Making age assurance work for everyone: inclusion considerations for age assurance and children

Authors: Zoe Hilton and Helen King

Contents

Executive Summary

This research is focused on understanding the inclusion considerations presented by age assurance technologies in relation to children and young people's access online. To understand the uptake of different age assurance methods within technology and social media companies, as well as the potential inclusion and exclusion considerations associated with them, this research conducted a wide range of interviews with companies, regulatory and standards bodies, policy makers and child safety groups. In addition, to fully explore the ways different methods might contribute to exclusion, children and young people from more excluded groups were interviewed. This included children in care, children with SEND (special educational needs and disabilities) and children educated outside mainstream school, as well as their parents and carers and the professionals who work with them. This has provided insight into how different age assurance methods would be likely to impact on these children and families.

Key Findings

The research has looked at four broad categories of age assurance methods and assessed the inclusion considerations presented by each category of approach. The analysis has been informed by interviews with children and young people, and their parents and carers. As well as representatives from technology companies, age assurance providers, regulators, policy officials, and child safety organisations.

Our analysis found that no single age assurance solution worked for all the user groups interviewed for this research. All of the measures presented a degree of exclusion risk. However, they also all presented benefits and opportunities for inclusion, depending on the circumstance of the user. This was due to the varied and complex backgrounds of the children, parents and carers that were interviewed. This highlighted the importance of providing users with a range of age assurance options to maximise inclusion. This research found that some online platforms were already exploring a 'layered' approach to age assurance, where they combined a number of different age assurance methods. Their motivation for this was to improve the accuracy of the age check. But it may also, based on the findings of this research, present the best way to maximise inclusion for children and young people.

Hard identifiers

- This approach is commonly referred to as age verification. The method relies on hard identifiers such as a passport, credit card or driving licence. As this information is only possessed by persons of a known minimum age, or, is linked to their identity it generally provides a high level of confidence in the age of a user. In general this approach was found to be the least inclusive of the four methods that were discussed with participants.
- The children and young people in the groups interviewed for this research generally did not have (in line with their age) suitable forms of ID or independent access to it - although a small number had a passport. There was often a complete lack of ID documents (or means to apply for them) for children in the care system where ID was felt to create a particularly acute barrier to access, and this was especially true for the subset of children in short-term care placements. For these children, our research

found that an age assurance method that relied on ID or another hard identifier would create a significant barrier to accessing online services, presenting an exclusion risk.
- In addition, the children and young people interviewed expressed concern about the security of their details if they were required to enter ID information into a site.

Verified Parental Consent

- Verified parental consent commonly requires an adult to verify their age to confirm the age of a child user and/ or approve access to a service for a child user. It also relies on a hard identifier, commonly a credit card. The research found a mixed response to this method, depending on the degree of engagement parents had with their children's online lives.
- For some SEND children this approach felt the most natural. Their parents already have a high degree of engagement with their safeguarding and these children may otherwise struggle to navigate an age assurance process independently.
- However, other children and young people interviewed for this research had more challenging relationships with their parents or had a desire to have privacy from them online.
- In addition, some of the carers and professionals interviewed felt that there was a risk that for children in care there was a lack of access to a consistent person with 'parental responsibility' to provide parental consent (and make appropriate judgements about consent).
- Several parents and carers interviewed expressed their reluctance to enter credit card details due to the widely shared experience of having children run up significant bills through in-game purchases. The experience of losing money through in-game purchases was common in the sample for this research.

Behavioural data using Artificial Intelligence:

- This method refers to the use of artificial intelligence (AI) to build a profile of a user's age based on their behaviour on a service, for example the accounts they have interacted with, what they have liked and content in posts or messages. It can also include analysis of a user's typing or literacy to estimate age. This category of method provides an estimation of age, as it is currently unlikely to provide a specific age to a high level of accuracy.
- Those interviewed for this research were generally receptive to and relatively positive about AI-based age assurance methods. These methods were generally seen to be the most inclusive for vulnerable children and young people. which could be used for age assurance purposes and there was generally no hostility to these methods.
- Some respondents believed that behavioural biometrics held promise because it would be relatively frictionless and inclusive, and felt the data to be less personal than other forms.
- A concern in relation to profiling was about whether children from the more excluded groups would 'read' as their true biological age within AI methods that assess age - particularly in methods that used content viewing and interests - or whether they would appear atypical for their age and face barriers to access as a result.

Biometric data and Artificial Intelligence

- This is an emerging type of age assurance method, which uses biometric data and AI to estimate a user's age.

- There was generally support from children, young people and parents for the use of age assurance methods that rely on biometric data. A small number of respondents instinctively disliked the idea of providing a facial scanning for age assessment, but most respondents we spoke to felt it could work.
- However, an important inclusion consideration for biometric methods is a user's race and ethnicity. The technology performs less well for darker skin-tones and those with an atypical facial structure. This is a challenge that is evident from research and was raised by industry participants.

Wider themes

In addition to the considerations identified above, wider themes emerged during the interviews, that were not explicitly on inclusion but have an impact on improvising inclusion in the use of age assurance technologies.

Support for age assurance processes

We found a marked difference in appetite for age assurance between companies and services implementing these approaches and the views of parents, carers, and professionals. Those working within companies described concerns around customer resistance and hostility, worry about user friction and exclusion risks, and concerns about offering a potentially reduced experience of their service. In contrast, the view from the parents, carers and professionals we interviewed was overwhelmingly positive and supportive of age assurance being implemented and enforced.

The parents and carers from these groups shared that they are often struggling on a day-to-day basis with keeping their children safe online. Many of the parents and carers interviewed for this research felt that legislative action to enforce minimum age requirements on online platforms could help to reduce the conflict in their households, reduce peer pressure and help to reinforce some of their own protective behaviours. Whilst they relayed some concerns about different age assurance methods, they were highly supportive of the aim of age assurance and understood its potential to support safeguarding. The views of children and young people themselves were more mixed, but they too seemed to understand and accept the principles of how age assurance methods worked and their role in online safety.

Data privacy and security

For many of those interviewed, it was less the specific methodology that mattered and more about the safeguards that were in place in terms of the security and privacy of the data. Many did not trust platforms with their personal data. For some respondents, this concern was based on perceptions of the methods. Once the proposed methodology for how their data would be used and treated was explained there tended to be far greater acceptance.

Circumvention vs. exclusion

During interviews with parents, carers and professionals there was also a view that many children would circumvent age assurance methods once the methodologies were understood. There was a sense that whilst many of these children and young people are less digitally capable or mature than their non-excluded peers, they may be highly motivated to gain access because the online environment is so important to them and one of the few places in their lives where they are included and accepted.

Digital exclusion risks for highly vulnerable children

For vulnerable children, age assurance fits into a broader set of inclusion considerations around how they access and use the internet. For children in care there are longstanding concerns about their more limited access to the online world due to a lack of digital access or support.[1] The children interviewed for this research shared that internet access was particularly important for them - an area of their life where they felt included and connected. Inclusion considerations when implementing age assurance methods are therefore more significant for these, already excluded, children.

[1] *Growing up Digital in Care*, Office of the Children's Commissioner, 2017

Introduction

This report explores the inclusion considerations for children presented by age assurance technologies. Age assurance is the term used to describe any method of assessing a user's age online, and includes age verification as an age assurance method that provides the highest confidence in the age of a user. The first part of this report covers the views on age assurance technologies and exclusion considerations from representatives from popular online platforms, as well as a wide range of policy makers and child safety experts. With popular platforms this research has sought to understand the age assurance methods they are exploring, and which they felt were likely to work for their platforms and services, as well as the challenges and complexities of implementing these. The interviews with child safety experts have sought to understand what they are hoping to see from the implementation of the age appropriate design code (AADC) and the future Online Safety Bill and, more broadly, their aspirations for the implementation of age assurance methods. Their experiences and perspectives of exclusion risks were gathered from both groups.

The first part of this report also sets the technology context by exploring some of the age assurance methods that are being progressed within companies. These broad categories of age assurance methods are also explored in interviews and engagements with children and young people, and their parents and carers in the second half of the report.

The second part of this report explores the impact on inclusion that different categories of age assurance methods would have for children who are excluded or from vulnerable groups - these include children in the care system, children who have been excluded from school and children with SEND (special educational needs and disabilities). The research also engaged with parents and carers of children within these groups, as well as professionals working with them. The report explores both the practical challenges of different age assurance methods, as well as the views and feelings of these groups in relation to the inclusion considerations of these methods.

This report aims to deliver a better understanding of the potential exclusion risks arising from age assurance methods, to increase awareness of these risks and to seek to avoid or reduce them wherever possible.

Part 1 age assurance from the perspective of companies, policy makers and child safety groups

1. Engaging with companies, policy makers and child safety groups

This research interviewed a range of industry stakeholders including service providers, social media, video sharing platforms and gaming companies. Age assurance providers were also interviewed to capture the status of emerging technologies. In addition to interviews with those within the technology industry, interviews were conducted with child safety leads from a range of children's charities and child online safety organisations. Policy officials in government, regulatory bodies, and those involved in standards and accreditation were also interviewed.

This section explores the extent to which different methods of age assurance are deployed across popular online platforms that are commonly used by children and young people, and how the use of these technologies is likely to change as a result of the evolving law and regulation in this area. The purpose of this is primarily to understand how age assurance methods, in use now, may change in future - to explore the extent to which they will change and the implications this has for users. By understanding the take up of different age assurance methods and by exploring how they might work, we can begin to understand what this could mean in relation to the exclusion risks facing children and young people. It should also mean that, where exclusion risks can be identified and explored, they can be better addressed, avoided, or reduced.

The first part summarises the current regulatory landscape that is driving the use of age assurance for child online safety. This formed the context for interviews with platforms, policy makers and child safety experts. The report then sets out the spectrum of age assurance methods, the legal and regulatory circumstances that underpin them, and the opinions and experiences that are shared by respondents, with analysis. The final section looks at the key challenges that were raised and some of the debates and issues around exclusion that are being worked through both within companies and more broadly.

Whilst service providers and platforms were helpful and engaged - and many of them willing to share in some detail their current thinking about age assurance - it should be recognised that for nearly all the companies interviewed, age assurance was a live, ongoing and 'evolving' conversation inside their organisations. For most companies there were a range of different options being considered and discussed. At this stage, none of the platforms interviewed were able to say with certainty the level of accuracy that they felt would be achievable from the different age assurance methods they were considering, developing, or planning[2]. However, some companies were able to share their thoughts and indicative trends around exclusionary pressures.

[2] Publication note: Since the time of writing, progress has been made across the sector and government to develop methods of understanding accuracy of age assurance solutions (see for example, 'Measurement of Age Assurance Technologies', ICO, 2022).

2. New laws and regulations in the age assurance space

New and emerging online safety regulation is expected to increase the use of age assurance solutions by in scope companies. Set out below are the three main regulatory frameworks that are expected to impact on the use of age assurance for child safety purposes in the UK. This regulatory landscape formed the context for interviews with platforms, policy makers and child safety experts.

The Age Appropriate Design Code

The AADC requires that platforms establish the age of their users to a level of certainty that depends on their own assessment of their platform's data risks. This enables them to appropriately protect children of different ages. This is ultimately so that they can ensure that the data risks experienced by users (and the protections available) are appropriate to different ages and developmental stages. This code came into force on 2 September 2020, with a 12-month transition period. Organisations had to conform by 2 September 2021. The code lists a range of methods that may be suitable for different platforms to establish the age of their users. There is a potential tension between the AADC's objectives to protect data and privacy rights and uphold data minimisation principles, and the data collection requirements of many age assurance methods is recognised within the information about the code. The ICO has been clear that the AADC does not prevent companies from collecting data for the purposes of age assurance.

The Video Sharing Platform regime (VSP regime)

There are currently a number of policy, legal and regulatory changes that have implications for the uptake of age assurance. Most recently we have seen the implementation of the European Union's AVMSD (Audiovisual Media Services Directive) which requires service providers to prevent children from accessing 18+ content. The video sharing platform regime is the UK's domestic implementation of the directive. This is expected to mean that many video sharing platforms put in place age verification technologies to support 18+ gateways[3,4]. Current processes that are being put in place on video sharing platforms include the removal of inappropriate content from sites altogether, or the implementation of blended approaches. For example, age inference from other viewing habits or browsing and, where there is uncertainty about the age of a user, age gating this content behind an age verification process that requires the user to provide an ID document[5]. Some of the companies we engaged with as part of this work suggested that there has been some useful learning for

[3] Ofcom – Regulating Video Sharing Platforms A guide to the new requirements on VSPs: 'VSP providers must take appropriate measures to protect children (under 18s) from content which might impair their physical, mental or moral development. VSP providers must also take appropriate measures to protect the general public from content inciting violence or hatred, and content constituting criminal offences relating to terrorism; child sexual exploitation and abuse; and racism and xenophobia. The measures VSP providers must consider are set out in legislation and are described in this document.'

[4] Publication note: Under the UK's Audiovisual Media Services Regulations 2020, video-sharing platform (VSP) providers are required to take 'appropriate measures' to protect users. Appropriate measures could include, but are not limited to, age assurance, parental controls, comprehensive terms and conditions.

[5] Publication note: Providers have a range of options for dealing with inappropriate content, including requesting more stringent forms of age verification.

them as a result, as they come to consider the broader application of age assurance methods in anticipation of achieving compliance with the AADC[6].

Forthcoming online safety legislation

The draft Online Safety Bill outlines the UK government's ambition to make the UK the safest place in the world to be online. The draft bill sets out a legal duty of care on online companies and gives them new responsibilities towards their users. Companies that are assessed as posing a risk to children must put in place appropriate measures to protect their child users. The new regulatory framework has been designed to be future-proofed against new and emerging harms and technologies, as well as people's changing use of online services. It is technology neutral and does not make reference to specific technical processes, including age assurance technologies[7].

3. The current landscape - how common are the different methods of age assurance?

This section sets out the current landscape of age assurance methods, including available methods and the legal and regulatory circumstances that are driving change in this area. This section uses the broad categories of age assurance methods that the Information Commissioner's Office (ICO) has referenced in relation to compliance with the AADC. It is helpful to look at this as the AADC is the first piece of regulation relating to age assurance that impacts across online services where the users may be children. The age assurance methods identified by the ICO are assessed below against their likelihood to be used by companies.

Self-declaration

This is where a user states their age, but does not provide any evidence to confirm it. It therefore provides a very low confidence level in the age of a user. This research found that most of the platforms interviewed are using self-declaration methods where their service is age restricted.

The 'self-declaration' sign-up process commonly requires users to enter a date of birth, and provided this shows them to be over the minimum age requirement, this date of birth is taken as the user's actual age. It is widely recognised (and supported by research) that children who are younger than the platforms' required age very commonly do not present truthfully at these gateways and tend to type in a fake date of birth to access the site with their peers and older friends.[8] Some platforms are taking steps to improve the 'gateway' process by making them 'neutral'. In this scenario, it is not stated or obvious what the services' minimum age requirement is, reducing the incentive for users to enter a false date of birth. Some platforms are also working to prevent a user from re-entering a different date of birth if they initially

[6] Publication note: The AADC came into force on 2 September 2020, with a 12 month transition period. Organisations were required to comply with the code by 2 September 2021.

[7] Publication note: Age assurance and age verification technologies are now referenced on the face of the Online Safety Bill, to make it clear that these are measures that the Government expects to be used for complying with the duties where it is proportionate to do so.

[8] E.g. the CHILDWISE 2019 Monitor survey of 2000 children.

provide an age that is below the minimum age requirements. It was generally acknowledged that children under the required age often lie to access the services. Some companies were exploring ways to incentivise honesty during self-declaration gateways. This included using 'neutral' age declaration screens (rather than nudging towards the selection of certain ages) or preventing users from immediately resubmitting a new age if they are denied access to a service when they first self-declare their age.

The use of self-declaration and 13 as a minimum age requirement by social media platforms and games platforms is based on US federal law, COPPA (Child Online Privacy Protection Act) principles. [9] [10] COPPA sets out obligations on organisations that collect and use data from children and where a company collects personal information from a child under the age of 13, COPPA demands that you seek parental consent. However, over the age of 13 children can effectively consent for themselves and it is compliant with COPPA principles to allow children to confirm themselves to be 13 or over at the sign-up stage without any further checks[11].

Hard identifiers (Age Verification)

Users can verify their age using solutions which link back to government issued ID or 'hard identifiers' such as a passport or driving licence, or documents that provide evidence of a minimum age such as a credit card. This is commonly referred to as age verification. The exclusion risks presented by this approach are acknowledged by the ICO in the AADC, which recommends avoiding this approach if possible: *'some children do not have access to formal identity documents and may have limited parental support, making it difficult for them to access age verified services at all, even if they are age appropriate.'*

This research found a significant number of our respondents, including from companies as well as those working in the child safety space, were concerned about the implications of requiring hard identifiers in relation to the possible exclusion risks. For the most part, companies providing services for older children were reluctant to use hard identifiers, although these appeared to sometimes be envisaged as potentially part of a blended solution as a final way to prove age if a person consistently appeared to be an outlier. There were some concerns raised about a shift towards the use of hard identifiers if companies' legal teams felt a more rigid approach to compliance would be necessary, depending - as one respondent described it - on '*whether companies took a conservative view of the rules.'* Concerns about hard identifiers were also raised in relation to parental consent mechanisms, and this is considered in more detail below.

Age verification is established in online gambling, where users need to verify that they are over 18 and is increasing in use for the sale of age restricted goods online. There are a range of identity and age verification solutions that support these sectors that appear to be relatively well established. These generally draw upon several public datasets, such as the electoral roll, credit history, mobile phone information, or passport or driving licence databases to corroborate the age information and, if necessary, the identity information asserted by an individual. This information is then used to provide a simple 18 plus or minus attribute - and the identification with these data sources is used to answer the question: is

[9] Federal Trade Commission, Complying with COPPA: Frequently Asked Questions.
[10] 5Rights Foundation, 5Rights Foundation leads joint UK letter to FTC on COPPA Rule Review
[11] GDPR also sets the age at which children can consent for themselves (as 13 in the UK) (link). The requirements of GDPR and AADC are discussed later in section 3.

the user over 18? Due to data challenges, age verification providers do not tend to offer services for the differentiation of age groups under 18, nor are they developing services for that purpose.

Account holder confirmation or Verified Parental Consent

This approach allows an existing account holder or verifiable adult to confirm a child user's age or give consent for them to access a service.

In interviews with companies, this approach was found to be very common and already highly popular with paid for experiences, such as many popular online games packages and subscription-based TV or video streaming services and is likely to be used to achieve compliance with the AADC. As companies and stakeholders themselves identified, there are a range of interrelated issues with this approach which have implications for inclusion, and potentially risk further excluding already more socially and economically excluded groups. The main consideration for inclusion is that this process relies on parenting and family context e.g. having a parent who can set up an account and who has practical means to prove their identity.

Some research participants raised concerns about the reliability of this approach. Many parents may provide an incorrect age for their child or children in order to provide them with access to the game or platform they want, regardless of its safety. This would result in the safety of the child's account being limited. This approach is largely the status quo for a significant amount of paid-for services, but obviously becomes more complex if it is used for services that were previously free to access: it is in these instances that children who might previously have been able to access a service might not be able to if their parent must sign in, set up an account and verify it. This method of relying on a verified parental account to prove a child's age or to give verified parental consent is considered in more detail in part two of this report, from the perspective of children and young people, and their parents and carers.

Learning from the implementation and strengthening of Verified Parental Consent mechanisms

Verified parental consent (VPC) presents a range of inclusion considerations, as detailed above. One company that we interviewed explained the impact of their recently strengthened process for the implementation of VPC for their signed in services.

They considered that, overall, the parental consent process was the right one in terms of the ability to safeguard children on their platform. However, they relayed that the introduction of the requirement for a parent to enter an ID or a credit card, had led to a significant drop off in users (somewhere in the range of 50-80%). They reflected that they had no information on why this was causing parents to drop off. It was unclear, for example, whether this was people not wanting to enter their details because it was too much effort, or whether this was a result of parents not having access to ID documents or credit cards. Nonetheless, they were concerned about the impact of the VPC process on access to their service and the impact on a child's legitimate access and enjoyment of the service.

The company recognised that age assurance requirements and processes would inevitably be challenging for some parents, highlighting that some groups of adults are less likely to have a passport or other forms of ID and that for some the process of VPC may feel relatively complex and long. They saw one of their hardest challenges as communicating the process and the reason for it to parents in a way that makes sense: "*it is a new paradigm for parents and they need more education to understand why they need to do this".*

Some of the most significant inclusion concerns raised by participants about the use of hard identifiers were related to companies that were seeking to strengthen their VPC process. Credit cards are commonly used to support VPC; however, if a parent does not have access to one, their child is excluded. As one respondent stated "*if the kid has a parent happy to consent for them to use this game but doesn't have a credit card… that kid will be excluded".* A stronger VPC mechanism may be something that companies choose to do to create a safer environment, but it needs to be considered how to support parents who face barriers to these processes.

User's concerns over data and cyber security were also raised by industry respondents. It was felt that more was needed to be done to build trust and confidence in the processes and technologies so that people are prepared to navigate them. One respondent said "*If you can somehow reach parents with the message that these are safe and formal platforms then it might start to address some of the disincentives in terms of loss of audience that come about".*

Behavioural data and Artificial Intelligence

An approach that uses behavioural data supported by AI is where a service or platform estimates a user's age by using artificial intelligence to analyse the way in which the user

interacts with their service. This age inference approach is sometimes referred to as profiling. This research found that this method was seen by a number of the large platforms that were interviewed as an important component of their future age assurance strategy. Some companies are already using the method, which suits their service as they already offer users content and services based on activities, searches, and preferences. It was seen by several research participants as the most realistic way of achieving compliance with the AADC and the future Online Safety Bill, and for addressing the challenges presented by age assurance. Some level of demographic inference already takes place across many platforms in terms of personalising services and in terms of targeting advertising, which is discussed further below.

A consideration in relation to the accuracy of this method, which was raised by companies, is that there is often less data held on younger users, because they have generally been on these platforms for less time. This in turn could mean a reduced level of accuracy in estimating their age. There is similarly a challenge in estimating ages for under 13s, where there may be difficulty in developing an accurate data training set for the AI as these children should be removed from a service before a strong age profile is developed for them. Another consideration raised was how reviewing and assessing data for the purpose of age inference can contribute to inequalities (and exclusion) by impacting unfairly on those who are most likely to deviate from the norm. These points are considered in more detail in the next section of this report.

Profiling techniques are commonly used as part of current advertising practices to serve adverts appropriately. At present, profiling techniques are often used to target age restricted advertising towards individuals who are determined to be adults based on their habits and interests (and equally directed away from being targeted at children).[12] Social media platforms in particular are able to make an inference of age and other demographics that enables them to target specific user profiles. This is a relatively widely used age assurance technique aimed at age restricting content (here advertising content) away from children.[13] The recent CAP (Code of Non-broadcasting Advertising and Direct & Promotional Marketing)[14] guidance on online advertising explains some of the mechanisms of age assurance for the purposes of serving age restricted advertising. This shows that, to achieve confidence around age restricted advertising, the declared age of users is insufficient and must be combined with other data about the user to ensure an appropriate inference of age.

Further methodologies

In addition to the age assurance methods listed in the guidance for the AADC, there are other relevant approaches that have been discussed and mentioned by stakeholders which are important to consider. These include:

Biometric data and Artificial Intelligence

[12] Age-restricted marketing communications are those for products subject to legal restrictions on their sale or where there is another policy basis for limiting the protected age group's exposure. The CAP Code includes media placement restrictions protecting: children (under-16s) from being targeted with marketing communications for products such as food or soft drinks high in fat, salt or sugar (rule 15.18) and lotteries (rule 17.14); and children and young people (under-18s) from being targeted with marketing communications for products such as gambling (rule 16.3.13), alcohol, (rule 18.15) and electronic-cigarettes (rule 22.11).

[13] Age Restricted Ads online CAP guidance Advertising (non-broadcast)

[14] (**CAP Code**) is the rule book for non-broadcast advertisements, sales promotions and direct marketing communications. See ASA, Non-Broadcast Code

‘Biometrics’ are body measurements and calculations related to human characteristics. This may include data related to a person's face, iris, DNA, veins, fingerprints, voice or gait. There are emerging technologies which allow for the inference of age from such measurements and calculations as distinct from the verification of *identity* using biometric traits (which is a separate set of technologies).

In this space, facial scanning for age estimation is currently a more advanced biometric technology for the use of age estimation. However, there are also technologies in development using other forms of biometric data for age estimation, such as age estimation from behavioural traits which relies on the collection and analysis of behavioural indicators from users via the nature of how they interact with an application. Examples of behavioural traits include mouse click speed, swipe speed, swipe pattern, typing cadence and style, key pressure, and accelerometer data (from mobile devices). The efficacy and reliability of many of these technologies rely on the quality of the labelled data that is available to train the model.[15]

In relation to inclusion, biometric data has the potential to be inclusive in many respects as it does not rely on background factors such as access to ID data, or access to a capable and informed parent with ID data. However, biometric technologies present other inclusion considerations in relation to race and ethnicity differences, which is explored below. It was also raised that some children may have different capabilities around their physical movements, e.g. dyspraxia, and may have atypical facial features as a result of their disability.

One of the pieces of advanced work that has been developed in this area, and offered as a third-party solution is the age estimation tool developed by the age assurance provider Yoti, based on facial scanning technology. This technology makes an assessment of the age of a user, including those under 18, without relying on hard identifiers or officially provided data. In developing the training data for their solution they have sought to cover a broad demographic, considering age, gender, and skin tone in order to improve the accuracy of their product offer.

As mentioned above, the differing accuracy of this approach for different ethnic groups presents exclusion considerations. Some stakeholders interviewed for this research cautioned about issues with demographic bias and skin tone within these technologies. Yoti has acknowledged the reduced accuracy for those with darker skin tones[16,17]. This has the risk of creating ‘false positives’ which is where a particular group is disproportionately asked for physical ID when they are in fact the correct age for the goods or services they are seeking. To help reduce this risk, the company Yoti has employed additional measures such as ‘Challenge 25’ to help to mitigate bias, as statistically any bias increases with a narrower confidence limit. [18] It is hoped that for these technologies an increased size and diversity of

[15] Yunlian Sun, Man Zhang, Zhenan Sun, Tieniu Tan (2018) - Demographic Analysis from Biometric Data: Achievements, Challenges and New Frontiers.

[16] At the time of drafting, Yoti shared that the highest error rates are found for women with darker skin.

[17] Publication note: Since this research was conducted, progress has been made by Yoti and other age assurance providers to improve accuracy for users with different demographics, including those with darker skin tones.

[18] Challenge 25 is a retail strategy which means that if an individual is seeking to buy age restricted 18 + adult goods and services - they will be asked for ID if they look under 25. This encourages anyone who is over 18 but

the training data set will mean that the accuracy of solutions will improve. This is something that Yoti also states in their 2020 white paper.[19]

Capacity testing

Capacity testing was mentioned as a method for determining broad parameters of age by a number of research participants. This method would involve asking children and young people a set of questions that they could be expected to know by the time they reach a certain age, or for them to complete a puzzle that could be expected of someone of their stated age. This method clearly has a relatively wide margin of error and might be used to identify a broad age range rather than specific ages. It also has the potential to exclude children that have much lower ability than other children in their age group.

Third party age verification services

Third party providers could offer a range of different age assurance measures to be used by a service. These services, by providing an age 'attribute' where you request confirmation of a 'yes' or 'no' answer to whether a user is a certain age, can reduce the amount of personal data collected by a company.

From interviews with online services and platforms, this work did not find many examples of partnerships or collaborations between large platforms and independent third-party age verification services[20]. This may be because companies have yet to fully develop and finalise their approaches to this issue (and any internal talks with third party vendors would be commercially sensitive).

As identified above there are a range of stand-alone solution providers that offer a confirmation of age for those over 18, and who can confirm or deny an applicant's claim to be an adult. There are currently few open and available technological solutions for age estimation that confidently differentiates younger users below the age of 18, and it is unknown what proprietary technology is being developed or built internally within companies. In the UK there is no easily accessible dataset of children's data that can be used to create an online ID or age attribute for children. One of the few commercially available solutions of the under 18 space is the biometric solution offered by Yoti, discussed above.

4. Companies - complexities and challenges of age assurance

Concerns about maximising inclusion and the potential trade-off between this and successful age assurance was raised by almost all companies. There was a common desire for some explicit recognition of the challenges presented by introducing age assurance and safety measures alongside delivering an inclusive service. One respondent said "*sometimes when you do introduce a safety measure … it will impact on the number of kids willing to engage*

looks under 25 to ID (a card bearing the PASS hologram, a photographic driving licence or a passport) if they wish to buy alcohol.

[19] See Yoti, White Paper October 2020

[20] Publication note: Since this research was written, there has been progress in partnerships between large platforms and independent third-party age verification services, such as the collaboration between Yoti and Meta (see: Facebook, New Ways to Verify Age on Instagram).

with that experience… it's probably easier [for the child] *to go through to one of the less regulated experiences or to try to impersonate an adult…they may go to a different place where there are less restrictions".*

Several of the popular platforms interviewed relayed the challenges they were facing in trying to implement age assurance on their platforms in a way that works for all users. From interviews it appeared that there is a high level of engagement from industry and a desire to get this right, but also that there were many complexities that companies were having to consider and resolve in relation to exclusion.

Data set challenges

It is important to note that not all platforms that were interviewed as part of this research were advanced in their thinking and planning around age assurance. Some did not think that either the AADC or the future Online Safety Bill would require or lead to significant changes for their company or platform. Some felt that age assurance was aspirational – but ultimately part of the long-term evolution of regulatory and legal changes. Several industry respondents felt that the government's Verification of Children Online (VoCO) project had demonstrated the complexities with data and implementation and had highlighted that there were no easy answers to age assurance challenges for under 18s. It was also expressed by some companies that the challenges of age assurance varied in terms of the way different individual companies gathered and used data already. Specifically, companies that have less access to social data about their users - or for example companies that have live streaming data rather than uploaded data - may be at a disadvantage in relation to using some age assurance methods such as profiling using behavioural data.

Data minimisation

A range of companies interviewed raised the challenge of acquiring accurate and unbiased data to support age assurance solutions. They described the challenge of the ethics of building datasets around behaviour or interests of children in order to do age inference effectively. It was also highlighted that for some companies they have much less data on younger users, because they have been on the platform for less time and also because of data minimisation protections in place for them. One respondent explained that the more detailed the age demarcations need to be, the more data is required.

Companies commonly raised the issue of the complexities and inherent tension between data protection legislation, including the AADC, and data gathering for age assurance. While the AADC does make provision for the collection of data for the purposes of age assurance, provided the data is treated in compliance with the principles of the AADC and GDPR, many industry respondents felt there remained a tension. It was also raised that making age assurance solutions work globally could be complex in terms of compliance with different countries' privacy regimes.

AI and exclusion

Some industry respondents expressed reservations about the development and use of AI tools for age assurance in relation to the exclusion risks they felt they presented, and were therefore hesitant about supporting the use of AI supported technologies as the direction of travel for age assurance. This concern was particularly around the risk of bias. An example that was given was inferring age through the quality of a user's English, which could be affected by being a non-native English speaker, their education, developmental needs and

speech impediments. One respondent said "*I don't want to reward people who happen to speak like me or punish people who don't."* These complexities were felt to be important and needed to be carefully considered going forward. One respondent stated "*I want us to be very conscientious about how we are moving forward and what implicit biases are included".*

The considerations on inclusion raised by respondents touched on the volume of data needed in order to make granular age demarcations, and the complexity of acquiring that data. However, for many of the companies interviewed, solutions based on AI were felt to be the most workable approach, in terms of managing the complexities of effectively knowing and understanding a user's age. A number of the larger 13+ platforms were already using profiling methods to establish age to support child safety efforts. Despite the concerns raised above, for many companies AI solutions were also felt to be the least exclusionary and have the least friction compared to other methods, such as those relying on hard identifiers. An example given was engaging with online gaming, where because of the ways gaming platforms are set up and shared within a household, and how they may be used fluidly by different people within that household, AI-based methods are likely to be a more accurate, as well as more fluid and frictionless, way to try to understand the age of each individual user.[21]

Public awareness raising and education

A common theme from industry respondents was uncertainty around the public's perception and likely response to the use of age assurance technologies. It was felt that, to date, there had been a lack of engagement with children, parents, carers and the wider public about the legal and regulatory changes that were coming down the track. Some companies interviewed were concerned that users' lack of knowledge about age assurance meant that they responded with hostility to changes companies have implemented. Part of this, these companies felt, was due to users believing companies had chosen to implement age assurance methods for commercial or data collection purposes, and not as a result of safety legislation.

Industry respondents also emphasised the importance, when developing policies relating to age assurance, of considering the views and opinions of the children and families they would impact. Some company representatives felt that there was limited public discussion, consensus or acknowledgement about the trade-offs that were being made between age assurance and accessibility. It was felt by these companies that this could mean that companies would independently decide what was appropriate.

A number of industry respondents shared that, they felt, the potentially exclusionary impacts of age assurance methods had not been explicitly recognised by the government or regulators. One company safety lead explained that they felt "*confident there will never be a technical barrier to implement any solution"* but that exclusion risks needed to be considered by all parties to ensure a solution was effective and did not unfairly remove access from legitimate users: *"the higher you raise the barrier for an upfront age assurance solution the higher the number of people will be captured, not because they are underage or because there is an objection by a parent but simply because the threshold has created too much friction".*

[21] Epic Games acquiring the children's safety technology company, SuperAwesome, is recognised in the sector as an important step forward. New technology options like Kidswitch (which is being developed to provide an understanding of how to base age assessment on the physical interaction of users with devices) hopes to deliver a passive and relatively frictionless assessment of age.

The desire to avoid hard identifiers

Many of the companies interviewed wanted to avoid hard barriers wherever possible because of the exclusion potential. Some respondents raised concerns about the degree of "intrusion" that requiring an ID or credit card might present, especially the perception from users. Some felt that it would exacerbate exclusion for already marginalised groups, with those with protected characteristics or from lower socio-economic groups being less able or willing to provide a hard identifier. One respondent said that excluding users who do not provide hard identifiers "*would be a huge loss in terms of what the internet is providing…seeing someone who is differently abled thrive and to be able to connect with others is really important… a feeling of not being alone if you are a teenager with special needs somewhere".* This concern was also picked up by those from child safety organisations, and we consider this in part 2, section 8, of the report.

5. Child safety organisations – shared themes, views, and concerns about exclusion risks

This work also engaged with a range of child safety advocates and organisations, as well as those involved in the policy and regulatory space. Whilst representatives from child safety organisations are not directly involved in the technical detail of implementing age assurance technologies, they shared views about the direction of travel for the use of these technologies, as well as potential opportunities and challenges for inclusion. There were a range of opinions and differences shared about the age assurance methods and the implications for inclusion.

Many of the child safety leads interviewed were positive about the changes that regulation would mean to the use of age assurance, seeing this as significant in terms of their positive impact on online experiences for children and young people. The main caveat they had was that there needed to be transparency around how regulation and technology was implemented, to ensure that it remains rights based and grounded in proportional judgements about the best interests of the child.

There were, however, several respondents from this space who highlighted specific concerns about the exclusion risks presented by age assurance. There was a concern that some companies would effectively over rely on users supplying ID or other hard identifiers, or would implement overly cautious or unnecessary 18+ age gates that did not reflect the reality of how we treat older teenagers in other aspects of their lives. A small number questioned whether creating different internet experiences at different developmental stages was a workable or realistic concept for the current age assurance market.

Accuracy vs inclusion

Child safety representatives similarly raised the challenge of creating sufficiently accurate and granular technologies and the volume of data and AI training required. In line with the industry representatives, child safety respondents acknowledged there would inevitably be some degree of trade-off between levels of accuracy and inclusion, e.g. lower accuracy will allow more inclusive approaches. There was an expressed desire on the part of child safety organisations to understand those trade-offs and for careful consideration of them, by government, regulators and companies. It was felt that discussions on this needed to be

"transparent" and to include the perspectives of broader civil society to agree on the right approach.

Child safety representatives felt that, to ensure that children are not excluded from a service that they have legitimate access to, services might have to allow for a larger margin of error in age estimation before considering them to be younger than the required age for the service. An approach that permitted age estimation and establishing age bands rather than specific ages was felt to be more realistic, and also likely to produce better outcomes for under 18s.

Parental consent

Several child safety respondents raised concerns about setting hard gateways for parental consent or verification mechanisms within or as part of the age assurance methodology. Some expressed a view that more innovative technical approaches were important (and more inclusive), and a hope that companies would not be put off from using these. As one respondent explained:

> "*There is a risk that companies get spooked around using biometrics or using back-end data, rather than using them appropriately*. *The problem with relying on verified parental consent is there are some families that will struggle to prove their identity, and there are other families where their parental engagement and judgement is just too varied. This could have the impact of being quite exclusionary, which is quite risky*".

Data minimisation

Several child safety organisations raised the issue of data minimisation and the importance of this principle in underpinning all of these methodologies. Many child safety respondents felt that the role of explaining these technologies to children and young people in effective ways, so they understand how profiling works and data is used, is an essential part of this evolving work. It was recognised that currently children, young people and their parents often have a very limited understanding of the existing data ecosystem and the ways their data is used. It was felt that this needed to be strengthened in order for them to have a better understanding of how age assurance technologies work and their implications for safety. This was seen as playing a role in increasing adoption and trust, and to some degree reducing exclusion.

It was also commonly felt by child safety representatives that there needed to be clear and transparent frameworks in place to safeguard the use of data and the security implications of age assurance technologies. It was felt that the government and the ICO should be involved in identifying and auditing the use of age assurance tools to make sure that they are not collecting additional data or being used for other commercial purposes. It was expressed that this requires a strict legal framework and oversight. There was a positive view of the trust framework approach[22], but it was also felt that there needed to be a strong and effective system of checks and a proactive stance from the regulator with strong action on any breaches. One child safety organisation had strong concerns about the use of AI age assurance technologies and the use of children's data to train algorithms. It was questioned

[22] UK digital identity & attributes trust framework, published by DCMS.

whether the privacy risks presented by these methods were proportionate to what it is trying to achieve.

Impact on excluded groups

There was a commonly held view that age assurance methods, if not implemented with inclusion in mind, may exacerbate the exclusionary dynamics for children who are already to some degree excluded. There was a spectrum of concerns about the impact of exclusion on children, which ranged from the complete exclusion from legitimate age-appropriate access from a platform or game (removal or inability to access services), through to concerns about exclusion from a particular experience or aspects of a platform that might in fact have been appropriate, enriching, or useful because the age barriers have been implemented too bluntly.

A number of child safety groups discussed inclusion considerations specific to children in more vulnerable groups: children in the care system, children with SEN, and children who have been excluded from mainstream school. The anchoring of age assurance solutions in parental consent and hard identifiers was felt to present exclusion risks to children in care. A few respondents raised that foster carers and social workers tend to place greater restrictions on children and this may mean they were less likely to approve legitimate access to a service. There was also concern about individuals who might self-exclude if the process is too frustrating, discriminatory, or confusing for them or if they simply do not have the confidence to manage it or seek support. Respondents also recognised the ways in which AI-driven methods posed inclusion considerations. In particular, raising concerns about whether children from excluded groups would present as a-typical for their age, resulting in unfair exclusion.

It was raised by a number of respondents that those in more vulnerable groups often had the greatest need to be included in the online experience. For those children that already face exclusion in other areas of their lives, removing or barring them from online services could be particularly damaging. As one respondent explained:

"[Research] makes it clear that with children with a range of vulnerabilities… the importance of being online is even more important than for children who aren't facing offline vulnerabilities… and that liberation is really important, so any solution at a user interface level has got to make some sort of provision or consideration for that".

6. Key themes from interviews with companies, policy makers and child safety groups

During interviews with industry, government, regulators and civil society stakeholders some key themes on age assurance and inclusion emerged. A priority shared by respondents was that companies should avoid using age assurance methods that rely on hard identifiers if they had legitimate child users. The exclusion risks presented by this approach were felt to carry a risk of significant user drop off, including the most socially excluded.

Across the stakeholder groups, reservations were expressed about AI-based methods in terms of the use of profiling techniques to infer age, but there was also a view that this would not necessarily be exclusionary. Challenges related to how the algorithm was developed and

the training data acquired. It was suggested by some that clear guidance would be helpful around how companies should build, train, and keep datasets in ways that are ethical and compliant. It was also felt that this build should be reviewed and tested and have public confidence. Inclusion opportunities could be improved by having more comprehensive datasets, and by using these technologies to estimate age bands rather than verify specific ages.

All respondents felt strongly that there was a need for greater public communication on the increasing use of age assurance and the changes to the online experience of children, young people and their parents and carers. This was felt to be important as it was considered that the public has a limited understanding of how their data is currently used and shared.

For child safety organisations a key theme was also around how the technologies would be appropriately implemented, with sufficient oversight and regulation to ensure that they are used and implemented in a way that respects children's rights and sets out very clear parameters around data privacy. This was seen to be critical to public confidence in age assurance solutions, to increase children and young people's willingness to understand and engage in age assurance processes.

Part 2 age assurance from the perspective of children and young people, parents, carers and professionals

7. Engagement with children and young people, parents and carers and the professionals supporting them

This research looked at the experiences of three specific groups of children in relation to their inclusion experience of different age assurance methods. These groups are: children in the care system, children with SEND, and children who have been excluded from mainstream school. This work engaged directly with the children and young people and families of those already most at risk of exclusion to explore how age assurance methods may impact on them. This section of the report covers the findings of these engagements. These three groups often have significant overlaps between them, and some of the children and young people interviewed fall into all three groups. Where possible, analysis has been made of the differences between these groups, as well as similarities and shared themes around age assurance.

This work has sought to explore the different dynamics and inclusion considerations relating to age assurance methods. This recognises that exclusion can occur in a range of ways. These include being fully cut off from access to a service or online experience, for example because a user is unable to prove their age with an ID document, or, if the user is unable to get a responsible adult to engage and confirm their age or ID on a site. Exclusion can also occur if a child finds the experience of going through an age assurance process stressful, complicated, or uncomfortable to the extent that it causes them to turn away from a service and go elsewhere. Also, it may occur where the age assessment methodology excludes a child or young person who is the right age for the service but who presents in a non-typical way for their age, either physically or behaviourally.

The focus of this research is on access to the sites and services themselves. It is not focused on looking at the scope and quality of children and young people's online experience. This is an issue that has been highlighted by other research on excluded groups that identified that children from some vulnerable groups, for example those with special needs, often have a more narrow and limited internet experience compared to their peers[23]. However, where relevant the research does explore existing aspects of these children's digital lives and some of the potential benefits and drawbacks of the wider deployment of age assurance methods.

8. Insights from children and young people

This section discusses the range of insights shared by children and young people who participated in this work. Many of the children interviewed fit into more than one of the

[23] *'Refuge and Risk', life online for vulnerable young people*. Katz, A and El Asam, A in partnership with Internet Matters

groups that are the focus of this study. Overall, a total of 65 children and young people between the ages of 10 and 17 years old were consulted with. Of these, 29 children and young people had experience of the care system or were currently in care. 38 children had some form of SEND and 23 were being educated in specialist educational provision outside of mainstream school (with one child being fully home-schooled). The leading views and perspectives that emerged across the three groups are discussed below. This analysis highlights any perspectives that appear to be distinct to the experience of only one of our three groups. The end of this section of the report discusses specific inclusion considerations for children with learning difficulties.

Support for enforcing minimum age requirements

For many of the children and young people interviewed there was general agreement (at least in principle) that the enforcement of age restrictions or the improvement of age assurance was needed, as current age restrictions were viewed as ineffective. It was felt that there was *"no point* [having an age limit on sites] *if you're not going to ask for proof"*. All of the children and young people who participated in this work had experience of simply entering false ages and dates of birth to gain access.

It was also felt that enforcing minimum age requirements would have some value, especially in protecting younger children. One 15-year-old boy from a pupil referral unit (PRU)[24] described seeing "*videos of people getting stabbed, weird stuff and inappropriate videos"* on TikTok and Facebook, and described watching a viral video of a livestreamed suicide "*a man was live on Facebook and he shot himself in the mouth".* The children interviewed recognised the risks of online harms and the need for a more age appropriate environment. As one younger child expressed:

> *"Sometimes I don't feel safe…I don't like it when people talk to you, like when you have your mic on, random people talk to you…they come through my headset* [when playing Fortnite]*".* Boy, 11 (PRU)

Some young people expressed a strong view that the status quo needs to change:

> *"People in my school have killed themselves over cyberbullying or bullying. Most bullying is done online through social media and it is horrible that people sit behind their screens and do that and get away with it". 'Girl*, 14 (PRU)

For many of the children and young people that we spoke to, there was genuine confusion about what the current minimum age requirements are for certain sites. Some children believed popular social media or video sharing sites such as Snapchat, TikTok, YouTube and Instagram had an age requirement of seven or eight. There was debate about this during the session, because many of the children and young people interviewed were familiar with the children they knew accessing such sites at a very young age.

Concerns over providing identity documents

When asked how they would feel about using ID to prove their age (e.g. a passport if they had one or, for some older young people, a driving licence) the children and young people raised concerns around their lack of access to these forms of ID. This was especially the

[24] PRUs are a type of school that caters for children who are not able to attend a mainstream school. Pupils are often referred there if they need greater care and support than their school can provide. See What is a pupil referral unit? | TheSchoolRun for the situations in which children might attend a PRU.

case for those both excluded from mainstream education *and* in care, as few knew where their ID documents were kept (if they did have them) and many did not have access to any ID documents relating to themselves. For some who did have passports, these were held by parents, and they were not given access. One child explained that their parent hid their passport from them.

The impact on inclusion presented by this approach also depended on how often they would be required to produce ID. One young man who was in the care system (looked after children or LAC) felt that a frequent need to present his ID would be too complex for his family situation: "*if it's every time you use a site, there's no point in using it...it's too much hassle.'* Boy, 16 (PRU, LAC).

It was clear for many of the children that this requirement would present significant difficulties and, for some, in common with the parental consent requirements discussed further below, feasibility depended on their link to their parents who held their ID.

Verified parental consent (VPC)

It was explained to children and young people in these groups that strengthening parental consent mechanisms was potentially one method of age assurance. This could be through a link to a parental account or might involve a parent going through a consent process and showing their own ID. Many felt this would be ineffective, or no more effective than the present situation. Overall, it was felt that parents would be likely to agree to enable access to the services their children wanted, regardless of age. It was also common for children to say that they would get hold of parental ID and simply set up the account as a parent. One boy described how they and their peers were adept at finding ways to circumvent restrictions, "*social media has been around for a long time and I have had a phone since I was about 10, so I have grown up and figured out new ways I can get past restrictions."* Boy, 14 (PRU). A number of children described how they used their parent's email address to circumvent checks:

"*I have access to my mum's email address. So, I put in my other email address and it sends the consent to that other one. And I just gave consent for myself like that.*" Girl, 13 (PRU).

'I've got my mum's email on my phone, so I see everything because her email is [linked to] *my Xbox account."* Boy, 15 (PRU).

There was a discussion in one group about whether a VPC approach would mean that age assurance would operate as a form of parental choice. One young man interviewed felt that it ought to be more of an active parental responsibility with clear parental involvement and decision-making: *"I think that is better than using my ID, I think they should reinforce parental control. I think the responsibilities lie with the parents"*. However, this view wasn't universal across the groups interviewed. Some of the young people interviewed felt that they were able to make their own decisions and parents would not have the time to give consent:

"*We can make our own decisions…there's just not enough time* [for parents to provide consent], *it means a different thing to them…they don't understand".'* Boy, 14 (PRU).

Some children expressed concerns about whether all parents would act in a responsible way towards their child's safety online. A number of children described how their parents were uninterested in what they did online and showed poor judgement in relation to their safety and wellbeing, "*Some people's parents let them do stupid things, like my mum at age 13 was*

letting me drink… what makes people think she's not going to let me go on something that I want to go on?" Boy, 15 (PRU).

Privacy was also commonly raised by children and young people when discussing VPC. It was felt there should be a balance in terms of how much involvement parents would need to have. There was a concern that parental consent could go beyond the checking of age and expand into parents potentially having stronger visibility on all aspects of their online lives. Children described wanting to have privacy from their parents over what they did online: "*I wouldn't want my parents to know what I was doing…maybe* [only give consent once] *rather than all the time"* Boy, 15 (SEN). One child described having blocked their family on social media because *"most of my stuff is private"*. There appeared to be a greater level of acceptance of parental involvement on the part of younger children.

> *"If my parent said I can't go online for safety, I would be fine because I want to be safe."* Girl, 12 (PRU).

The young people interviewed were often sceptical about parents using age assurance on their behalf as a reliable or feasible method. The children and young people did not generally raise the idea that their parents might not have the capacity to set up linked accounts – but they tended to express the view that they would do this fraudulently themselves if necessary. This could reflect that they have not yet experienced barriers around parental consent or account confirmation that present significant challenges (or require parental ID for example). Many of the children and young people that took part in this research presented a picture of parents who were largely disengaged from their online lives.

Biometric data

The idea of using different kinds of biometric data to infer age was discussed with the children and young people, this included the use of facial scans as a relatively advanced technology in this space.

The groups of children and young people involved in this research were largely accepting of the idea of using biometric data in this way (including taking a facial image for analysis). They were also familiar with the use of finger and thumb prints for unlocking their phones. Many did not have a problem with this, if it enabled access to the service. One young man reflected on having analysis of a facial image as acceptable given the level of other data that children already share:

> *"I wouldn't mind taking an age photo… some people may not feel comfortable taking a picture of their face - that being said, if you get a social media account, you share things on there."* Boy, 14 (PRU).

Some, however, initially disliked the concept and were hesitant about this method of age assurance. One young person was adamant that he would not want to have a selfie taken under any circumstances (even when it was explained that the picture would only be used by a computer and not be kept):

> *"No, I wouldn't do that…I don't want random people seeing a photo of me to confirm my age…I think a lot of people would be insecure about using a photo of their face, so wouldn't do it and wouldn't be able to get access."'* Boy, 15 (Mainstream school, LAC).

In general, however, there tended to be greater acceptance once the process (and the principle that the photo would not be stored) was explained properly. One young person said that the methodology "*wouldn't bother me… because no one would see that photo…*[although] *I would flip my lid if it said I wasn't old enough."* Boy, 13 (PRU).

Some young people expressed an anxiety around the accuracy of biometric facial analytics solutions, and that they would appear younger than they perhaps should. This made them nervous about using the technology. Several young people expressed concerns about accuracy for their age group, with children commenting that some children look older than their peers while some look younger "*Some 14-year-olds look about 10 and you have some that look like 20, even though the technology is getting more advanced it would be hard to tell someone's age… just by their face."* Boy, 14 (PRU).

Some of the children interviewed expressed worry about the security of the process. This concern remained even after it was explained that the image would not be stored: "*But for that split second, someone could be hacking and make it go slower so they can get the picture, then keep it, then they still have it'.* Boy, 12 (special school).[25]

Behavioural biometrics

Another area of biometric data discussed with the children was the idea of behavioural biometrics - age estimation from physical interactions with the device (typing cadence, swipe, mouse click etc). Many of the young people we talked to thought this was '*weird*' or *'creepy'* but most did not raise particular concerns or barriers for them. One young person described it as being "creepy" but was also impressed by the technology: "*It's kind of creepy how that sort of thing could happen and how they would work out your age but kind of clever. Yeh I don't mind that."* Boy, 15 (LAC).

However, some children raised concerns they might be slower as a result of lower literacy levels making them slower at these functions and therefore giving a misleading picture of their age. One child described their concern that they would present as younger than their peers:

> *"I am definitely slower at typing than my friends and my spelling isn't great – I think that would be a problem when working out how old I am, because probably they'd think I was five or six or something by just looking at how I use a laptop or iPad."* Boy, 10 (SEN).

Profiling

The general view of the groups of children and young people in relation to profiling age assurance methods was that, although they felt it to be a bit strange that data would be gathered in this way, it was acceptable to them. However, a small number expressed some concerns and unease about this methodology in relation to the volume and type of data platforms would be collecting on users. One young girl expressed concern over what the implications were for sharing greater data with the platforms she uses:

> *"Social media platforms already have so much information about you, your personal password, date of birth (fake or not), email, where you are from... They can have your precise location on some of the apps …. I feel they have too much power over so many people."* Girl, 13 (PRU).

[25] Special schools are those that provide an education for children with a special educational need or disability.

For some types of platforms, children and young people expressed uncertainty about whether a profiling method would accurately estimate a user's biological age. They gave the example of gaming where players may have a maturity of playing ability that was not representative of their biological age: "s*ome 12-year-olds would be better than 30-year-olds… how does that work? Most adults do worse than a 12-year-old."* Boy, 16 (PRU). Similarly, several young people expressed concern about whether they or others could be disadvantaged by this method, for example if you had less mature or age typical behaviours or interests. The potential impact on children with learning difficulties was also raised: "[if] *you have Down's Syndrome, then you're a bit* [less advanced] *… on that site but you're old enough to be on it… and it kicks you off... that's a problem."* Boy, 16 (PRU). In these circumstances, some of the children interviewed felt there would be a role for parents to give consent for access *"but parents should be able to help them on the website".*

The accuracy and reliability of profiling methods on shared devices and accounts was also raised. One child gave the example of regularly sharing their phone with a younger brother: "*he normally watches Ben and Holly, Peppa pig... If someone was helping their friends with a problem who might be young, then they may think this person is younger because she is searching up Peppa pig".* This child also questioned what would happen if a parent borrowed the phone, *"My mum uses my phone a lot when her phone is dead. So, she might search up things that are much older and they could look at it and then be like, this person is way too old and should not be on this app.".* Girl, 12 (SEN).

Capacity testing

Capacity testing assesses a user's age by testing their abilities to see if they are typical for age-based norms. This could consist of a puzzle or set of questions that a child or young person could be expected to be able to complete for an age or age range. For this research, capacity testing was discussed in the context of providing services with broad parameters of age. This approach was received with anxiety with the children and young people who participated in this research. Many knew that they were educationally behind their peers or had specific learning difficulties which would mean they would present as a-typical for their age: "a*nything with reading and writing I am out*." Girl, 14 (SEN).

Data privacy concerns

All of the groups of children and young people interviewed expressed concerns around their data security and use of their data. In general, these concerns tended to relate to fears over potential fraud or criminal activity:

> *'That would be a massive safety hazard… let's say something happens to that site or that bank they have people's ID.'* Boy, 16 (PRU)
>
> *'It could be a scam… when you tell people your ID, they could steal your ID and do stuff… I would just put in fake stuff. So, you don't know who it is or what it is. So, you are safe from them stealing your ID.'* Boy, 12 (Special School)

However, while concerns about data privacy and data security tended to focus on the risks of hacking, fraud, and identity theft, some respondents shared broader concerns that companies might hold onto their data or might not be truthful about what they say they will do with it. It was common for there to be uncertainty about whether you should trust a technology company:

'It might be used for something else… I trust them but sometimes people you trust sometimes lie to you.' Boy, 16 (SEN)

Some young people expressed that they would prefer an independent third-party verification system that allowed them to have an age token, rather than a company collecting data and knowing more about them:

'That is a lot better, I don't know why. I would feel a lot better. If I wanted to make a Facebook account… Facebook would have that [data about me] *but if it were a third party* [identifying my age] *I would probably feel better.'* Girl, 15, (SEN)

Overall, we found that these young people, despite some anxieties about data, would share data in return for access to the online sites and services they wanted to get onto. Whilst some children mentioned finding other sites or going elsewhere, mostly they were willing to share data despite their reservations. The young girl quoted below was typical in having significant reservations about data security and identity theft but indicating that they would not stop her seeking access to sites:

'I would think it's almost like a trap. If you give them your information and ID, they could do whatever they want with it really…. If you show people, show the sites your ID they have a photo of you on there, your name and like your age. They could use it for whatever really. I have heard of it happening. It wouldn't be me but other people like teenagers or older people on there, they could take it and make a fake ID to get into parties…' Girl, 12 (SEN)
[Interviewer - would this stop you going onto sites?]

'No, I would probably still do it.' Girl, 12 (SEN)

Considerations for Children with Special Educational Needs and Disabilities (SEND)

This section looks at some inclusion considerations facing children with learning difficulties. In terms of the national picture, the children with special educational needs and disabilities are the biggest and most diverse group that this research engaged with. SEND encompasses a very broad range of levels and types of need. This picture was reflected in our engagements with a significant diversity and spectrum of need within the research group. There were also some very significant differences in family background among this group - with many of these children having very informed, vigilant, and engaged parents. This was distinct from the more challenging family backgrounds of many of the children that the research engaged with across the other groups.

The prospect of sharing ID documents for age assurance purposes caused some concern with SEND children, including one group of children with moderate learning difficulties. This was similar to the other groups of children but was more pronounced. This group had experienced a range of previous ICT sessions on digital safety that had reinforced why they should never share their personal information. Age assurance methods that relied on ID raised questions and uncertainty from them about why you would use these methods for age assurance. The young people in this group struggled with understanding the change or shift

in this messaging which contradicted previous messaging they received about staying safe online.

This group also had some of the most significant learning difficulties among the children we engaged with and they found it difficult to grasp how these methodologies would work safely and why they would be justified. For one young man, the idea of profiling felt too intrusive, and his responses showed that he struggled to understand or accept how it would work in practice. When the methodology for profiling was explained to him, he tended to return to an idea that it would include monitoring of individual personal messages. The experience with this group suggests a need for further work and tools and resources to support children and young people with SEND.

One of the participating groups was a small group of children with autism. They expressed similar views to other children about the methodologies. For one of these children, the concerns about data privacy were more fixed and extreme. They explained that they were so concerned about the treatment of their personal data online that they would read the terms of service and the company's data policy: "[If people don't read the policy] *they don't know if it's a legitimate* [service] *or a copy. Their details could be found out and tracked."* Boy 15, (SEN).

One young person interviewed for this research had severe dyslexia, such that she could not use the internet. This serves as a reminder that some children with more severe learning difficulties may already be excluded from using the internet (or have a very narrow experience of it). Despite being 16 years old, she described her only internet use as occasionally using Roblox (not logged in) and engaging with other platforms via her friend:

> *"Sometimes, if I am sitting next to* [my friend] *and she is scrolling through Instagram, I might look over and watch what she is doing, and she will show me something but apart from that because I can't read anything or write anything, I don't feel like I am missing out."* Girl 16, (SEN)

9. Parents and carers

This section looks at the insights from foster carers, parents of children who have SEND, and parents of children who have been excluded from mainstream school.

Foster carers

The discussion with foster carers offered insights into the complexities and challenges of providing care for children who are perhaps among the most highly vulnerable online. Several high-risk issues were raised in the margins of this discussion. Many of the foster carers we spoke to had had police involvement in their children's digital lives due to dangerous and harmful incidents and relayed that they struggled to keep them safe.

Perhaps as a result of the extent of the challenges facing these foster carers, they were highly supportive of the purpose of age assurance methods, despite flagging some concerns about practicalities of some aspects of them. There was a strong feeling that clearer efforts from the platforms themselves to enforce age assurance would be helpful for their own digital parenting. Currently many of them feel unsupported in trying to help the very vulnerable children they care for stay safe on platforms. It was felt that platforms proactively

doing more would help them in their relationships and in their day-to-day negotiations and discussions with their foster children about keeping them safe:

> '*When this becomes legislation, it will be easier for us to discuss with the children'.*

It was also felt it would help with the peer pressure issues around some of these platforms, where some children the same age are allowed, and others are not. This issue was raised by other parent groups too. The emotions around peer pressure were felt to be particularly intense for children in care.

There was also a sense that, although some of the methods may feel challenging to start with, this could dissipate if they became an everyday feature of the ways children and young people use the internet:

> *"Hopefully, long-term for every user, it will be part of it if you want to purchase* [or use a game or online service] *…[it] won't be emotive… it'll be part of it if you want to use this game…"*

Parental consent

An age assurance method that relied on verified parental consent presented complexities for foster carers in relation to the boundaries of their own role in online parenting and its relationship to the children's social worker. They explained that their judgement and that of the social worker did not always align. One foster carer gave a recent example that their child who is underage has been allowed to play a PEGI rated 18 game by his social worker (because the multi-player game was important to him socially). Others had a range of examples around the social worker being more permissive around age rating. Therefore, if an age assurance method relied on parental consent there would be questions around who the 'responsible adult' should be providing consent: the social worker, or the foster parent.

Overall, in practical terms, they felt any parental consent requirement would need to be offered by the foster carer as they hold the day-to-day relationship. However, they felt it was often challenging making the right judgements around these issues. They felt more training and support was needed and the extent of their delegated authority needed to be clarified and strengthened.

Challenges with ID and officially provided data

Obtaining ID documents for the children in their care was felt to be very challenging by the foster carers who participated in this research. The children they care for often lack stability, moving home frequently and not always having ID documents or knowing where they have stored their passport, if they have one. Several carers were particularly apprehensive about the requirement to enter their credit card into a platform or site to link accounts. This related to their experience of children accessing their credit-card details through games and spending large amounts of money on in-game purchases.

Some felt that putting credit card details in would be relatively straight-forward and acceptable, but willingness would relate to whether the service or platform was trusted and "*how many of these companies are genuine*"? Some foster carers felt that the children in their care would find ways to circumvent gateways that required ID by using older friends' or siblings' details to create accounts and, if necessary, by getting hold of parental ID without them knowing.

Age estimation using biometric data

Among this group there was support for the idea of using biometric data to estimate age, specifically a facial image. Overall, this group felt that children taking pictures of themselves was already a part of their lives, and provided that the data was not held on to, this was regarded as a valid and relatively frictionless method. There were, however, concerns about whether it would be circumvented. They felt that the children in their care were adept at getting around restrictions.

They raised some issues around the data protection implications of these methods and specific considerations for children in care. They recognised that images would not be retained or posted, however they explained that children in care should not post pictures of their faces online or share their location because of the contact risks - so these methods could confuse established messaging: "*we cannot put photos of the children on any social media at all, I'd be concerned* [about using this method]*."*

Age estimation using behavioural data

Generally, the group of foster carers interviewed for this research felt that continuous monitoring methods such as profiling would be effective and beneficial, and they did not have a problem with services using data in this way. Many in this group were more comfortable with a 'passive' (as they saw it) AI-based methodology as this would be less likely to introduce conflict or stress in their households - in contrast to requiring an ID or a parental consent process. They also felt that this methodology would limit the ability for children to circumvent the check.

Parents of SEND children

Individual, one-on-one interviews were held with parents of children with SEN.

Parent of a child with Down's Syndrome

We spoke to one parent of one of the moderate learning needs group, whose son has Down's Syndrome. She described him as having good ICT skills. She expressed some concern about his safety online, in particular she felt that his learning disability had made him more susceptible to misinformation. This parent was supportive and accepting of all of the potential methodologies of age assurance. She explained that the nature of her son's disability means he has less independence and that sometimes, when he does not understand something, he seeks support from his parents or brother. However, she also raised the risk of self-exclusion. Despite the online world being incredibly important to him and him spending a lot of time on it, she felt he would struggle more on encountering barriers or gateways: *"he's more likely to give up trying to access a site as he wouldn't understand what was required".* This was something that she felt was likely to happen if a site relied on ID for age assurance, where he was unlikely to persist with a process if it was complex.

This parent had concerns about age assurance methods based on behavioural data. She felt that this could be potentially exclusionary for her son as he would be unlikely to present as age-typical, due to having interests and preferences that were usually held by younger children. She was worried that, if an incorrect age estimation was made and then shared with other platforms, that it could disadvantage him and reinforce exclusion. Overall, this parent preferred the use of verified parental consent as it would provide more protection and

'a little bit of control' in terms of what her son was accessing, however she also felt he would be likely to need parental support.

Parents of children with Autism

We spoke with a group of parents whose children had autism. There were concerns about the data implication of age assurance methods, in particular methods that used IDs: "*they do have passports but I would be concerned when asking us to upload pictures of passports. Is that safe? I don't trust the platform. Who is going to get hold of the information? I don't trust them… I would worry whose hands it would get into and would someone start cloning identity".* This parent explained that she did not trust online platforms with personal information and would feel more confident if a third party was responsible for the process.

In contrast to her hostility to the use of an ID document like a passport, she explained why she would not worry about the user privacy implications of AI-driven methods: *"They [technology companies] gather so much data, so to pick out one person and to try and take issue with them is going to be very difficult…The chances that they are looking at my kids are very slim".* For methods that relied on a facial image it was felt that this didn't provide "*any important information ... it's just a picture".* This was aligned with many respondents' concerns about data privacy.

Data privacy was generally a worry in relation to data breaches where an individual could have their data stolen as a result of a fraudulent site or because the platform's system security was insufficient. By contrast, there were fewer concerns raised about the potential for companies to harvest data and use it in a way that went beyond the stated purpose of the initial collection. Data risks such as data being unfairly shared with others, or collected and aggregated for commercial purposes, were less prominent. This may be due to a lack of awareness or knowledge of these issues or because this kind of risk can feel more abstract to users.

Concerns were raised around methods that relied on behavioural data, in common with other parents of SEND children, around access and whether these methods might produce an inaccurate result that would lead to their children being unfairly excluded. One parent explained that her children's viewing habits were likely to produce an inaccurate result:

> *"People with autism don't fall into these* [age] *categories...My daughter is quite childlike in her behaviour. With an autistic child, they fixate on things a neurotypical child would not fixate on, it's difficult...So, the site will say 'well you must be a child' but you're not it just your brain is wired to do things differently. How do you take that into account?".*

Overall, these parents expressed strong support for age assurance processes (and the protections they could bring) due to the lack of social understanding and awareness her children have. One parent explained: *"I know our youngest, if someone* [online] *said I'm nine, I live in London and I go to this school, he would absolutely believe that".*

Parents of children educated outside of mainstream school

We spoke to a number of parents of children who were being educated outside of mainstream education who shared their thoughts about the challenges around exclusion from mainstream school as a specific aspect of digital parenting. One parent described how

many parents with children in alternative provision had given up on active and positive involvement in their children's online lives:

> *"Parents whose kids aren't in mainstream school just feel at a loss: they feel like they've no control and the system is telling them to control their kids, which hasn't worked because they've rebelled against the system...I think, with the internet, it's don't do this because it's dangerous. There's never really any information on the good stuff on the internet".*

This parent explained that the inconsistent way in which age restrictions were enforced - children and young people using different internet services at different ages, depending on what their parents allow - had caused difficulties for her children and tension between her and other parents. She explained that, despite the fact she allowed her children a lot of 'choice', believing that children needed to learn through experience and mistakes (she had had to get the police involved with her daughter because of attempted grooming on Instagram), she was still seen as a 'strict parent' by many others that she knew for setting any boundaries at all. She felt it would be a positive thing if access were restricted for underage users.

This parent was relatively supportive of all the age assurance methodologies in this report and was accepting of the more advanced methods. She could see the advantage of those that relied on biometric data: *"quick and easy. If you're told within a couple of seconds or minutes that yes or no, I think that's quite good".* She also thought methods that relied on behavioural data could work well too. The use of personal data was not a concern for her seeing it as *"the way the internet is going anyway...We willingly give our data away, so it's just expected… when anyone uses the internet, it's out of your control what algorithm is running behind it, it's kind of what you buy into isn't it?".* Although this parent, in common with many of the parents we engaged with, would be resistant to using a credit card:

> *"I wouldn't put a credit card in, they rinse them… We've been down that path. My son spent about £400 pounds on the Xbox, not even on my account, it was my sister's… and she couldn't end up paying her mortgage that month. No credit cards are linked to my kids accounts".*

This parent was convinced that many children would circumvent age assurance methods. For example, deliberately creating a distorted picture of their age online by typing differently or searching for content popular with an older age group to skew their age demographic.

However, it was felt that age assurance methods would have a valuable contribution to make, even though young people may find ways to circumvent safety measures:

> *"There's never going to be a 100% way of keeping the kids safe online".'*

10. Professionals

As part of this research, one-on-one interviews were held with key professionals. These included professionals who work in pupil referral units (PRUs) and specialist educational settings. This group showed strong support for the ambition of age assurance and the safeguards this would entail:

> *"From a safeguarding position, absolutely, I think it's the right ambition. I think it's quite late in the scheme of things, I'm surprised we are only talking about it now. I've*

taught in a school for 10 years… I'm happy it's being addressed or attempted to be addressed…you are safeguarding those children from grooming from all kinds of issues that vulnerable kids might get into…"

For many of the professionals we spoke to, they were (as specialist teachers) one of the most consistent professionals (and, in the case of children in care, among the most consistent adults) available in the lives of many of these children. These teachers often described their students as having challenging home lives, and emotional difficulties that resulted from this. Many of these children were also in the care system.

These professionals highlighted the risks taken by the children they work with and the level of "naivety" in their attitudes. This was seen to be particularly the case in relation to meeting strangers or believing people are who they say they are online, where it was felt they were more likely to seek attention and affirmation from adult strangers. One teacher felt that the children he worked with (at the more excluded end of the spectrum) struggle disproportionately with some of the negative and difficult aspects of the internet: *"the majority of their experiences online are negative. It's what we deal with on a Monday, especially after a long weekend on these platforms, the abuse, whatever has gone on...*[it is] *basically spilling over into our settings".* It was felt that the exclusion that these children have experienced was driving a desire for connection, acceptance, and relationships that they can find online:

"They have been excluded from so many different settings, including maybe the family setting, friendship groups, school groups, by the time they get to us they have probably failed in up to 10-12 settings... this is why they are online so much and get into so much trouble and get into inappropriate situations… maybe in the back of their minds they think I'm not quite sure about this… because they want to be accepted and they want to be loved… they put themselves in that situation anyway."

ID and Verified Parental consent for children in care

The professionals we spoke to expressed that any formal requirement for an ID document could create a significant barrier for their kids, especially for those in care who often do not have access to ID. Similar thoughts were expressed around methodologies dependent on parental consent. They explained that because foster children can move homes and carers so frequently it can present challenges for providing a responsible adult. Similarly, a new foster carer may not know the child's ability or what is safe to allow them to access online.

One teacher explained how, even for children who were not in the care system, the parents of more excluded groups were much more challenging to engage with. They explained it was common for the parents to struggle with literacy and numeracy. They felt that this may present challenges for some age assurance methods, where parents might struggle to understand what a platform was asking them to do. In addition many of these parents would also be unlikely to have a passport or access to ID, *"I think some of them* [the parents] *would have a bank card, although not all of them and not necessarily a credit card".*

One teacher had concerns that relying on an adult to engage with an online process and provide an ID (without checking that they held parental responsibility) could further draw these children into some of the exploitative relationships they faced with adults who were not

their parents: *"we have a number of kids who are exploited by county line gangs who ask them to do XYZ and they then give them £10, £15, £20 pounds".*

Methods that rely on biometric and behavioural data

In general, this group was supportive of AI methods that rely on biometric or behavioural data, considering them to be more inclusive for children. There were concerns around how companies would use the data. However, provided there was reassurance around this aspect, they felt the method could work well.

Methods that rely on behavioural data were broadly supported as an approach that took pressure off parents, carers and households. The concerns raised were more about whether it would hold up as a technical solution in a world of device-sharing and in situations where there may be no requirement to sign in. It was considered to be standard for a device to be shared between family members, with children and adults of different ages searching and viewing different content.

In common with the parents' groups, concerns were raised over whether behavioural profiling would accurately 'read' a child's age'. Many of the children they work with are developmentally behind their peers and might present as younger than their age. There was a concern that this may mean that they are then subject to more intrusive profiling from the platform, or removed from the platform, or asked for ID, rather than being accepted by the site or platform as the age they are. One teacher explored this further in terms of developmental gaps where children have been excluded from school and had long periods out (away from school and peers). He felt that some of his children were using the online environment to fill the gaps in their development and education "*they would probably be quite ashamed if those in the 18+ knew they are still watching 7/8 age-appropriate stuff".*

Transition to age assurance

There was a view from professionals that the transition to an online environment where age assurance was used widely needed to be considered carefully. They felt that children and young people needed appropriate support to understand the process, and offered enough flexibility of methods for them to achieve age-appropriate access. One teacher raised the issues of younger children needing additional support if access to social media was removed (e.g. because they are under 13): "*some of them use social media as their only means of communication and, if we take that away from them again, how do we monitor that in terms of mental health and what they then get up to".*

11. Survey Data

Online, interactive surveys were used to reach a larger group of children and young people, and parents and carers. The aim of the surveys was to find themes and views from a wider pool of respondents and contribute to our analysis and findings. An important caveat in relation to the survey data is the fact that some of these methodologies are difficult to present and explain via a survey. Some age assurance methods are complex in terms of both how the technology works as well as the nuances of how they are likely to be

implemented. A survey may be more conducive to people sharing their initial thoughts and feelings about an approach as opposed to a more informed view.

The adult survey was completed by 61 respondents, including 57 parents/and or carers (three residential care workers and one social worker) and 48 children and young people. Although the survey was sent out via channels that were selected to target our three groups, we found that ultimately many of those that completed the survey fell outside the target groups. Of the 57 parents, only 22 of the parents who completed the survey had children who were a combination of SEN, LAC or out of mainstream school, and there were 4 professionals with relevant experience. Of the 48 children who completed our survey, only 16 of them chose to identify that they were in one or more of these respective groups (a further ten stated that they would prefer not to say). The survey data also skewed to a slightly younger age group of children and young people completing it.

However, despite these caveats, the survey data was useful in reinforcing many of the themes that arose in the qualitative data and suggested the potential for some commonalities between the parents of our more excluded groups and other parents. The survey data suggested that many people (children and young people and parents and carers) across all groups had concerns about all of these methods from the perspective of the safety and security of their data, with 46 (75%) of those who completed the adult survey indicating that they would be concerned that their ID details would fall into the wrong hands and 44 respondents (65%) indicating they would not trust companies to not use the data for other purposes. This was particularly the case if children were using some form of their own ID. This concern lessened somewhat if it was a parent-led process (with parental ID and consent) but the concern was still present with 21 of the total adult respondents (34%) saying that they would not trust the site with their own details either. There was also a significant minority of parents who stated that they would struggle to be available for parental consent processes (14 respondents, or 23%), that it would invade their children's privacy (nine respondents, or 15%), and that it would cause conflict in their home (seven respondents, or 11%). In addition, two parents stated that they did not have access to ID and one foster carer that they did not have the authority to give parental consent.

The parents and carers survey demonstrated similar concerns about biometric data and profiling techniques as there were to the use of ID. In relation to the collection of biometric data, the majority of survey respondents (34 respondents, or 56%) felt that it would depend on the precise method and how it worked. However, 34 respondents (56%) said that they did not trust companies to delete the data and 36 respondents (59%) had the concern that it would fall into the wrong hands. The least favourable method in our survey was age estimation from profiling, with more thinking it would be an issue (33 respondents, or 54%) than those considering it not an issue (26 respondents, or 43%). Here, concerns related to accuracy and fairness for their child (37 respondents, or 61%) as well as a concern the data could fall into the wrong hands (33 respondents, or 54%) or be used for something else (27 respondents, or 44%).

In terms of the children and young people's survey, it was clear that most of the methodologies seemed acceptable to children and young people but that, for a small group, several of them were not acceptable. Nine (18%) of the respondents, for example, stated that finding an ID document would be a problem and for eight respondents (16%) parental

consent would also be a problem. A significant minority of 11 respondents (22%) would not be happy with the use of age estimation or profiling techniques, with eight respondents (16%) saying they would be unhappy with the use of biometric data.

The surveys overall show that there was no consistent signal around any particular methodology being the clear one to use for all groups, and for all methods some reservations and anxieties or reluctance was evident. The surveys reinforce the importance of making sure that the methodologies are explained to users and that safeguards around data security and privacy are put in place and communicated effectively. All of these methods need to be explored and explained in order to enhance their acceptability and the confidence with children and young people, and their parents and carers.

Part 3 Findings

12. Discussion and analysis of exclusion impact

This research is focused on understanding the inclusion considerations presented by age assurance technologies in relation to children and young people's access online. To understand the uptake of different age assurance methods within technology and social media companies, as well as the potential inclusion and exclusion considerations associated with them, this research conducted a wide range of interviews with companies, regulatory and standards bodies, policy makers and child safety groups.

In addition, to fully explore the ways different methods might contribute to exclusion, children and young people from more excluded groups were interviewed. This included children in care, children with SEND and children educated outside mainstream school, as well as their parents and carers and the professionals who work with them. This has provided insight into how different age assurance methods would be likely to impact on these children and families.

The children, parents, and carers interviewed for this research ranged in their vulnerability to exclusion, exhibiting a range of attitudes, knowledge, and resources with which to approach their online lives. In addition, there is currently limited visibility on the age assurance methods that the major platforms will choose to implement and how they will look at addressing inclusion considerations. All of this context has an impact on how individuals within different groups would experience or approach different age assurance methods.

Notwithstanding the above, the research revealed some common themes in relation to exclusion. These are:

- **Potential barriers or blocks to access** e.g. not having a 'hard identifier', particularly an identity document (ID) such as a passport. Or having a parent or carer that does not have access to a hard identifier eg. passport, driving licence, credit card or credit/financial records.
- **Processes that could make it harder for children and young people to access a service** e.g. a parent who is not accessible, or a foster carer that does not have authority to give consent.
- **Technology that somehow discriminates** based on developmental capacity or physical features in a way that could create an unfair exclusionary barrier.
- **Self-exclusion on the basis that the process is difficult or complex** to understand for those with additional needs or learning difficulties.
- **Self-exclusion on the basis that parents, or children do not feel that their data will be used safely or securely.**

Key Findings

The research has looked at four broad categories of age assurance methods and assessed the inclusion considerations presented by each method. This assessment has been informed by interviews with children and young people, and their parents and carers. As well as representatives from technology companies, age assurance providers, regulators, policy officials, and child safety organisations.

Our analysis found that no single age assurance solution worked for all the user groups interviewed for this research. All of the measures presented a degree of exclusion concern however, they also all presented benefits and opportunities for inclusion, depending on the circumstance of the user. This was due to the varied and complex backgrounds of the children, parents and carers that were interviewed. This highlighted **the importance of providing users with a range of age assurance options to maximise inclusion**. This research found that some online platforms were already exploring a 'layered' approach to age assurance, where they combined a number of different age assurance methods. Their motivation for this was to improve the accuracy of the age check. But it may also, based on the findings of this research, present the best way to maximise inclusion for children and young people.

Hard identifiers

- This approach is commonly referred to as age verification. The method relies on hard identifiers such as a passport, credit card or driving licence. As this information is only possessed by persons of a known minimum age, or, is linked to their identity it generally provides a high level of confidence in the age of a user. In general, this approach was found to be the least inclusive of the four methods that were discussed with participants.
- The children and young people in the groups interviewed for this research generally did not have (in line with their age) suitable forms of ID or independent access to it - although a small number had a passport. There was often a complete lack of ID documents (or means to apply for them) for children in the care system where ID was felt to create a particularly acute barrier, and this was especially true for the subset of children in short-term care placements. For these children, our research found that an age assurance method that relied on ID or another hard identifier would create significant exclusion risk for these children and young people.
- In addition, the children and young people interviewed expressed concern about the security of their details if they were required to enter ID information into a site.

Parental consent (and ID requirements)

- Verified parental consent commonly requires an adult to verify their age to confirm the age or a child user and/ or approve access to a service. for a child user. It also relies on a hard identifier, commonly a credit card. The research found a mixed response to this method, depending on the degree of engagement parents had with their children's online lives.
- For some SEND children this approach felt the most natural. Their parents already have a high degree of engagement with their safeguarding and these children may otherwise struggle to navigate an age assurance process independently.

- However, some of the children and young people interviewed for this research raised issues with parental consent in relation to difficulties of engaging with their parents about their online lives and the need to have privacy from them. There were also concerns about whether parents would be able to execute age assurance processes effectively. Whether parents would have the relevant literacy skills and confidence to go through an online parental consent process or to set up a linked account was also a concern raised by professionals in the care and SEND sector.
- The professionals interviewed also raised concern about the willingness of many of the parents of children outside mainstream school to engage and act protectively towards their children. The risk that children would easily circumvent parental consent processes was also raised.
- Some of the carers and professionals interviewed felt that there was a risk that for children in care there was a lack of access to a person with 'parental responsibility' to provide parental consent (and make appropriate judgements about consent) and this was seen as especially the case for children in short-term care placements. There were a range of reasons described for this, including a lack of training and support for carers as well as a lack of clarity about the terms of carers' 'delegated authority'. It was felt that this issue needed to be clarified if parental consent requirements were to be implemented more strictly.
- Several parents and carers interviewed expressed their reluctance to enter credit card details due to the widely shared experience of having children run up significant bills through in-game purchases. The experience of losing money through in-game purchases was common in the sample for this research.
- In addition, there was widespread anxiety from parents and carers about data security. In general, there was more concern about entering personal details or documents and having these corrupted or stolen, than using methods that relied on AI. Some parents were adamant they simply would not supply ID documents for themselves or their children.

Behavioural data using Artificial Intelligence:

- This method refers to the use of artificial intelligence (AI) to build a profile of a user's age based on their behaviour on a service, for example the accounts they have interacted with, what they have liked and content in posts or messages. It can also include analysis of a user's typing or literacy to estimate age. This category of method provides an estimation of age, as it is currently unlikely to provide a specific age to a high level of accuracy.
- Those interviewed for this research were generally receptive to and relatively positive about AI-based age assurance methods. These methods were generally seen to be the most inclusive for vulnerable children and young people. which could be used for age assurance purposes and there was generally no hostility to these methods.
- Some respondents believed that behavioural biometrics held promise because it would be relatively frictionless and inclusive, and felt the data to be less personal than other forms. A number of respondents reinforced that safeguards around the use of these technologies and the data collection was important (and some respondents suggested having an independent third party perform this role would be reassuring).

- A widespread concern in relation to profiling was about whether children from the more excluded groups would 'read' as their true biological age within AI methods that assess age - particularly in methods that used content viewing and interests - or whether they would appear atypical for their age and face barriers to access as a result. There was concern about the potential for children with disabilities to appear atypical from biometric data e.g. by having less advanced fine motor skills. This issue was raised by children and young people themselves as well as parents, carers, and professionals. This related to a concern that these children could face more gateways, intrusive methods, or unfair exclusion from a platform in a way that could significantly impact on their wellbeing.
- Some of the children, young people and parents interviewed preferred an ID based method, regarding them as more transparent. However, there was commonly a view that AI related technologies were part of life and should be used for good. Amongst many there was an active preference for AI technologies and approaches.

Biometric data and Artificial Intelligence

- This is an emerging type of age assurance method, which uses biometric data and AI to estimate a user's age.
- There was generally support from children, young people and parents for the use of biometric data (in combination with AI technologies) as a relatively frictionless method of age assurance. A small number of respondents instinctively disliked the idea of providing a facial scanning for age assessment, but most respondents we spoke to felt it could work.
- An important inclusion consideration for biometric methods, which is evident from research and raised by companies, is in relation to race and ethnicity, where the technology performs less well for darker skin-tones.[26] The issue of potential racial discrimination and potential disproportionate exclusion of certain groups needs to remain in focus when considering exclusion risks.

Wider themes

In addition to the considerations identified above, wider themes emerged during the interviews, that were not explicitly on inclusion but have an impact on improving inclusion in the use of age assurance technologies.

Support for age assurance processes

We found a marked difference in appetite for age assurance between companies and services implementing these approaches and the views of parents, carers, and professionals. Those working within companies described several complexities and challenges including customer resistance and hostility, worry about user friction and exclusion risks, and concerns about offering a potentially reduced experience of their service. In contrast, the view from the parents, carers and professionals we interviewed was overwhelmingly positive and supportive of age assurance being properly implemented and enforced. The parents and carers from these groups shared that they are often struggling on

[26] Publication note: Since this research was conducted, progress has been made to improve performance of age assurance technologies for darker skin-tones. Please also see footnote 17.

a day-to-day basis with keeping their children safe online. Many of the parents and carers interviewed for this research felt that legislative action to enforce minimum age requirements on online platforms could help to reduce the conflict in their households, reduce peer pressure and help to reinforce some of their own protective behaviours. Whilst they relayed some concerns about different age assurance methods, they were highly supportive of the aim of age assurance and understood its potential to support safeguarding.

The views of children and young people themselves were more mixed, but they too seemed to understand and accept the principles of how age assurance methods worked and their role in online safety. Key concerns for young people interviewed for this research were security of the data and fairness in how age assurance was applied. They wanted to be confident their identity would not be stolen and used, and they wanted reassurance that age assurance methods would work fairly despite, for example, the physical and developmental differences between children of a similar age (that they were often very conscious of). Many did express that they would find it frustrating if they were to be removed from services they had previously been able to access. However, a more consistent access requirement based on age made sense to them.

Circumvention vs. exclusion

During interviews with parents, carers and professionals there was also a view that many children would circumvent age assurance methods once the methodologies were understood. Some respondents immediately expressed that children and young people would circumvent age assurance profiling methods by setting up fake accounts and feigning adult interests or behaviours - whilst sharing what works with peers. This was also stated by some children, who explained how they could get hold of a parent's ID or a credit card if they wanted, take control of their parents' accounts, and use selfies of other older children to circumvent a biometric method. They felt confident that they would go to significant lengths to circumvent an age assurance method.

The above perhaps demonstrates that, even within these more excluded groups of children, there was a wide spectrum of skills, confidence, and capability. There was also a sense that whilst many of these children and young people are less digitally capable or mature than their non-excluded peers, they may be highly motivated to gain access because the online environment is so important to them and one of the few places in their lives where they are included and accepted.

In contrast to this, in our engagement with children and young people with more significant learning difficulties we found that there was uncertainty and hesitancy about the legitimacy of age assurance technologies. The notion of data sharing conflicted with the messaging this group of children had been taught about how to protect themselves online during online safety sessions. A concern about potential self-exclusion was also raised where this group of children may be more likely to withdraw or self-exclude if faced with a process that they are unsure about.

Data privacy and security

For many of those interviewed, it was less the specific methodology that mattered and more about the safeguards that were in place in terms of the security and privacy of the data (and many clearly did not trust platforms). Sometimes respondents would have an initial negative response to the data approach of a particular methodology, but once the methodology was

explored in more detail there tended to be far greater acceptance (e.g. children were more accepting if there were assurances that data, such as a picture for example, would not be kept or shared). Children, young people and parents often wanted assurances about data and the issues of independence, regulation and accountability for any data collected were raised.

Digital exclusion risks for highly vulnerable children

It is worth noting that for the children that are the focus of this study the potential exclusion risk around age assurance technology fits into a much broader set of concerns around how they access and use the internet. Most recently, the digital exclusion of disadvantaged groups has been highlighted and exacerbated by the Covid-19 pandemic which, in necessitating home schooling and online learning for a large part of the year, has been hugely challenging for families with more limited access to devices.[27] For children in care there are longstanding concerns about their more limited access to the online world due to a lack of digital access or support.[28]

For the children interviewed for this research, they shared that their internet access was of particularly strong significance for them - an area of their life where they felt included and connected. This research accords with other recent research which found that while vulnerable children and young people are more at risk online, they are also more reliant on the online world for positive connections and escape[29]. The implications of this go beyond the focus of this study, but there is clearly a concern with this group (many of whom have had adverse childhood experiences) around a propensity to seek risky experiences, and negative attention online. For these children, whilst it is important that they are not unfairly excluded it is also clear that they need broader support in terms of their current internet use. Many within this group need specific interventions and support online that will enable them to enjoy richer online experiences and safer connections.

Legitimate loss of access to online services

Although also outside the specific focus of this report, one of the issues encountered during this research is the potential impact of the legitimate loss of access for children and young people who are underage for a service, when age assurance methods are implemented. In discussing the 13+ age requirements for many social media sites, professionals highlighted that whilst they believe more effective enforcement of minimum age requirements will protect many children from harm and be supportive of their wellbeing in the long run, for some children who have their access removed this could lead to other forms of risky behaviour or result in poor mental health and heightened anxiety. Thought needs to be given to the risks associated with suddenly revoking access to communications and social media for a cohort of children who are currently heavy social media users. To counter this, it is important that there is work with this cohort so that children and young people understand that they are not being singled out and to ensure that they are supported to use age-appropriate alternatives.

One of the points of uncertainty and discussion from many of our respondents has been the extent to which age assurance methods can enable a better internet experience, and not a more restricted or age gated one, or one that displaces children to less safe spaces. One of

[27] Ofcom's survey, *Technology Tracker 2020: households with children access to internet and devices* January - March 2020, found 9% of households with children did not have access to a laptop, desktop, PC or tablet.
[28] *Growing up Digital in Care*, Office of the Children's Commissioner, 2017
[29] *Refuge and Risk Life Online for Vulnerable People*, Internet Matters

the young girls interviewed described the lack of alternatives she had found when coming off her favourite social media service:

> *"I was off Tik-Tok for quite a while because it was quite dangerous and me and my mum were trying to find apps like Tik-Tok, but we could not find any. …. I had to come off* [at eight years old] *because there were random people following me and I didn't know how to put my account on 'private'. So, I came off it for a couple of years and then I went back on it."* Girl 12, (SEN)