Jumio's Privacy Policy, date accessed 11 October 2021.

[88] Under the General Data Protection Regulation (GDPR), purpose limitation is a requirement that personal data be collected for specified, explicit, and legitimate purposes, and not be processed further in a manner incompatible with those purposes (Article 5(1)(b), GDPR).

service's required age check, for example, that they are over 16. It is possible for an age token to be generated or extracted from a digital ID.

The level of assurance a token provides will depend on the initial method used by the attribute provider generating the age token. The UK digital identity trust and attributes framework[89] sets out how attribute providers should create a 'score' and share attributes. The BSI standard PAS 1296:2018[90] also introduces the concept of 'age check exchanges', which gives accreditation to third party age verification providers that meet agreed standards for sharing age tokens. The government has rightly identified age tokens as a productive area of innovation for age assurance.

An interesting consideration is that if this technology was fully trusted and widely available, it would be possible for institutions such as schools or GP surgeries to offer an age token that establishes the age or age range of a child as a single attribute. This would broaden the number of places from which a service could verify a child's age and reduce the need for centralised data sets.

Summary:

- Tokenised age checking relies on the attribute provider conducting an initial stage of verification, so the level of assurance will depend on the data sources used by the attribute provider. For example, age tokens that are created using self-declared age do not offer a high level of assurance.
- The technology to create age tokens is not readily available or taken up by many of the trusted institutions that hold age information about children. For example, GP surgeries, hospitals and schools do not currently offer this form of tokenised age checking.
- Since data collection is a commercial priority for many tech companies, most do not restrict their data collection to a single attribute. The introduction of common standards and a regulatory oversight regime would drive the market for age tokens.
- The government's troubles with its own digital identity assurance scheme have made it favour commercial third parties, which has stunted the potential of trusted public institutions to provide information on a distributed and non-commercial basis.

Age tokens minimise the amount of data that is shared with services and could be used more widely if the technology was readily available to a greater number of trusted institutions.

[89] UK digital identity and attributes trust framework, Department for Digital, Culture Media & Sport, 11 February 2021

[90] PAS 1296, Online Age Checking. Provision and use of online age check services. Code of Practice, British Standards Institution and EURIM Digital Policy Alliance, March 2018.

8. Account holder confirmation

A child's age or age range can be confirmed by an adult, often a parent or carer. Many forms of identification are only available to adults, such as a credit card or proof of eligibility to vote. This mean that in many scenarios, it is easier for an adult to prove their age than it is for a child. Account holder confirmation leverages the knowledge that a service is likely to have about an adult user and gives the adult responsibility for confirming the age of the child.

In this approach, an adult account holder is either asked to confirm the age of the child user or they may be asked to set up a special account for the child, as is the case with streaming services such as Netflix. In both scenarios, the adult takes responsibility for establishing the age of the child.

Once the account holder is confirmed, the service will then ask them to provide confirmation of the child's age. This can be through self-declaration, where the adult types in the child's age, age range or ticks a box, or by providing a hard identifier. As with other age assurance methods, the level of assurance the service has in the age of a child is determined by the integrity of the data sources. In this case, a service will have a higher degree of confidence that they have been provided with a child's true age if they have first verified the age of the assuring adult with a hard identifier, rather than through self-declaration.

The data processing activities in this approach are not always transparent, and it is possible that the adult's details are then permanently linked to the child's to build up the data picture the service has of both users.

This approach can result in the creation of a 'child account' rather than simply establishing age. Many 'child accounts' are entirely focused on content and do not give sufficient consideration to conduct, contact and in particular, contract risks. The provision of a child account does not in itself prove that a child's rights and needs are being protected and fulfilled.

GoHenry, a digital banking service aimed at children, requires parent/guardian verification to authenticate a child's account. A 'Know Your Customer' (KYC) check is first carried out to match an adult's details against a number of public databases or hard identifier.[91] After being verified as an adult, a parent/guardian is able to set up a child's account with the service and confirm the child's age.

[91] What identification and information will I need to open a GoHenry account? GoHenry, April 2019.

Netflix, a video-streaming subscription service, allows child profiles to be set up under an account belonging to a user above the age of 18. An adult user, by providing credit or debit card details, can set up profiles for one or more children and set specific age-restrictions for each child's account which can only be changed using a PIN. Parental controls also allow parents or carers to switch autoplay off on a child's profile.[92]

Summary:

- Confirmation by a person the service 'knows' to be an adult is useful for parents and children sharing accounts, such as streaming services, or who wish to have tailored accounts, particularly for younger children.
- The linking of accounts raises concerns about additional profiling including a company's ability to link a child's network to an adult's network.
- 'Child accounts' should be designed to mitigate all risks to children (against the 4 Cs risk framework) rather than simply offering content controls or screen time limits.
- This approach may exclude some adults (and by extension, children) who do not have access to hard identifiers and/or the skills to navigate digital technology.[93]
- Lack of transparent standards of data collection, processing and storage may make some adults reluctant to identify themselves.
- Older children may need to access services without adult involvement, for example, doing homework when their parent or carer is working, or accessing sexual health services.
- Like many approaches, the lack of common standards and regulation makes it possible for companies to prioritise commercial considerations over the need to establish age.

Account holder confirmation may be appropriate for younger children and for some services, but raises issues concerning a child's right to privacy, including from their parents, and may exclude some children who face obstacles to obtaining confirmation from their parent or carer. Children's accounts should provide for age-appropriate experiences, not only with respect to content filtering but in all aspects of design.

[92] How to turn autoplay on or off, Netflix Help Center.

[93] Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes, Mariya Stoilova, Sonia Livingstone and Rana Khazbak, February 2021.

9. Device/operating system controls

Many devices, operating systems[94] and even broadband setups offer controls designed to deliver more age appropriate experiences for children. They are generally limited to controls that restrict the websites and apps a child can access, filter content or set time-outs.

This approach can also be applied at a system or device level to create a 'children's phone' or put an existing phone into 'child mode', making features, services and content age appropriate by default. This has the advantage of requiring little engagement from the child but may have a detrimental effect on a child's right to participation and would require transparency about what basis 'age appropriate' had been determined upon.

There is some overlap between device/system level controls and account holder confirmation as described above.

Google Family Link allows parents and carers to set controls on a child's Android device. The parent/carer will first confirm they are an adult through their Google account via self-declaration. A unique code is then generated to link a parent's Google account with their child's account. This link allows a parent to monitor and set controls, for example, to view location data from a child's device, accept or deny requests to download apps on the Google Play Store or set time limits for device usage.[95]

Circle is an in-home device that allows parents and carers to set a variety of controls on their child's device(s). These include pre-loaded filters for popular apps such as Amazon, Disney, TikTok and YouTube that limit the type of search results that are displayed. The parent/carer can also manage and set restrictions on screen time, track their child's device location and give device-related "rewards" in the form of bonus screen-time. Circle also provides a full history of a child's website viewing and app usage (provided the services are not encrypted) and the option to pause access to WiFi.[96]

[94] An operating system refers to the software that allows smartphones, tablets, computers and other devices to run applications and programs.

[95] Family Link, Google, date accessed March 26 2021.

[96] Frequently Asked Questions, Circle, date accessed March 26 2021.

Summary:

- Device or system level controls put product makers and those who control systems, primarily Apple and Google, in an extraordinarily powerful position to decide what constitutes an age appropriate experience.
- Without agreed standards, it is likely this approach will focus on filtering adult material and content moderation or take down, and less on the design features or commercial drivers that put children at risk.
- Device-level controls do not always account for mixed ages within the same family group. Those designed primarily to shape the experiences of younger children can result in access being overly and unfairly restricted for older children.[97]
- Controls operated by parents may not be appropriate for older children, or may concentrate on adult anxieties such as screen time, while leaving many children vulnerable to less obvious risks.
- 'Child' settings, if left in the hands of commercial providers, may inadvertently create a visible market of children who can then be targeted for commercial purposes.
- A walled garden approach is not popular with young people who want to roam freely. They want a less aggressive commercial and social environment rather than a designated 'child' experience.[98]
- Without common standards and greater understanding of the risks children face, device/operating system controls have the potential to bring false security to parents while leaving children in an aggressively commercial world that continues to overexpose and target them.

Device/operating system controls may be a good way of establishing a 'base-line' of age-appropriate settings from the outset. However, putting the full experience of childhood in the hands of private companies is unlikely to deliver a rights-respecting digital environment for children or cater for their evolving capacities.

10. Flagging

Flagging is generally used to identify or 'flag' that something may be wrong. In the context of age assurance, it allows users to 'flag' other users they believe do not meet a service's age requirements. For example, a user of a dating app or subscription-based

[97] Children have a right to privacy even from their parents according to Article 16 of the UNCRC. This is particularly important as children often use digital services for matters that may require privacy, for example seeking health or relationship advice.

[98] "[children] were concerned that decision makers' values translate into restrictive government legislation, such as bans and other forms of censorship." Our rights in the digital world: A report on the children's consultations to inform UNCRC General Comment 25, p.23, Amanda Third and Lily Moody, 2021.

service selling adult content may be able to spot a user under the age of 18.[99] Once a user is flagged to the service, their account can be blocked or a moderator may ask for proof of age.

Services report that many users who are asked for additional proof of age do not give it (this is not restricted to flagging but is true of all assurance methods). This is widely considered to be because they are children.

> TikTok has implemented an in-app button to enable users to “quickly and easily” report users who they suspect may be under the age of 13, which is TikTok’s stated minimum age of use.[100] If a user is flagged as being under the age of 13, their account will be reviewed by a TikTok moderator who may remove the user’s account.

Summary:

- Flagging as an age assurance method places the onus on the users of a service to identify and report underage users.
- If an underage account is flagged, it means a child has already accessed a service for which they are underage and are likely to have already been targeted or subject to data collections practices that are prohibited against children, or engaged in risky or adult behaviour long before their account is flagged to a moderator.
- While it may be possible to see that a user does not meet a service’s age requirements on services that offer visual functions such as live-streaming or video-chat, it may be more difficult to identify and flag underage users on services that are anonymous or text based.

Flagging may provide an additional layer of assurance after initial age checks, but it places responsibility on users rather than services to identify children, and is only possible once a child is already using a service.

[99] #Nudes4Sale Uncovers The Shocking Truth About Selling Nudes Online, Refinery29, April 2020.

[100] TikTok will recheck the age of every user in Italy after DPA order, Tech Crunch, February 2021.

Combining approaches

This report deliberately focuses on *approaches* to age assurance rather than specific products, data sources or technical solutions. In practice, many services use a combination of methods for age assurance or different approaches for different parts of the same service. For example, self-declaration may provide enough assurance for a child to leave a review on an e-commerce site, but proof of age would be needed if they then tried to buy a restricted product. Similarly, confirmation from an account holder may be adequate for streaming services such as Disney+ or BBC iPlayer, but more robust verification is required for YouTube which contains vast amounts of user-generated content, including misinformation, extreme, violent and adult content.

Below are some common approaches that combine age assurance solutions:

- **Self-declaration and inference:** A user declares their age when registering for a service, then the service provider profiles the user to check that the given age is consistent with the user's activity. For example, if a child states that they are 16 then likes or comments on videos of cartoon characters or games which typically appeal to much younger users, service moderators may be alerted and additional age checks carried out.
- **Account holder confirmation and facial analysis:** A parent/carer proves they are an adult and gives their child's age. The child is asked to complete a facial analysis scan to confirm if they meet the age or age range provided by their parent/carer.
- **Facial analysis and hard identifier:** A user is asked to upload a 'selfie', which is used to estimate their age or age range. A hard identifier may be requested to verify the ages of users on the threshold of an age restriction (for example, at 13 or 18).
- **Cross account authentication and third party age assurance provider:** A user registers for a service using an existing account and a third party is employed by the service to check the user against an existing database.

An emerging market

Age assurance is a fast-changing area with a growing market.[101] Pressure for better services and treatment for children will lead to greater investment and further innovation. It is likely that new products offering particular features or protections will fall into one or more of the above categories, many of which offer potentially good solutions for different circumstances. What 'good' looks like will be determined as much by developing standards and accountability as by technical innovation.

One technology to consider in the development of age assurance solutions is blockchain. Already we are seeing blockchain disrupt the banking and finance sectors, and increasingly be used in manufacturing, healthcare and the digital identity market.[102] Data stored in a blockchain is recorded, stored, and distributed across decentralised servers, meaning it is not managed by any single central authority. When information is generated, it can be written and encoded into the blockchain, then accessed with a private key, providing a high level of security and privacy. A service seeking to assure a child's age would be able to obtain an age token directly from the securely stored data. This means that at any given point, neither a third party nor a service will have direct access to a child's data. The use of blockchain technology for age assurance would remove the need for children to create accounts, exchange passwords or store information with a third party at any stage of the age assurance process. However, information is stored permanently and difficult to modify in a blockchain, so if a mistake is made in the age assurance process (intentional or otherwise), it will be difficult to correct. GDPR also creates certain caveats for the use of blockchain for personal data, so to comply with the right to erasure, personal age data must be stored in an "off-chain" data store, where only its evidence (the URL[103] and cryptographic hash) is indexed in the chain.[104] This will satisfy the requirement under GDPR to be able to delete individual data from the external database.

Curiously, the biggest tech companies in the world have been largely silent on the subject of age assurance. Some have modified or enhanced their age assurance systems, in particular through the development of AI and inference models , or in the case of YouTube, by introducing a requirement to provide hard identifiers to view adult content.[105] However, there is legitimate concern that once age assurance is established in law, these companies will move fast to put in place age assurance solutions that tie children to their dominant services, making them the default age assurers and squeezing out more ethical or accountable providers.

[101] In 2018-19, the UK safety tech market alone was valued at an estimated £503 million (See: Safer technology, safer users: The UK as a world-leader in Safety Tech)

[102] ID 2020: Digital Identity with Blockchain and Biometrics, Accenture, 2020.

[103] What does GDPR mean for blockchain technologies? IBM, February 2019.

[104] Blockchain and GDPR, IBM, 2018.

[105] Using technology to more consistently apply age restrictions, YouTube Official Blog, September 2020.

Ultimately, the way the age assurance market develops will be as much shaped by the appetite of governments for regulation as it will by innovation. To work towards a shared goal of a digital world that anticipates and responds to the different ages and capacities of children, we need a mixed economy of age assurance methods that are privacy-preserving, transparent, accountable and suitable for the context in which they are used. These will have to be developed to agreed standards that can be upheld by services and enforced by a regulator.

In the following section, we set out the common standards to which age assurance solutions should adhere.

Common standards for age assurance

Age assurance can and should be conceived as a nuanced, proportionate tool to support children's engagement with digital products and services. It should not be seen as an end in itself, but the first step in anticipating children's presence in the digital world. While the approaches will vary, there are a set of common standards which should be consistent and mandated.

The following standards are interdependent and interconnected. To be effective, providers must adhere to all and not only those that are most convenient.

- **Age assurance must be privacy preserving**

All age assurance tools must be operated in compliance with the principles set out in GDPR.[106] This means that age assurance solutions must be predicated on the principles of data minimisation and purpose limitation, meaning the minimum amount of information necessary to establish the age of a user is taken with the minimum amount of intrusion and must not be stored or used for any purpose.[107] Specifically, companies must not use age assurance as cover for their aggressive data collection practices or as an excuse to avoid implementing children's entitlements.[108] Where children's data is captured for the purposes of age assurance it must be stored, managed and deleted in a privacy preserving way.

> Many third party verification providers supply services with a user's age range, without sharing any personally identifiable information. This minimises the amount of data a service collects about the child and adheres to the data minimisation standard set out in the Age Appropriate Design Code.[109]

- **Age assurance should be proportionate to risk and purpose**

Where possible, services and products should be designed to be suitable for all users, including children, and therefore require no age assurance at all. If a service or product

[106] Organisations must ensure that their use of age assurance complies with principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy. storage limitation, integrity and confidentiality (security), as set out in the GDPR principles. (See: ICO Guide to the General Data Protection Regulation)

[107] Article 5 of the GDPR requires that the collection of personal data be "adequate, relevant and limited to what is necessary in relation to the purposes for which [it is] processed ('data minimisation')". Article 25 states that data minimisation is to be applied by default "to each specific purpose of the processing." Recital 38 states that "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."

[108] Standard 3: Age appropriate application, ICO, September 2020.

[109] Age appropriate design: a code of practice for online services, ICO, 2020.

contains individual features that present risk, or if the service wants to offer children a tailored experience, it can take a 'layered' approach, using different levels of age assurance for different features.[110] Where something is expressly forbidden, for example the purchasing of age-restricted goods or services, a robust verification method must be used.

If establishing age range rather than the exact age of a child, a service or product must be made suitable for the youngest possible user within the range, rather than the median age. If hard identifiers are used to verify age on high-risk services, there must be sufficient authentication that the hard identifier can be matched to the child being verified.

The effectiveness of any age assurance method must be measured against its potential impact. For example, if age assurance is used for the purposes of restricting a child's access to extreme violent or sexual content or potential contact with anonymous adult users, it must be designed and operated to the highest standards of assurance, accuracy and efficacy.

- **Age assurance should be easy for the child to use**

It is critical for the successful adoption and acceptance of age assurance that it is convenient and easy to use and does not put undue burden on users. Making it easy does not mean configuring age assurance in ways that encourage children to 'game' access, for example 'tick box' age declaration or cross account authentication that may not provide the level of assurance needed.

Age assurance that is easy to use does not mean it should be invisible. Children's development depends on understanding boundaries, societal norms and at times, transgressing both. Confusing and difficult-to-use privacy and safety settings must be addressed by regulation and appropriate levels of friction must be normalised in situations where it is required.[111]

- **Age assurance must enhance children's experiences, not merely restrict them**

Age assurance should embody a child's rights to participation, so that as well as being protected, children will be assured their freedom from discrimination, access to information, freedom of expression and association, access to health and education services as well as those parts of the digital world that allow them leisure, play and a cultural life. Age assurance should not be used to freeze out children from areas of the

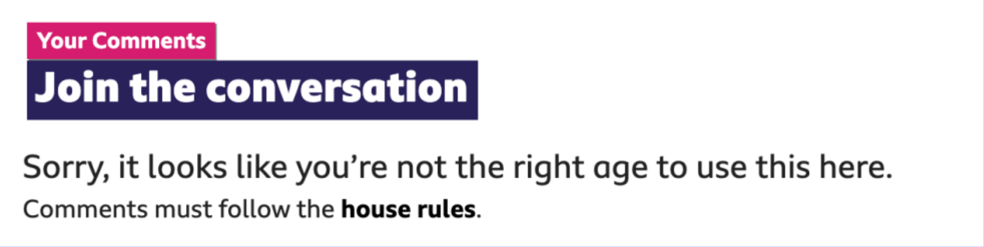
[110] For example, the 'Lego Life' app requires parental consent to unlock certain features and functions.

[111] Research conducted by Privolta shows it takes a user 17 clicks to opt out of Google's data collection in the UK, and only one click to consent to all data being collected. See more from: Default settings for privacy – we need to talk, CNET, December 2019.

digital world which they have a right to enjoy, as a way of companies avoiding their responsibilities to make a service age appropriate.

Identifying children can also provide access to opportunities which they may not have in offline environments, for example, the opportunity to take part in civic action,[112] to express themselves and be heard or engage in matters that affect them, such as political priorities or the allocation of local resources for play and cultural activities.

CBBC's Newsround website has 'house rules' that state only users under the age of 15 can post comments relating to featured content. Newsround's age-restrictions help younger viewers to have their voices heard and reduce the risk of inappropriate material being posted by older users.



Your Comments

Join the conversation

Sorry, it looks like you're not the right age to use this here.

Comments must follow the **house rules**.

Figure 2: Screenshot from CBBC's Newsround comment section

- **Age assurance providers must offer a high level of security**

All age assurance providers and those in the value chain of assuring age must ensure their products are secure. The collection, processing, sharing and storing of children's data for the purposes of age assurance must have sufficient protections and security built-in to agreed standards that are set out in regulation.

- **Age assurance providers must offer routes to challenge and redress**

When a service uses age assurance technology, it must allow users to challenge the outcome of the decision, including when the process is automated. This is to comply with the right to rectification (Article 16, GDPR) and, in the case of automated decision-making, the right to human review (Article 22, GDPR).[113] Age estimation systems in particular have a degree of error and should have clear and easy routes to challenge, subject to minimum response times. Services should always offer a way for users to challenge the outcome of an age assurance decision, for example if a user is denied access to a service following a failed age check or if a parent wishes to challenge the acceptance of an underage child. Additionally, a child should never be asked to prove

[112] What TikTok teens and K-pop stans teach us about child rights online, 5Rights Foundation, June 2020

[113] Article 16 and Article 22, GDPR.

their age to have content taken down if they were not asked to do so to post or share content in the first place.[114]

- **Age assurance must be accessible and inclusive**

Each age assurance solution may not be suitable for all children. Reflecting the diversity of children's needs and experiences in the digital world should extend to offering flexible and varied types of age assurance. Services must account for different languages, abilities, races, developmental capacities, socioeconomic statuses, access to parents/carers — among the other characteristics discussed in this report — to ensure all children are able to engage with age assurance mechanisms safely and effectively.

DCMS research on age assurance and exclusion risks

In advance of the government's Online Safety Bill, the Department for Digital, Culture, Media and Sport (DCMS) will deliver a research package[115] to consider the possible exclusion risks posed by age assurance solutions. Information from the tender notice[116] indicates that DCMS are aware that age assurance solutions may, in varying degrees, contribute to exclusion risks to vulnerable children. Understanding and mitigating these risks will help providers develop and offer more accessible and inclusive solutions.

- **Age assurance must be transparent and accountable**

All service and product providers, companies, organisations, government bodies or third party age verification providers must be transparent about the methods they use to assure the age of users. This must include clarity on the data collected, how that data will be processed, and how it measures against regulatory requirements, guidance and other relevant treaties or laws.

Companies must be accountable for implementing appropriate age restrictions on their products and services in compliance with regulation, and for operating age assurance systems in a way that incorporates these standards.

[114] Childline, in partnership with the Internet Watch Foundation, run a service that helps children to report naked or sexual photos of themselves posted online. To use this service, children must first confirm their identity using the digital identity provider Yoti, for which they need a UK passport, driver's licence or citizen card or young person's ID card.

[115] Online Harms White Paper: Full response to the consultation, Department for Digital, Culture, Media & Sport and Home Office, 15 December 2020

[116] GB-LONDON: Exclusion risks posed by age assurance technologies to children | A Tender Notice by Department for Digital, Culture, Media and Sport, 1 December 2020

- **Age assurance should anticipate that children don't always tell the truth**

It must be acknowledged that a number of children, for reasons of transgression or aspiration, pretend to be older online. While much is made of children lying about their age, the responsibilities of companies to provide clear boundaries have been woefully inadequate. A necessary part of child development is the need to transgress boundaries, and creating proportionate friction is part of helping them understand the nature of the spaces and services they engage with. What is not appropriate is for digital services to treat children as adult by default. If children are offered and understand the benefits that come from age assurance, it would create a positive incentive to give their correct age.

While profiling or data processing for the purposes of age assurance should be limited, if the data that services hold indicate they are dealing with a child, that is, they have 'constructive knowledge', the service has a responsibility to treat that user as a child.

- **Age assurance must be subject to agreed standards**

The government should introduce legislation that requires age assurance systems to meet a set of minimum standards in advance of the upcoming Online Safety Bill.[117]

In the meantime, providers should adhere to the standards set out in the digital identity trusts and attributes framework[118] and seek accreditation through recognised certification agencies. Services must also comply with existing age assurance requirements set out in the Age Appropriate Design Code and video-sharing platform regulation, and to the standards set out in this report.

- **Age assurance must be rights-respecting**

Children have existing rights codified in the United Nations Convention on the Rights of the Child.[119] These include the right to privacy, protection from violence and all other forms of exploitation, access to reliable information from a variety of sources, the right to freely express their views and to think and believe what they choose. The application of these rights in the digital world is set out in general comment No. 25 (2021) on children's rights in relation to the digital environment.[120]

[117] In May 2021, Baroness Kidron introduced a Private Members Bill that requires age assurance systems for online or digital services or products to must meet certain minimum standards; and for connected purposes.

[118] UK Digital Identity and Attributes Trust Framework, February 2011

[119] UN Convention on the Rights of the Child, UN Office of the High Commissioner, November 1989.

[120] General Comment No. 25 (2021) on children's rights in relation to the digital environment, OHCHR, March 2021.

> **"It's absolutely essential that young people understand their rights in the digital world and how to use them. Everyone has the right to know what information is being held about them, to be secure and safe, and to make informed decisions. If something isn't acceptable offline, then it shouldn't be OK online – that's what we're working to achieve."**[121]
>
> Young person, UK

These rights are underpinned by the overarching principle that a child's best interests are given primary consideration in all actions concerning them.[122] This principle has practical application when used in relation to technological innovation, development and distribution. A child's 'best interests' is a concept widely established in legal judgements. It is unlikely that the commercial interests of a company will trump the best interests of a child. Age assurance approaches must embody the rights of children and be deployed in their best interests.

[121] 5Rights Young Scot Youth Leadership Group Launch, 5Rights Foundation, 2018.

[122] Article 3, UNCRC states "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."

Applying these standards

We wanted to imagine how each age assurance approach would look if the common standards were applied. The table below shows the qualities each age assurance method would have if we applied the standards. Green shows where each approach would meet a standard, amber is used where the approach may or may not meet a standard depending on how it is applied, and red is used where the approach is unlikely to meet a standard. Not all approaches can be used in all circumstances, as demonstrated by those approaches that score red against some standards. The table is for illustrative purposes only and does not refer to individual products.

If each of the approaches met the **highest bar of these standards and were used proportionately**, the chart *could* in the future look like this:

		Privacy preserving	Proportionate	Easy to use	Experience-enhancing	Secure	Offers redress	Accessible and inclusive	Transparent/accountable	Levels of friction
1. Self-declaration		🟢	🟢	🟢	🟢	🟢	🟠	🟢	🟢	🟠
2. Hard identifiers		🟢	🟢	🔴	🟢	🟢	🟢	🔴	🟢	🟢
3. Biometric estimation		🟢	🟢	🟢	🟢	🟢	🟢	🟠	🟢	🟢
4. Profiling (AI)		🔴	🟠	🟢	🟠	🟠	🟠	🟢	🔴	🔴
5. Capacity testing		🟢	🟢	🟢	🟢	🟢	🟢	🟠	🟢	🟢
6. Cross-account authentication		🟠	🟢	🟢	🟢	🟢	🟢	🟢	🟠	🟢
7. Third party age assurance provider	a. Digital identity	🟢	🟢	🟠	🟢	🟢	🟢	🟠	🟢	🟢
	b. B2B	🟠	🟢	🟢	🟢	🟠	🟠	🟠	🟠	🟢
	c. Age tokens	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
8. Account holder confirmation		🟠	🟢	🟠	🟠	🟢	🔴	🟠	🟢	🟢
9. Device/operating system controls		🟠	🟠	🟢	🟠	🟢	🔴	🟠	🟢	🟢
10. Flagging		🟠	🟠	🟢	🟠	🟢	🟢	🔴	🔴	🟠

Figure 3: Ten approaches to age assurance that meet the highest bar of common standards

There are many well-intentioned players in the age assurance space who are developing effective, privacy-preserving and rights-respecting tools for services to know the age of their users. But unfortunately, without the standards in place to benchmark or assess the efficacy of solutions, and without a coherent regulatory framework, the ecosystem of age assurance is little more than a sea of known unknowns in amber, many of which could also be red.

		Privacy preserving	Proportionate	Easy to use	Experience-enhancing	Secure	Offers redress	Accessible and inclusive	Transparent/accountable	Levels of friction
1. Self-declaration		🟡	🟡	🟢	🟡	🟡	🟡	🟢	🔴	🔴
2. Hard identifiers		🟡	🟡	🔴	🟡	🟡	🟡	🔴	🟡	🟢
3. Biometric estimation		🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡
4. Profiling (AI)		🔴	🟡	🟢	🟡	🟡	🔴	🟡	🔴	🔴
5. Capacity testing		🟡	🟡	🟢	🟡	🟢	🟡	🔴	🔴	🟡
6. Cross-account authentication		🟡	🟡	🟢	🟡	🟡	🟡	🟢	🔴	🟡
7. Third party age assurance provider	**a. Digital identity**	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢
	b. B2B	🟡	🟡	🟢	🟡	🟡	🟡	🟡	🟡	🟢
	c. Age tokens	🟢	🟡	🟢	🟢	🟢	🟡	🟡	🟡	🟡
8. Account holder confirmation		🔴	🟡	🟡	🟡	🟡	🔴	🟡	🟡	🟢
9. Device/operating system controls		🔴	🔴	🟢	🟡	🟡	🔴	🟡	🟡	🟡
10. Flagging		🟡	🟡	🟢	🟡	🟡	🟡	🔴	🔴	🟡

Figure 4: Ten approaches to age assurances as they are currently deployed, scored against common standards

Finally, any approach to age assurance must be underpinned by the two standards not included in these tables. They must be subject to common rules set out in regulation, and uphold, embed and protect children's rights.

Who is responsible?

It is widely understood that we are all responsible for good outcomes for children and childhood, but age assurance in the digital world has some primary players:

- Children
- Parents
- Business
- Government

The production of tools and governance strategies will support the development and use of rights-respecting age assurance approaches suitable for the myriad of circumstances and risks of the digital world. Unless and until government and business introduce the necessary standards and make the necessary investments, the other two primary players — children and parents — don't stand a chance.

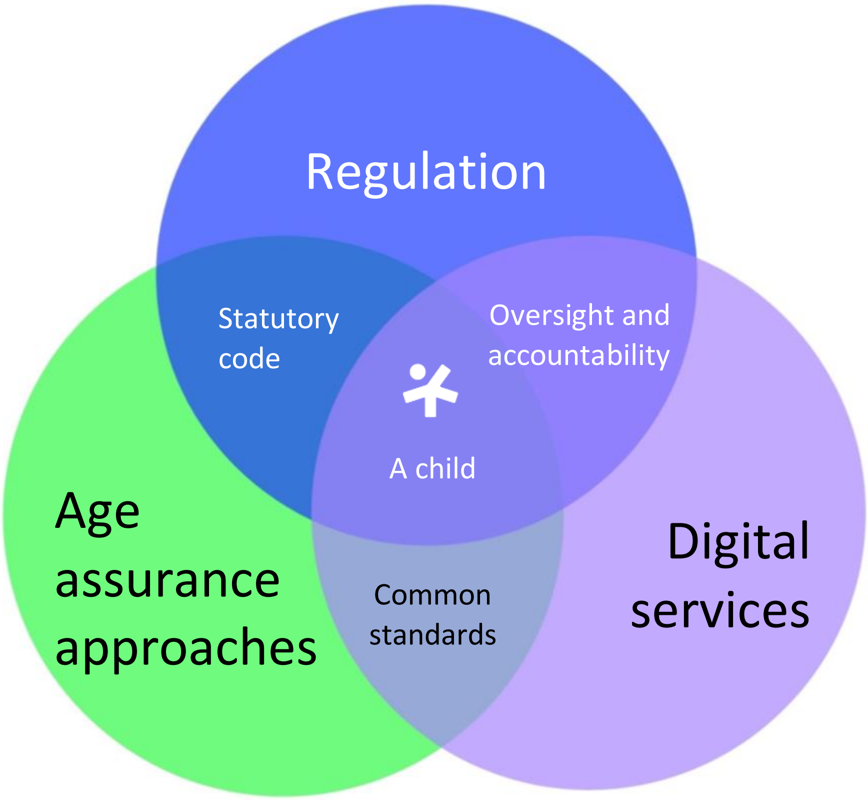


Figure 5: Matrix of responsibility for the development of rights-respecting age assurance solutions

Conclusion

We are at a tipping point where civil society, parents, children and regulators are all demanding a better deal for children online. In order to achieve this, children need to be recognised in the digital environment.

Age assurance is simply the suite of tools and approaches through which this can be made possible. These tools come in many forms, each with different benefits and weaknesses, but all are currently undermined by the commercial interests of services and a lack of common standards, regulatory accountability and oversight.

The government should introduce a statutory code of age assurance in anticipation of the Online Safety Act passing into law, to ensure that age assurance develops as a positive experience for children's participation, not a draconian act of exclusion that embeds the current inequities of the digital world.

The ultimate purpose of age assurance is to support the protection and flourishing of children and young people. It is not the destination but part of the journey to building the digital world that young people deserve.

Building the digital world that young people deserve

5RIGHTS FOUNDATION

Website: 5rightsfoundation.com
Twitter: @5RightsFound

Email: info@5rightsfoundation.com