DRCF

Digital Regulation Cooperation Forum

Families' attitudes towards age assurance

Research commissioned by the ICO and Ofcom

REVEALING REALITY

Contents

Preface

The Information Commissioner's Office (ICO) is the UK's independent regulator for information rights legislation. This includes the Data Protection Act 2018 and the UK General Data Protection Regulation (UKGDPR). In September 2021, the ICO's Age Appropriate Design Code (AADC or Children's code), a statutory code, came into force. This requires organisations which are offering online services likely to be accessed by children to conform to 15 standards. Standard three of the code sets an expectation that online platforms either establish the age of their users with an appropriate degree of certainty, or apply the standards in the code to all users.

Ofcom has a statutory duty to promote and research media literacy, including in respect of material available on the internet. A key way it seeks to fulfil this duty is through its Making Sense of Media programme, which aims to help improve the online skills, knowledge and understanding of children and adults in the UK. Ofcom was also given powers in autumn 2020 to regulate UK-established video-sharing platforms (VSPs). And in December 2020, the Government confirmed its intention to nominate Ofcom as the regulator for online safety in the UK, under the Online Safety Bill.

The Digital Regulation Cooperation Forum (DRCF) brings together four UK regulators tasked with regulating digital services to collectively drive greater regulatory co-operation and deliver coherent approaches to digital regulation. Through the DRCF workplan for 2022-23, the ICO and Ofcom committed to working together on protecting children online and synchronising their efforts – with a particular focus on improving outcomes for children and parents – by ensuring privacy and online safety protections work in unison. This includes joint research on age assurance, as well as a joint working framework to support the oversight of Ofcom's Video Sharing Platform (VSP) regulatory framework and the ICO's Children's code.

This research will also inform Ofcom's preparations for implementing the new online safety laws, as referenced in Ofcom's Roadmap to Online Safety Regulation. As part of these preparations, Ofcom is building a robust evidence base, bringing together internal and external data, collected using different methods, from a variety of different sources. This programme of research will further develop Ofcom's understanding of online harms and how it can help to promote a safer user experience.

Age Assurance Research

Age assurance refers to a number of measures which would allow organisations to prevent children from accessing services which are inappropriate for their age, and also to tailor services to suit their developmental needs[1].

The role of age assurance in children's use of online services is an area of mutual interest for both the ICO and Ofcom as age assurance products that comply with data protection legislation and meet further online safety objectives will help to deliver a stronger, more positive outcome for children online. Given it is an area where there are interlinking responsibilities, this research has been commissioned to aid coherence between these two bodies and will help to inform policies and guidance in this area.

This research provides an understanding of the attitudes parents and children have about age assurance. The research shows there is parental and child support for the principle of age assurance, but also recognises some methods raise concerns related to privacy, parental control, child autonomy and usability.

The ICO and Ofcom will play close attention to these concerns as they continue to develop and refine their policies.

[1] Age assurance is the broader term which encapsulates age verification and age estimation. Age verification (AV) provides a higher degree of certainty of the age of an individual, as information provided would have to be verified against some form of official identification. Age estimation (AE) is usually dependent on algorithms which provide an estimate of the age of an individual.

There are a number of important considerations when reading this report:

- Where the report refers to **particular services and platforms by name, this is because these were direct examples given by participants about their own experiences and opinions. Nothing in the report referring to any specific services or platforms should be taken as reflecting the ICO or Ofcom's views**. Participants were not directly asked questions about specific platforms; questions were kept broad as participants were only asked about the platforms and services they used, therefore all named platforms were unprompted platform names given by participants.

- The research goes beyond platforms' safety systems and processes to help shed broader light on what people are experiencing online. It therefore touches on issues that are beyond the scope of current data protection legislation and the VSP regime, and the proposed online safety regime.

- The research reflects people's views and experiences of their online world: the families that took part were sampled across a variety of criteria to ensure a diversity of experiences was captured. This included standard demographics, parent and child characteristics, family size and composition, and potential vulnerabilities. For more detailed information on the methodology and sample used in this research see, 'Annex: Methodology and sample detail'.

About Revealing Reality

Revealing Reality is an independent social research agency, working with regulators, government and charities to provide independent and rigorous insight into young people's online behaviours and experiences.

Studying how the digital world is shaping people's lives is something Revealing Reality do every day. The agency has been tracking children's media use and the impact it has on them for the past eight years as part of Ofcom's Children's Media Lives research, alongside conducting detailed qualitative behavioural research on digital behaviours, observing how people really use digital products, services and technology.

Revealing Reality has a strict Ethics and Safeguarding Policy in place to ensure, as far as possible, that taking part in research is a positive experience for children and that they are not placed under any undue risk, stress or discomfort during the project. This policy is reviewed regularly to ensure that it is in line with all industry standards, including those of the Market Research Society and the Government Social Research Service.

Executive summary

This research was commissioned by the ICO and Ofcom to explore parents' and children's attitudes towards potential age assurance methods and provide context for how current methods fit into families' daily behaviour. Age assurance refers to various methods used to estimate or establish a user's age, which can be used to provide an age-appropriate experience online as well as preventing children from accessing adult, harmful, or otherwise inappropriate material.

The research included in-depth interviews with eighteen families, involving media diary tasks, and eight focus groups – four with parents of children of similar ages and four with children in age groups ranging from 13 to 17. For more detailed information on the methodology and sample used in this research see, 'Annex: Methodology and sample detail'.

This report represents the views of research participants obtained through the commissioned research, and not those of the ICO or Ofcom.

Key findings

What do families think about the concept of age assurance?

- **Most parents felt that services should have age assurance measures, but it can sit in tension with their desire for control and flexibility over what their children do online**. Many parents consider not only their child's numerical age, but also their child's maturity and their own perceived risk of the online platform when making decisions about what their children should and should not have access to. These attitudes were common across parents from different socioeconomic backgrounds and household set ups.

- **Parents and children felt age assurance was most appropriate for activities that are more traditionally associated with age restrictions offline.** This included activities such as gambling, watching pornography or buying alcohol. In contrast, many parents saw minimum age limits on social media and games platforms as arbitrary, and not always reflective of what they thought was appropriate for their child.
- **Most children had circumvented current age assurance methods themselves (typically self-declaration on social media platforms) or knew someone who had.** This was typically across social media and gaming platforms and parents were often aware of this, and sometimes facilitated it. An underlying paradox in this research was that researchers were asking parents to consider how they might use age assurance methods to best effect, whilst at the same time acknowledging that currently, their prevailing attitude was not to enforce them, or indeed to encourage their children to circumvent them.

What do families think about different age assurance methods?

Parents and children were introduced to seven different age assurance methods and processes through which age assurance could be undertaken. Researchers used visual prompts, such as written definitions, scenarios, images, to gradually introduce and explain each method. Respondents were prompted to consider age assurance across a range of online activities, including social media, gaming, video sharing platforms and buying age-restricted products.

- **Many families felt the type of platform the age assurance method was being used on was critical context for which method felt the most appropriate.** Families rarely had a clear preference for one method over another as they also acknowledged that there were trade-offs to be made, for example between the effectiveness of a method and the effort required.

- **Parents and children felt that hard identifiers such as a passport or driving licence were the most effective age assurance method** and leaned towards these for traditionally age-restricted activities, such as gambling or accessing pornography, that they felt required "tougher measures."

- **When discussing accessing social media, games and video sharing platforms, children tended to default to self-declaration**, due to the perceived ease of circumvention and desire to be able to access these platforms. **Parents often preferred parental confirmation**, due to the perception of control and flexibility.

- **Both parents and children had concerns about the amount of effort required to use methods** such as hard identifiers and did not want to have to use age assurance methods repeatedly each time they accessed a platform.

- **Some parents and children raised concerns about the amount of data sharing required** in order to age assure using behavioural profiling, hard identifiers, and facial image analysis, but felt that using a secure third-party could mitigate some of these risks.

How do families currently approach parental controls and monitoring?

Families' current approaches to online monitoring and parental controls provide important context for appreciating how age assurance may complement or contradict existing measures parents take.

- **Parents were using a range of methods to oversee their child's online behaviours**. This ranged from checking their child's devices, listening / watching their children use their devices, and using parental control settings on devices or accounts. However, parents often felt that maintaining good communication with their child about their online behaviours was a high priority over other methods.

- **As children get older or are perceived to be more mature, parents' motivation and ability to monitor their online activities or introduce parental controls decreases.** Parents become less motivated to restrict their child's online activities as they get older or as they perceive them to be more mature, while children become more motivated and able to circumvent measures.

- **Children were able to circumvent parental rules or controls in a number of ways**. This included gaining access to their parents' settings or parental control apps, creating new accounts online when parents followed them on social media, and changing their IP address using a VPN to avoid controls on Wi-Fi settings.

Background & methodology

Background to the project

The term 'age assurance' refers to a variety of methods which can be used to verify or estimate an online user's age in order to provide services appropriate to their age. Age assurance can be used to:

- provide assurance that children are not able to access adult, harmful or otherwise inappropriate content while online;
- ensure that added protections are in place for the processing of children's data; and
- estimate or establish the age of a user to tailor services to their needs and put in place appropriate protections for their age.

Various forms of age assurance are already used by many services and platforms, including social media, age-restricted websites, video streaming, and online games. Existing methods of age assurance include self-declaration, verification using hard identifiers such as a passport or driving licence, behavioural profiling, and facial analysis, amongst others.

However, there is currently uncertainty about the accuracy and efficacy of some of these methods, alongside competing considerations such as privacy and user experience. Ongoing development of legislation has also led to some ambiguity for online services and platforms around what methods they should be putting in place.

The ICO is responsible for enforcing compliance with the data protection legislation in the UK, and conformance to the Children's Code, ensuring that services are designed to be age-appropriate and protecting the processing of children's personal data. In autumn 2020, Ofcom was given powers to regulate UK-established video-sharing platforms (VSPs). With the upcoming Online Safety Bill, Ofcom will have new responsibilities for protecting the safety of online platform users.

Both Ofcom and the ICO have an interest in understanding the current landscape of age assurance and how it can be improved for users, and especially children, to ensure they are kept safe from harm and encounter age-appropriate content and experiences online. The ICO and Ofcom are committed to incorporate the voices and experiences of children and parents into age assurance decision-making and policy development.

The ICO and Ofcom therefore commissioned this research to gather insights from both parents and children about current family dynamics and behaviours around online use/safety and attitudes towards current and future age assurance methods.

Research objectives

This research aimed to:

- Explore attitudes towards online safety and age assurance across a mix of parents/guardians and children.
    - Assess the attitudes towards current age assurance approaches amongst different user/household types.
    - Explore the perceived benefits and risks of possible future age assurance solutions.
    - Observe the household dynamics around online safety and age assurance.
- Explore how parents/guardians and children balance the benefits and risks of age assurance across different contexts.
    - Understand how parents/guardians and children balance various considerations (e.g., safety, privacy, usability, convenience and social impact) where age assurance is used by online services.
    - Understand how attitudes towards age assurance, and the balancing of relevant considerations, change depending on the technique used and the context of the online service.

Methodology & approach

This research was conducted from May to August 2022. A mixed method qualitative approach was used to capture both current household contexts and detailed reflections on age assurance techniques. This approach encompassed both investigative and deliberative methods across a diverse range of households to understand age assurance attitudes and experiences, to explore actual behaviours, and to provide space for respondents to reflect in more detail about the range of different age assurance methods and approaches.

Media diaries

This task was used to introduce families to the research and offer to researchers a glimpse into the family and their media life, including the role media plays in the daily life of parents and their children.

Parents and children separately completed a 'media diary' where they recorded their online and offline behaviours in 3-hourly intervals across the day for three days. To accompany the media diary, parents and children were also asked to complete:

- Screen recordings of their normal app use
- A short video introducing themselves and their family
- Photos and screenshots of their online and offline activities

In home interviews

Eighteen in-depth interviews with families were conducted. The in-depth interviews involved spending four hours with each household, including an interview with parents, an interview with the lead child[2] and an hour of unstructured participant observation which enabled the researcher to gain a greater feel for family dynamics and relationships.

Interviews with the child and parent were conducted separately when possible. In each interview, the themes explored included:

- Family life
- Parenting
- Rules and responsibilities
- Children and parent media use
- Media use oversight by parents
- Attitudes and opinions around existing age assurance methods
- Attitudes and opinions toward potential future age assurance technologies

Deliberative focus groups

Focus groups were used to explore reactions to age assurance technologies more deliberatively through the presentation of relevant information and visual stimuli (such as written definitions, scenarios and images) from the group's facilitator. This enabled participants to give informed responses to current and future age assurance concepts.

These groups were designed to further explore the objectives from the household immersions with more explicit focus on the perceived tensions around the concepts of age assurance and individual methods, including privacy and user experience. The respondents in the focus groups were different to those involved in the household interviews and media diaries.

[2] 'Lead child' is the one child in the family taking part in the interview and diary task.

The researchers conducted eight focus groups, four of these with parents grouped by having children of similar ages:

- Three parents / guardians with children aged 8-10
- Five parents / guardians with children aged 11-12
- Four parents / guardians with children aged 13-14
- Four parents / guardians with children aged 15-17

In the other four focus groups, children were grouped by gender and age, and were recruited as pairs of friends. This decision was made based on the importance of children feeling comfortable to talk about what they do online and having some reassurance by being accompanied by a friend.

- Five boys aged 13 and 14
- Six girls aged 13 and 14
- Six boys aged 16 and 17
- Six girls aged 16 and 17[3]

Sample Overview

Within this research, it was vital to include the experiences of a broad range of households. Therefore, both the interviews and focus groups covered a broad spread of household compositions and characteristics.

The sample included a geographical spread across England, Scotland, Wales and Northern Ireland, with a regional spread across England and a mix of urban, suburban and rural locations.

Household composition was a key sampling consideration. Households included both joint and single parents and households with step-parents and step-children, as well as children who split their time between two homes with different parents or guardians. The sample also included a range of child ages and number of children in the household (including only children), and a range of age gaps and birth order between the lead child and siblings.

A number of potential vulnerabilities and a spread of socioeconomic status were also included to ensure a range of experiences were represented in the research. Potential vulnerabilities included financial vulnerabilities and parents and children with mental or physical health conditions.

In addition, the sample included a range of criteria around digital device usage. This included the number of devices owned by the child, the child's primary device and online activities, screen time and level of parental oversight around their online activity.

For more detailed information on the methodology and sample used in this research see, 'Annex: Methodology and sample detail'.

[3] The children's focus groups were grouped in these age brackets to ensure that all respondents were within a small age bracket. The focus was on 13- and 14-year-olds as a group who had recently reached the age for using the most popular social media platforms as permitted by the services' terms and conditions, and 16- and 17-year-olds who were at an age at which they would be beginning to do more independently and could look back retrospectively on their online experiences.

Section 1
What do families think about the concept of age assurance, and why?

This section explores what parents said about the level of control or oversight they wanted to have over their children's online media use, as well as what parents and children thought about the concept of age assurance.

This provides important context for understanding the preferences that families have around age assurance technologies and provides an important backdrop for appreciating how age assurance may complement or contradict existing measures parents take. These preferences, attitudes, and behaviours did not appear to be linked to socioeconomic group or household type, but rather a wider range of factors that will be further discussed in Section 3.

It was important to consider the wider oversight parents wanted to have because, critically, if age assurance methods do not align with such preferences, there is a likelihood that parents will support children in circumventing these methods.

Parents wanted to keep their children safe online, whilst also wanting them to learn how to handle risks independently

There is an ongoing parenting tension between protecting children and allowing them to learn through experience. Parents understood they would not be able to control what their child does forever, and that their child would need to foster resilience and develop the necessary skills to live independently in a world that parents cannot protect them from.

Parents agreed they would like a safer online environment for their children. However, they also want choice and flexibility in the level of control they have over their child's online activities: they want to feel they know what their child is doing, but also to support them in growing into responsible adults.

As children get older or more mature, parents' motivation and ability to monitor their online activities decreases

As will be discussed in later sections, there are tensions between what parents may want in terms of parental oversight and what they are willing to compromise, which changes as their child gets older. As children get older, parents' motivation and ability to restrict their online activities or introduce parental controls decreases, whilst children's motivation and ability to overcome parental rules and controls increases. Crucially, this has implications for age assurance as it shapes parents' desired level of involvement with their child's activities.

Most parents were positive about the concept of age assurance in principle, but it can sit in tension with their desire for control and flexibility

Overall, most parents said they agree with age assurance in principle as a means of preventing children from accessing inappropriate content and coming to harm online. However, when thinking about the implications of age assurance for their own children, some parents disliked the idea of external authorities (e.g. platforms, regulators, government) deciding what was and was not appropriate for children at different ages. They were therefore uncomfortable with these restrictions being enforced with age assurance.

Many parents preferred to have flexibility in what their children could and couldn't access. They wanted to have a role in choosing whether they wanted their child to access certain services and content themselves, which could sit in tension with age assurance measures.

Against this backdrop, age assurance methods could feel like a threat to the sense of control parents have over their children's online media use, as they often assumed these technologies would enforce rigid age restrictions that they may not agree with or feel are inappropriate.

> *"It's like, are you going to let your 13-year-old watch a 15-rated movie? It depends on the content. So most movies yes, but then I've not let her watch Dirty Dancing yet because it's about abortion. I don't even want Izzy knowing what abortion is yet. That's my choice. There should be an override. Maybe the website says you've got to be 15, but sometimes I'll say 'it's okay she's 13, it's fine'"* – **Amy, mother of Isobel (13)**[4]

Parents and children saw age assurance technologies as most important for activities traditionally associated with age restrictions but were less in favour of the idea of age restrictions on social media and gaming

Both parents and children saw age assurance as most important for gambling, online shopping of age restricted items (such as knives, alcohol and tobacco), pornography, and other adult-rated online content. Generally, parents and children saw age assurance as less important for social media, video sharing, and games platforms, even where these might contain age-rated content.

> *"I don't see anything that's going to be in a game that should be restricted to being 18. That's a bit overzealous"* – **Lianne, mother of James (14)**

Parents did not always recognise the potential for online platforms, including social media and gaming, to be harmful. Even among parents who did recognise this harm, it was often felt that restricting a child's access to a platform, although sometimes desired, presented difficulties. They felt it was a challenging decision since it would be unfair to prevent their children from engaging in activities that all their peers were engaging in.

Therefore, most parents did not regard age restrictions and existing age assurance measures on social media and gaming with the same importance as traditionally age-restricted activities. Instead, parents were more likely to circumvent these measures or allow children to access these online activities. For example, some parents were aware that their children had circumvented age assurance methods, such as when signing up for social media platforms. In some cases, parents had facilitated their children circumventing age assurance measures, such as telling them to use an incorrect date of birth. **Karla**, for example, allowed her son Jack (12) to play 18+ rated games, after he received his own games console for his 8th birthday.

Many parents were unaware that age assurance could help platforms tailor content and features based on a child's age, as opposed to simply restricting the child from accessing the platform

When discussing age assurance, parents often assumed that age assurance technologies' principal use would be enforcing a rigid distinction between being allowed on a platform or not, rather than enabling more gradual changes of a child's experience on the platform.

Despite this, where parents had encountered examples of age-appropriate features on platforms, they liked and supported these features. For example, several parents talked positively about YouTube Kids, for which the only issue was that there was not a 'middle ground' as their younger children grew into teenagers for whom the content on YouTube Kids was felt to be too young.

Children seemed slightly more aware of how platforms used their age to tailor the on-platform experience, and many were aware of different features they could access at different ages on the platforms they used. For example, many children who used TikTok talked about features that couldn't be accessed unless the user was

[4] Pseudonyms have been used for parents/guardians and children throughout the report

registered as 16+. However, they seemed less aware that platforms could use their age to tailor the content they saw when introduced to this in focus groups.

> *"I only knew about the livestreams [being restricted], I didn't know about the other things"* – **Focus group, 16-year-old girl**
>
> *"I know about YouTube Kids, but I didn't know about how TikTok changes depending on your age"* – **Focus group, 17-year-old boy**

Many parents were unaware why 13 was an age minimum, and several disagreed with a specific age being used as a blanket minimum

Most parents were aware that the minimum age was 13 for most social media platforms, others assumed there was a minimum age but were not sure what this age was[5].

Those parents who were aware that the minimum age to access most social media platforms was 13 had a range of theories as to why this was the case, but none articulated reasons relating to regulation or legislation. Most parents questioned why 13 was the set age as it did not mirror any other important educational milestones or offline age restrictions (15+ or 18+ movies).

> *"It seems like a strange age, because kids start high school at 11 and they want all the things that 13-year-olds have. So I don't think it makes that much difference...I'm guessing it's based on some kind of research about their brains"* – **Sally, mother of Marcy (16)**

Additionally, a rigid age minimum was seen as relatively arbitrary and did not reflect the differences between the perceived risks that different platforms were associated with.

Lucy, mother of Alex (11)

Lucy thought most social media platforms had a minimum age of 12, apart from WhatsApp which she said had a minimum age of 16. She thought these age minimums were not in line with the potential risks on these platforms. She was very worried about children bullying each other on Snapchat, and the social connections being very tenuous. She was particularly concerned about her son saying things that would upset people online and creating a digital footprint that would affect him in the future.

In relation to her daughter, she was more concerned about content influencing her mental health, particularly social media algorithms presenting pro-anorexia content.

"I know that WhatsApp is 16, and funny enough that's the highest threshold. For me, that's the app that I worry about the least. I think Snapchat, Instagram, TikTok, they're all 12 or 13"

[5] The minimum age limit for the platforms discussed in this report are as follows: Instagram (13), Snapchat (13), Facebook (13), Twitter (13), TikTok (13), YouTube (13), WhatsApp (16). Source: Internet matters

When asked, most parents felt that ultimately it was their responsibility to keep their child safe online

Parents typically saw children's online safety as their – and other parents' – responsibility. While some did express the need for further measures, understandably, it was hard for them to articulate how this might be achieved before they were introduced to the possible future age assurance technologies.

It is important to note that, unsurprisingly, parents tended to want to demonstrate that they were responsible for and attentive of their children's activities. Parents were using a variety of parental controls and techniques around their children's online activities, which will be covered in more detail in section 3. All parents tended to justify the level of control they had as an exercise of parental judgement and responsibility, however what this looked like varied widely across families, and many parents struggled to achieve their own ideals.

> *"I think maybe we need to be a little bit more proactive in checking what the children do online... I think it's probably what a responsible parent should do"* – **Julie, mother of Sam (15)**

For some parents, there was a sense that despite their own best efforts, other parents were too lenient over their children's online activities and were not responsible enough. **Kerry** felt that she was one of few parents she knew who was putting measures in place to stop her son from accessing potentially harmful content or contact online and was disappointed by what she felt was a lack of parental responsibility in other families.

> *"I think a lot of parents don't care, anything for a quiet life, they let their kids do what they want"* – **Kerry, mother of David (14)**

It was common for parents to feel that platforms and the government also held some responsibility for keeping children safe online. The desire for government to be involved often stemmed from a distrust of platforms, and a few parents felt that the government should introduce regulations to hold platforms accountable for protecting children.

> *"It's a mixture, the companies who make the websites, but then the government need to do a bit more to have more impact on their decisions and technologies. All I can control is what I do as a parent, which is to try and make sure my children are only in contact with their friends and people they know, and to be honest without scaring them"* – **Focus group, father of 11-year-old girl**

> *"Ultimately it is the parent's responsibility, but then there are a lot of other factors that feed into that... I also think that the actual social media companies have to take some responsibility too, because I think some of what they're doing to exploit children and they're doing that for profit and they should be thinking more about safety. And then it's the government as well because there should be regulations in place. And then I think the school also has a role to play in educating children about online safety. But I guess ultimately it is parents"* – **Sally, mother of Marcy (16)**

Some reflected that online platforms did not benefit from restricting access to users, and so were unlikely to be designed with children's safety in mind without external intervention.

> *"I'm not so sure it's in the platform's interest to limit the amount of people using it and so wouldn't entirely trust them to do it, or to do it properly. I guess that's where the government has responsibilities to regulate them and put measures in place to make sure companies do provide assurance"* – **Orla, mother of Katie (13)**

A few parents thought that creating legal minimum age restrictions around accessing online platforms and services would help to support parents in protecting children online. They thought that such a law would make parents more likely to comply with age restrictions so that all children of the same age would be exposed to similar platforms and experiences. One mother knew her son had heard of inappropriate content from friends whose parents had let them access age-restricted content, and felt it was a "battle" to follow these rules as a parent given the peer pressure present.

> *"Unless these things [age assurance methods] are made law and parents legally had to do it, if not there are a lot of parents who don't bother. And that's the problem, because we can't control what our children learn because it's coming from friends whose parents let them go on whatever site. That's been the biggest battle we've had"* – **Focus group, mother of 16-year-old boy**

Children often shared similar opinions to their parents but were more likely to suggest that platforms were responsible for the safety of their users

Whilst children often agreed that their parents were responsible for their online activities, they also frequently reflected that platforms held a greater power to protect users online and were therefore also responsible.

Children inferred that, since online platforms provided the medium through which harmful things took place, they had greater responsibility to control what is shared by users. Some children recognised that age assurance – usually talking about age limits for using platforms – may help to reduce the risk of coming into contact with harms online.

For example, in a focus group of 16–17-year-old girls, two respondents discussed ideas about measures platforms could introduce to reduce harm:

> *"There should be more on the app to be able to change your settings. If certain videos may upset you, you should be able to not have those videos in front of you"* – **Focus group, 16-year-old girl**

> *"They should make the rules stronger about each app. More staff to check content that breaks guidelines, and they should stop people who aren't the right age for the app from accessing the app, like needing proof for asking for your birthday to stop young people seeing bad things at a young age"* – **Focus group, 16-year-old girl**

Parents' and children's expectations of different age assurance methods were limited by previous knowledge or experiences of them

When asked about the concept of age assurance, parents and children generally linked it to their previous experiences, which were often with self-declaration. All respondents could think of an occasion where they, their children, or someone they know, would have circumvented these methods, which influenced their feedback on the potential age assurance methods presented to them in this research.

Parents' initial reactions to the effectiveness of age assurance tended to be negative because they immediately associated it with self-declaration

When first discussing age assurance, parents' initial reaction was that current methods are ineffective. This was often because parents immediately associated age assurance with self-declaration as this was the method they were most familiar with and was perceived as being ineffective or "pointless." Many saw self-declaration as a 'tick box' exercise that was easy to get around, and some saw it as a means for platforms to show that they were doing something to check the ages of users.

> *"It's pointless because anyone can say anything. I know on Facebook, if you're 13 they don't let you set up an account, but anyone can just make their age up"* – **Focus group, father of 11-year-old girl**

> "*It's more for the platform's benefit rather than to stop children. If it's easy for the child to get around that question and they want to access it, it's not going to stop them. It's more for the website to provide a disclaimer to say the person answered they're over 18 or the age of the restriction so it's no longer their responsibility"* – **Nikola, mother of Amin (16)**

Most children were aware that there were – in theory – age limits on some of the websites they used but could easily get around these.

> *"I notice it with games, you have to be a certain age to play some of them but most of the time you just put you're older if you're too young"* – **Focus group, 13-year-old boy**

> *"I had a TikTok account when it was Musical.ly, when I was 9 or 10 or something, there was an age restriction I think, but I just put I was older"* – **Focus group, 16-year-old girl**

> *"I'm not really sure there's measures in place, they just ask for your date of birth but then everyone I know just puts 1999 or something"* – **Focus group, 17-year-old boy**

Section summary:

- Parents wanted to keep their children safe online whilst also wanting them to learn independently. As a result, most parents had a desire for flexibility when it came to controlling what their children could do online. Overall, they were generally positive about the broader concept of age assurance, but this can sit in tension with their desire for flexibility.

- Most parents defaulted to saying they should be responsible for keeping their children safe online, although this could have been driven, at least in part, by the understandable desire to show themselves in the research as highly attentive parents.

- Parents and children felt that age assurance was most appropriate for activities that traditionally required age verification, and less appropriate for social media or gaming.

- For parents and children, perceptions of age assurance were shaped by their current knowledge of age assurance methods, particularly self-declaration.

- Critically, if age assurance methods do not align with the type of parental oversight that parents want, there is a risk that parents will support children in circumventing these methods.

Section 2
What do families think about age assurance methods?

This section presents the feedback families gave on each age assurance method introduced to them. This feedback should not be considered in isolation, but rather alongside the background set out above and in section 3. As will be discussed in section 3, the research identified tensions and variations between what families said and how they behave, and so the opinions given when they were asked about different age assurance methods may not always reflect their actions in reality.

The age assurance methods explored during this research were:

Self-declaration: the user states their age or date of birth

Hard identifiers: the submission of official documentation, or a scan of such documentation, such as a credit card, passport, or driving license

Facial image analysis (age estimation): a facial image is analysed by an AI system that has been trained on a database of facial images of known ages

Behavioural profiling and inference (age estimation): the analysis of a user's service usage behaviours and interactions, which are typically automated, to estimate age

Parent / guardian confirmation: a user's age or age range is confirmed by another connected accountholder, for example a parent or guardian, using their account to confirm the ages of their children and their accounts

The research also looked at different processes which could be used to facilitate age assurance but are not methods themselves. It explored:

Third-party age verification: a third-party provider confirms a user's age credential through reference to their database of registered users, who have provided proof of age at another point

Cross-service authentication: the use of an age-assured account with one service to establish an account or access another connected service

Considerations to account for when interpreting the feedback on age assurance methods

Respondents' initial reactions to age assurance methods often changed when they were prompted to think about specific pros and cons of each method

When discussing age assurance methods, researchers gave a brief description of each method. Parents and children were then given the opportunity to share their spontaneous attitudes towards the method, which they were often previously unfamiliar with, before being prompted to think about the potential positives and negatives. Some respondents' opinions of the methods changed once they had a chance to reflect on them during the discussion, which will be highlighted below.

Most parents defaulted to thinking about their own preferences – for themselves and their children – while children defaulted to thinking about other children who were younger than them

Respondents' reactions to age assurance also varied depending on who they were thinking about. For example, opinions could change when parents were prompted to think about how well a method would work for others in society. Meanwhile, children often thought about age assurance in terms of children younger than themselves being protected from harm, rather than something that they would need themselves, or would have been useful when they were younger.

For example, a 14-year-old boy reflected on age assurance being a positive thing in the case that "if you're a 5-year-old on your mum's phone and you see something that scars you for the rest of your life," as it could stop this child from seeing harmful content.

Initially respondents' responses to the different age assurance methods were often theoretical rather than anchored in their actual behaviour

An underlying paradox in this research was that researchers were asking parents to consider how they might use age assurance methods to best effect, whilst at the same time the researchers acknowledged that, currently, their prevailing attitude was not to enforce them or indeed to encourage their children to circumvent them.

Indeed, parents' responses to each age assurance method often differed from their real-life behaviours, which frequently involved *not enforcing current age restrictions* on social media or gaming, and actively supporting their children to *circumvent current age assurance* methods.

Similarly, whilst concerns with privacy were common throughout both interviews and focus groups, these same concerns did not always reflect parents' nor children's current online behaviours. For example, many described concerns with sharing images of their faces to social media companies when asked about facial image analysis, despite regularly uploading photos of themselves on these platforms. Most were also worried about their behaviour being tracked online, while at the same time they were accepting 'all cookies' on all websites. This is known as the 'privacy paradox', which describes the difference between how a person intends to protect their online privacy compared to how they actually behave online.

Given their limited exposure to some of the age assurance methods introduced, parents could only give feedback on the idea or assumption of how each method would work. Therefore, when asked about age assurance methods in focus groups and interviews, parents tended to think of their preferences in an ideal world as they were evaluating each method theoretically, rather than thinking about how they would actually engage with a method if it was implemented in 'real life.'

Using a deliberative approach enabled researchers to introduce information and scenarios which helped respondents to move from thinking theoretically to more realistically about how they would engage with each age assurance method.

Parents and children reflected on the accuracy, effectiveness, effort, and risk associated with different types of age assurance

These four themes of accuracy, effectiveness, effort, and risk were raised by parents and children within the in-depth interviews as important factors to consider around age assurance methods. Researchers probed these themes during the in-depth interviews, and they were later explored more deliberatively in focus groups to understand parents' and children's perceptions of age assurance technologies, both generally and in different scenarios.

- Accuracy: How good is the method at estimating and verifying someone's age?
- Effectiveness: How well does the method work in practice?
- Effort: How much hassle do people have to go through to use this method?
- Risk: How safe and private is someone's information?

Parents' and children's perceptions on these four factors will be presented with a colour code to represent low, medium, and high perceptions. As high accuracy and effectiveness represent positive qualities, these are represented in green, whereas high effort and risk represent negative qualities, and are represented in red.

Perception rating scale:

Self-declaration

All parents had encountered self-declaration before, and all thought it was an ineffective method for age assurance

Parents were familiar with self-declaration and were aware of it being easy to circumvent, therefore they did not think it was an effective method. Many were open about themselves and their children lying about their ages, sometimes to access services and, much more rarely, because of data concerns.

Zack's mum noted it being convenient in certain situations to use an incorrect age:

> *"When setting up the Switches or iPads or anything, I've always put in their birth date but the year as in 2000 so I don't get any pop ups. When I've put their actual date of birth on Nintendo Switch, they kept coming up to me for some kind of authorisation. So to skip all that I default to year 2000 so I don't get any headache, which sounds really bad I know"* – **Zack (10)**

Many felt it was a "pointless" barrier to have in place given the ease of circumventing it. However, a few said it was useful to ensure people were aware of what the age limits were on a given platform.

> *"Children can just put false information, can't they? You don't have to prove anything... my children confessed they made up their ages when setting up TikTok"* – **Cara, mother of Harley (10)**

> *"I don't think it's effective. Maybe the first time you use it you might be honest about it, but then kids learn after that first time and can do it again and then they can just pick any year. I suppose if you're a parent then it at least raises a flag that there could be content that isn't age appropriate"* – **Orla, mother of Katie (13)**

Lionel, focus group, father of a 16-year-old boy

One father of a 16-year-old boy talked about, as a family, not being honest about their dates of birth online. He had told his children to state the actual year they were born but an incorrect day and month, as he did not want their children's information to be available online. **Lionel** admitted that he also allowed his children to select a different year so that they were able to use a platform that blocked them because they were not old enough, and knew many other children were doing this too:

> *"I know Facebook and those type of apps were supposed to be over 13, but anybody under 13 just lies about their age... When my kids were 12 or so, when they started senior school and we started ramping up their phones, there were a couple of platforms they went onto and they put in their fake birthday and actual birth year... and they got blocked because they were not old enough based on the year. We reviewed and discussed it and then changed it to make another account with a different year. All that system does is keep honest people honest"*

Children often sided with self-declaration whilst acknowledging its limited efficacy

Children felt self-declaration was the easiest option for them to use and requiring the least effort. However, they also reflected that it was neither effective nor accurate, and many had either used incorrect ages themselves or were aware of friends doing this.

James talked about his friends easily lying about their age on different platforms. Although James had only just started using Snapchat a few weeks before the interview, he had helped a friend download Snapchat when he was 12, saying he was born in 1822.

> *"You can just have any age, it doesn't really matter, everyone in my school had Snapchat before they were 13"* – **James (14)**

Many children openly admitted to picking a random age or a slightly older age than reality to circumvent age restrictions. In some cases, children chose particular ages as they were aware that this would allow them not only to access the platform, but also to unlock particular age-restricted features once on the platform.

For example, **Rana** used an age of 17 or over when registering on TikTok as she felt that it was easier for under-16s to get banned from TikTok and had been banned herself:

> *"Even though I'm 15 now, I still put for my TikTok that I'm 17 or 18 because they've started to ban you over silly things now. If you're under the age of 16, they ban you even just for showing a bit of skin, so I've put 17 or 18... I've been banned loads and loads, so I have to make fake emails and stuff just so I can get back on TikTok"* – **Rana (15)**

A few children reflected that the design of these features – particularly the scroller – made it easier to select the incorrect age. Importantly, the design of the scroller for selecting an age means that it requires more effort to find and select an accurate age than to scroll to select a random age. The perception of greater ease in selecting a random age over an accurate age could mean that motivation to do so increases.

> "*There's a few things that I just can't be bothered with, or if I predict that it's not going to let me in, I just scroll and put whatever age*" – **Sam (15)**

Despite being aware that the method was ineffective, children tended to prefer it in scenarios where they wanted to use the platforms, because it meant it was easy to access the platforms and content they wanted without parental oversight.

16 and 17-year-old boys in a focus group felt that only self-declaration should be necessary to play a game or engage in anything else apart from gambling or using credit cards to spend money, which they felt should be age assured in a more effective way. They were happy for stronger age assurance methods, which they were less knowledgeable about circumventing, to be implemented for 'riskier' activities. These were often activities they were less likely to be engaging with due to their age and age limitations on these activities, such as gambling or online shopping for age-restricted products.

Similarly, the group of 16 and 17-year-old girls said that methods other than self-declaration were only appropriate for more 'risky' behaviours like gambling, when you need to be old enough to understand what you are doing and what you are getting into.

Parents felt self-declaration was only appropriate when other age checks were also in place

Most parents saw this method as appropriate when used as a starting point which led onto stronger age checks, such as facial recognition, ID checks, or fingerprint checks. Parents also thought self-declaration was appropriate if used on an ongoing basis to confirm it was the same person trying to log in, or for online activities perceived to be less risky (such as social media or video streaming).

> *"It's easy to get around it and lie about their age. It might work better if it's backed up with facial recognition or signing in with fingerprint as a way of verifying age"* – **Kim, mother of Polly (10)**

Hard Identifiers

Hard identifiers were viewed as the most effective method for age assurance and appropriate for more 'risky' situations

Most families considered hard identifiers to be the most effective for age assurance. Parents typically felt this method was more appropriate for traditionally 'risky' and age restricted activities, such as buying alcohol or tobacco. Some felt it would be "too much" to use this method on social media, online films, or video games.

Parents and children overwhelmingly preferred hard identifiers above all other measures for websites featuring pornography and gambling. This contrasted with social media platforms, online gaming, video streaming, private messaging platforms and online shopping where alternative technologies – notably parent/guardian authentication – were supported equally or more than the use of hard identifiers.

Where people did support hard identifiers on social media and other online platforms, they felt it was most acceptable as a one-off at account creation, provided it had the necessary data protection caveats, and when used along with facial recognition to confirm a person's identity.

Many families had reservations about the data sharing risks involved in using hard identifiers

Most families felt hard identifiers would be more effective than self-declaration but had concerns over the information that this involved sharing. This was almost unanimous across the sample – both within the focus groups and interviews – though there was disagreement on whether the data risk outweighed the perceived benefits.

Those families worried about data breaches or identity fraud said they would be reassured if they had to upload the ID to a government website rather than to a company. They were often more comfortable with the use of a government platform as they would have issued the hard identifier and would already be familiar with it, unlike social media companies or other websites who may have more vested interests. Parents across single and non-single households and from low to high socioeconomic backgrounds were worried about data risks, without any specific demographic differences arising.

Some parents thought of alternatives they had seen in other real-life scenarios which did not involve the storing of their information from their ID. For example, the focus group of parents with younger children compared it to showing your ID when buying alcohol or cigarettes, or entering a club, where the staff would look at your date of birth in the moment but would not need to store that information.

> *"How long do they hold it? Or is there an automated thing to verify it and delete it? Are there stops and checks in place for data security?... Nowadays, there's so many bots and systems in place, I'm guessing they can automate all this somehow... They shouldn't need to hold it for a second longer than they have to"* – **Focus group, father of 9- and 12-year-old girls**

Both children and adults felt that sharing the level of information on a passport was not proportionate to an age check in a less risky scenario, where only confirmation of the users' age was perceived to be necessary. A few people made a distinction between a passport and driving licence, feeling that a driving licence was slightly less risky than a passport. For example, the focus group of 16 and 17-year-old girls reflected they would like to have different types of ID to show as proof in different scenarios, depending on how risky that situation was. For example, they talked about using their provisional licence if it was a video game or for social media. One respondent in particular expressed some concerns about what some platforms would do with the information on her passport:

> *"Your passport it's like your whole identity. I wouldn't like to show a picture of my passport"* – **Focus group, 16-year-old girl**

A few parents also brought up the inconvenience for adults accessing 18+ content and said they would feel uneasy about sharing this level of information in such spaces.

Parents also had concerns about the effort that using this method could require

Respondents in focus groups were presented with some scenarios of people in different situations, which prompted them to also reflect on the limitations of this method for elderly people, people with learning difficulties, or people who are digitally excluded. For example, one parent raised concerns about an elderly relative who only uses a desktop and would not be able to use a service if he had to get a photo of his passport on to the computer:

> *"I think of my parents in their 80s – my dad can use the internet, but he doesn't have a smartphone. How does he get a photo from his big camera to the computer? He'd just give up"* – **Orla, mother of Katie (13)**

Some also felt that if this had to be done often it would be a major inconvenience, especially if it required using a passport, which people did not always have easy access to. Overall, families said they would rather have to verify using hard identifiers on a one-off basis rather than multiple times, given the perception of effort required.

Researchers did not speak to anyone in this research who said they did not have any access to hard identifiers themselves, and therefore this was not raised as an issue.

Children viewed hard identifiers to be the most effective method for age assurance, yet still preferred self-declaration for activities they were already engaged in

Children generally thought hard identifiers would be an effective method for most situations as it seemed the most accurate to them and accessible to most people they knew. More generally, children thought it would be difficult to get around this method without having access to their parents' or another adult's passport, although they did still acknowledge that there may be ways to circumvent it. Some children were concerned about having to ask their parents for access to their own passports repeatedly, as well as the risk that parents would refuse to let them use it for certain purposes.

Given the perceived effectiveness of this method, children said they would prefer to use self-declaration for the platforms they already used and wanted to continue to have access to. This was especially true where the activities they were engaged in had age restrictions that they were too young to comply with and would be excluded from. By contrast, they preferred hard identifiers for traditionally risky activities – those that they were not currently able to do – such as gambling or buying age-restricted products.

> *"For most things I think self-identification is okay, but then anything only meant for adults or involving money there should be something else in place. I don't see the point of having to go through so much just to play a game"* – **Focus group, 16-year-old boy**

When discussing a ranking exercise during the focus group session in which respondents selected their preferred methods for different online activities, one 16-year-old girl reflected:

> "*For buying products, I put hard identifiers because you can't buy stuff at a younger age and would need to prove your age for alcohol and knives. Whereas for social media you could be almost the age, it doesn't feel as serious"* – **Focus group, 16-year-old girl**

Parents and children had concerns about sharing images of their passports and other hard identifiers with online platforms and other websites

Parents and children preferred the idea of uploading their ID to only one platform which could verify their age but would not store details of their ID. In general, people did not feel as comfortable with having to provide, for example, their passport to social media companies, as they were not confident these would only be used for the purposes of age assurance.

> *"If it's a major institution I've got no problem with it, but if it's Facebook, no chance"* – **Focus group, father of 12-year-old girl**

Some felt that these measures might be excessive on social media platforms or felt other documents containing less personal information may be more appropriate. Some preferred a driving licence over a passport as they felt this contained less unique information, and others suggested different documents, such as a National Union of Students (NUS) card. A few parents raised concerns about sharing this personal information on certain platforms and suggested using something more "generic":

> *"It's personal to me and it has personal unique ID numbers... They should maybe look to do something more generic rather than having to use your passport or driver's licence"* – **Nubia, mother of Kali (8)**

At the same time, most parents felt like there were certain websites they would not want to provide any type of ID to. This included social media companies and video streaming websites.

> *"If I was wanting to watch a film online and it popped up asking for my passport, I'd be like what?!"* – **Lara, mother of Zack (10)**

> *"Facebook owns so many other social media app companies like WhatsApp and Instagram, and so my concern is that you're producing your ID, which is accessible by all these big [companies] and that worries me"* – **Focus group, father of 12-year-old girl**

Parents thought hard identifiers, whilst not fool proof, were still the most effective method they were shown

Parents felt hard identifiers online could only be as effective as they were in real life – and that fake IDs as well as parents using their IDs on their children's behalf were always possible.

> "*Do you just need to present a photo online? No one's actually checking the physical document? It might not be a genuine document in the first place"* – **Focus group, mother of 9-year-old girl**

Nevertheless, some felt that the steps children had to go through to obtain a fake ID were too cumbersome to create real issues. Generally, parents felt as though it was up to other parents to decide whether to help their child circumvent measures.

This was true in the case of **Jack** (12) who asked his mum to help him set up a social media account to access a Fortnite group. His mum **Karla** didn't fully agree with Jack using social media but agreed to do it if she had access to his account and he only used it for this gaming group. However, when asked to upload an ID to prove Jack was over 13, Karla said she felt a bit relieved and told her son there was nothing else she could do as it would be evident that he was only 12.

Behavioural Profiling

Accuracy		Effort	
Effectiveness		Risk	

Parents and children had multiple concerns around behavioural profiling as a method for age assurance

This was the least popular of the choices with very few parents supporting its use. It was seen as being overly invasive and a breach of online users' privacy. Many parents and children felt the behavioural profiling used on websites was already overbearing and would not want a similar technology being used to detect user's ages online. These concerns mainly stemmed from issues with data privacy and the reliability and accuracy of behavioural profiling as an age assurance method.

Data privacy was a common concern for parents when it came to behavioural profiling

Many parents noted the similarities between this method of age assurance and the behavioural profiling they identified as being for marketing purposes, and recognised that they were already being profiled online. Both parents and children felt that this profiling was already overbearing and uncomfortable. Many parents also

doubted how this technology would work given the amount of data they imagined it would need to estimate a user's age. They remarked on preferring less, not more of this kind of technology, especially when it came to private message analysis.

> *"It's very intrusive, I don't even like the adverts, and now this... It's over the top"* – **Focus group, mother of 12-year-old boy**

> *"At what point is this used? If you're opening an account how long does it track your behaviour to establish your age? If you open an account and say you're 21 how long would it take to establish you're right?"* – **Focus group, mother of 15-year-old girl**

Data privacy was therefore a major concern when it came to the behaviour profiling method of age assurance, especially when it came to exactly what information would be used to determine age, how much information would be gathered, how long this would take, and the general desire for less monitoring of behavioural data rather than more. In terms of how this data was checked, respondents, in general, felt more comfortable with AI instead of human checks if this method were to be used. This was in part due to concerns about data being used inappropriately or for purposes other than age verification.

Both parents and children doubted the reliability and accuracy of behavioural profiling

In addition to this, there were often doubts about behavioural profiling being reliable or accurate and the possibility of easily misestimating user's ages based on their behaviour. This provoked concerns about excluding users from accessing certain platforms/features or being inappropriate for devices which were shared by families.

For example, **Sam**, who is interested in supercars, worried about how behavioural profiling might interpret his age:

> *"For browsing habits, when I'm looking on eBay, I'll be looking at cars, things I can't buy yet, so I don't think it could really judge your age"* – **Sam (15)**

> *"For our family I don't think it would work, for example David is a really slow typer, his spelling age is under 10 years, and he went through a stage recently of watching Alvin and The Chipmunks every morning, which would have made him out to be seven or eight"* – **Kerry, mother of David (14)**

> *"It's not going to get everybody right because not everybody is 'normal', what about neurodiverse people, people with autism or learning disabilities, they want to use things and set up accounts. I can't see how this would work accurately for all sorts of people... I wouldn't want it stopping the service of somebody that was legitimately the right age because they seemed immature"* – **Focus group, mother of 15-year-old girl**

> "*You can't know it's that person's footprint either, you could be using somebody else's device or sharing it"* – **Focus group, mother of 9-year-old boy**

Due to the range of abilities and preferences of the people using online platforms and services, as well as the possibility for multiple family members to use a device, many families were concerned about how reliable and accurate this method would be. Some parents also assumed that children may attempt to act older than their age in order to manipulate the system.

Where behavioural profiling was seen as appropriate was as a 'background check' that did not collect private information on the user

Some felt that behavioural profiling might work well as a way of double-checking age and prompting a more effective method, but not as the principal mechanism for estimating age. Overall, there was a distinction between how people felt about their public posts and private messages being reviewed. Respondents did not usually want their private messages or browsing history to be checked but felt slightly less concerned about public posts as they were choosing to share these publicly.

> *"Your public posts are fine because you're putting them out there for people to see. But with private chats, you're not doing that. You're sending that to what might be one person or a few people and don't want that to go outside of the people that you're talking to"* – **Focus group, 16-year-old girl**

Parent / Guardian Confirmation

Parents liked the concept of parent / guardian confirmation as it gave them control and flexibility

Across focus groups and interviews, parent / guardian confirmation was one of the most popular methods, particularly for parents. This was seen as a method that provided parents with flexibility and created opportunities to communicate with children about what they were doing online, whilst allowing parents to assess what was and was not acceptable for their children. It was particularly appealing for those who disliked the idea of external authorities deciding what was or was not appropriate for their child.

> *"It gives you some comfort and security as a parent and gives you that compromise between controlling your kids' lives and looking out for them"* – **Focus group, father of 12-year-old girl**

A central benefit to this method was its perception as a support to parenting

One of the reasons this method was so popular was that it was seen to support parenting, rather than remove or replace parental choice and responsibility. This links to existing parental oversight methods, by which parents wanted measures to become gradually more flexible so as to build their child's resilience and independence.

Many parents already used similar measures in their parenting, such as through creating their children's gaming or social media accounts with their own details or by using family settings. Nevertheless, they felt that building such checks into creating an account would further strengthen parental oversight. While a potentially beneficial opportunity for discussion and conversation when in moderation, parents did also intuit that this measure would introduce extra effort to both them and their children's online use.

> *"We already do this, but I think it needs to be a stronger thing. When I think of a parent with their first child who signs them up to Snapchat, they haven't a clue. It would make that process of agreeing to it a bit more serious"* – **Lucy, mother of Alex (11)**

> *"I wouldn't mind being notified every time they tried to do something, as long as it would be easy to approve or deny it"* – **Bonnie, mother of Bea (13)**

> *"I wouldn't mind doing it intermittently, but every time they log on would be a bit much"* **– Nubia, mother of Kali (8)**

Whilst this method was preferred in many cases, parents did express reservations around how appropriate this measure would be for certain sites and services that they traditionally associated with 18+ age restrictions, such as gambling, pornography, and the purchase of age-restricted items. In these instances, parents tended to prefer more stringent age assurance technologies.

Similarly, researchers reflected on the risk that relying on parental authentication as the preferred age assurance method could undermine efforts to keep children safe, as not all parents are fully aware of online risks or how online platforms operate.

Despite preferring parent / guardian confirmation over other methods, many parents were unsure how this method would work effectively in practice

At times, parents felt that this method alone was sufficient, given their preference for deciding what, when and how their children engaged with online content. However, several parents were concerned by how effective this method would be at verifying the relationship between parent and child and how accessible it would be for parents. Additionally, for parents who cared for a child whose other parent lived separately to them, there were concerns about how the parent / guardian who would give permissions would be decided.

> *"I'm not sure how this works if they're separated people. I would want some way for both parents to agree on a guardian so it's not just one parent deciding on their own"* – **Focus group, mother of 9-year-old girl**

> *"At first it sounded quite straightforward, but then I was thinking about it in terms of the kids. But as adults having to do it, I'm not sure how that would work, who would verify us?"* – **Focus group, mother of 14-year-old boy**

> *"It seems like you could just get someone else to be your mum and dad, I'm not sure how it would work"* – **Focus group, mother of 9-year-old boy**

Without additional checks in place, parents were concerned that children could easily get around this measure, either by creating a fake email address or account and claiming to be their own parent, or instead using the information of an older friend or another adult.

Some parents who already used family settings on their devices were aware of the limitations of these technologies. The uses of scenarios with people in different situations also prompted some concern about children in care being excluded from online activities entirely with this method. Nevertheless, they supported this technology being incorporated where children might attempt to set up online accounts, particularly if it also allowed them greater oversight of their children's account settings.

Many children also thought parent / guardian confirmation was an appropriate measure, since their parents 'knew best'

When children were presented with this option, they also thought it was appropriate since they thought their parents knew what was most appropriate for them. However, children worried that given the different rules their friends' parents had around online media use, they may be excluded from some online activities their peers were taking part in. Echoing the tensions mentioned in section 3 below, children's opinions on this method did not always align to their behaviours, as many were circumventing current parental controls their parents already had in place.

Families thought this method would be most appropriate for sign-ups and downloads

Parents and children thought this method would work best during the sign-up or download of a service or platform. This could include online activities such as social media, video streaming, and videos games where parents already had some flexibility in their oversight. Parent/guardian confirmation was seen as less appropriate for traditionally age-restricted services/items which parents felt were inappropriate for children.

Facial Image Analysis

Both parents and children had doubts about how effective facial image analysis was as an age assurance method

Both parents and children expressed doubt about how effective this technology would be in ensuring the face being shown was from the person wanting to use the platform, and not someone older.

Parents and children thought using facial image analysis would be inaccurate for estimating someone's age and this risk was particularly true across the age groups where the purpose of establishing age was most important. For instance, several children referred to friends who looked much older than their age, or to others who had a "baby face"

> *"I don't think it would prevent young people. I know friends that had like fully grown beards in year 8, they could pretty much access almost everything when they'd only be 13 years old"* – **Focus group, 16-year-old boy**

Parents expressed similar concerns, adding that the appearance of teenagers can vary widely given differences in the age of puberty and development, and it would be much harder to identify differences between, for example,

a 15-year-old and a 16-year-old. They also thought that it could be inconvenient for certain adults who might be regularly mis-aged by this technology.

> *"I'm not sure how effective it would be at the younger years, people's faces change very quickly, far quicker than ours"* – **Focus group, father of 16-year-old girl**

> *"At work some people look younger than their age and they'd be pretty annoyed about it"* – **Orla, mother of Katie (13)**

Parents felt this technology would have to be very accurate for it to be worthwhile. They thought this method could only be as reliable as, if not less than, humans who may judge their age in supermarkets.

Parents were familiar with facial recognition technology, but were doubtful of a method based on inference

Whilst many were familiar with using biometric face scans to unlock their devices, this did not necessarily add to their confidence around facial image analysis technology given that the former worked on recognition whilst the latter had to make an inference about a person's age. Because of this, most felt this technology would be ineffective in isolation. Many suggested it should be coupled with an official document containing a person's image that verified their identity, and some assumed it would work this way as they had experienced similar processes when registering with banks or the NHS, for example.

> "*How do they know that the person using the facial recognition is the person that it's supposed to be. I could get my mate Dave; he looks 20 years older than me. If you can prevent that, great, if not then it's useless ultimately, isn't it? It would only be any good if you could verify it against hard identification"* – **Focus group, father of 10-year-old boy**

Families suggested a number of ways in which this method could be circumvented

Whilst doubts about the accuracy of facial image analysis in determining someone's age dominated, there were additional concerns amongst parents and children relating to both the efficacy of its use and the information they would be sharing. Both parents and children noted how easy they thought it would be to use someone else's face or photographs/videos taken online of older individuals to access online services or items. For this reason, it was felt that a live video was the most effective form of media to use.

> "*My kids could just stick the phone in front of my face, and 'right there you go', there'd be no time for me to process what I'd be consenting to"* – **Focus group, father of 11-year-old girl**

> "*I think in isolation it's quite risky. You could just hold the screen up against a photo of your mum and it would go 'yeah, she's definitely old'"* – **Amy, mother of Imogen (13)**

> *"If you have to move your face and it's a video it would be better than a picture of yourself. You can get a picture in internet very easily"* **– Focus group, 16-year-old girl**

The idea of sharing facial photos caused discomfort for some parents and children

Some parents and children felt uneasy about having to share their face with a website. While a few parents changed their minds after reflecting upon their child's existing online presence, many remained uncomfortable with sharing photos of their child's face online. In comparison to using hard-identifiers, however, parents were generally less concerned with data sharing when it came to facial image analysis.

> "*Websites having a photo of my child's face, that would make me feel a bit awkward, I guess if it was a credible site then perhaps I wouldn't feel so uncomfortable about that*" **– Focus group, mother of 11-year-old twin boys**

> *"I would feel a bit uncomfortable that sites would know more about you – whether you're a boy, girl, person of colour…"* – **Lara, mother of Zack (10)**

> *"I don't suppose I'd be too comfortable with this for Polly. But at the same time, we post pictures of her on Facebook."* **– Kim, mother of Polly (10)**

> "*If you show your passport there's your date of birth, your full name, all this other information. If it's just a face, that would be less risky"* – **Focus group, mother of 11-year-old girl**

"It doesn't bother me so much. You can already see my face, there's photos of me on the internet anyway, and if I was in a shop or a bar to be ID'd they'd see your face, so it's just the online version" – **Amy, mother of Imogen (13)**

Finally, some adults expressed concern about having to use an image of their face in order to access websites hosting adult-content, where they were eligible to do so, and felt uneasy about how their online activities could be associated with their identity.

Much like parent/guardian confirmation, facial image analysis was felt to be most appropriate for 'low risk' online settings

Most families felt facial image analysis was more appropriate on online platforms where age sensitivity was viewed as less significant, for example some parents mentioned they thought it might be appropriate for YouTube, Netflix and some social media platforms. It was, however, felt to be inadequate for activities perceived as being inappropriate for children if not used alongside a photo identification check or parental authentication.

Processes that can be used to facilitate age assurance: Third-party verification

In general, parents felt that their concerns around data sharing risks could be minimised by using a secure third-party

Many families expressed a preference for a third-party platform to verify their age and be used as "evidence" when trying to do other age restricted activities. People liked the idea of being able to confirm their age on several platforms by reusing the verification they received from the third-party provider.

"I like the security of that, you don't have to take a risk with loads of websites but just one that has to gain your trust, which is perhaps partly government funded. You could give Instagram, Facebook and TikTok permission to check it and they're maybe viewing it but they're not holding your data, so it would reduce the number of places that your personal data is held. I like this" – **Lucy, mother of Alex (11)**

Parents and children assumed this method would not need to store a person's data, instead it would simply use ID to initially register the user as over18 and then delete the data. Therefore, parents assumed third-party platforms were safer, quicker, and easier, and it would meet their preference of only having to verify their and their child's age once, rather than providing a hard identifier to multiple online platforms or websites.

"I'm not sure how comfortable I would be holding up a passport containing passport numbers, but a government gateway with a one-off authentication of some description, like when you're doing your tax returns online. You do the age verification thing once with that online service and all the other companies sign up for that. If you have to do an age verification for everything that's going to be a bit of a pain" – **Focus group, father of 15-year-old boy**

However, parents did not initially think about how long it might take to initially verify a person's age with a third party. When prompted about this, they were still happier with verifying once, as they felt this would still save them time over having to provide a hard identifier to multiple websites.

"*I think it's a good idea, obviously it's more efficient, not having to do it on every website"* – **Focus group, father of 9-year-old girl**

Security of data was a common concern related to this method

Some general concerns amongst parents included how this would operate, how the third party would make money or be funded, and how secure it would be.

"I don't know if I'd prefer a private company or the government or government agency. Probably the latter, I think with the Covid passports in Northern Ireland, I was happy to add my identity to that because it was a government website. I suppose with a private company you might be a little more suspicious, what might they be doing with your data?" – **Orla, mother of Katie (13)**

> *"If it's not a paid app then you have to question where the apps are getting their money from. The only way is by selling your data"* – **Focus group, father of 17-year-old boy**

A few respondents saw a third-party organisation as an easy target for data breaches or being hacked. When thinking about what would make parents trust a third-party platform, they talked about having a good reputation, being a well-known company, knowing other people using it and, most preferably, if it was from the government as they already hold large datasets of personal information.

> *"I guess this would be a government led thing? So the information would be retained by a trustworthy recipient and then the platform doesn't have visibility? If so, that wouldn't worry me, that seems quite secure to me"* – **Focus group, mother of 13-year-old girl**

> *"As long as they're held to account then companies could compete with each other to provide the best and quickest service to provide better solutions to the end users like us"* – **Focus group, father of 9-year-old girl**

Cross-service authentication

Cross-service authentication is a way to allow users to declare or verify their age through an age-assured account with one service. They can then use this account to access other services without needing to age-assure again. An example of this would be using an Apple ID for app downloads. Most families were aware of cross-service authentication, and some had occasionally used it across social media platforms. Children mostly related this option to creating an account on different sites using their existing email account as it was quicker. Most children could remember seeing this option but did not understand much how it worked and what impact it had on their information.

A few parents said they never selected this option as they were using platforms for different purposes, and they did not want their information to be "added up" to build a more detailed profile of themselves. For example, they did not want their Instagram to be connected to their LinkedIn.

In summary, parents did not want to use this as they did not want their information to be cross-referenced but they could see the convenience of this process.

For example, **Omar** had logged into other websites with his Google account and could now log in without inserting his password, but felt uneasy as he could not recall when he had approved this:

> *"I've done this with Google without really fully understanding it... I must have logged in somewhere once where I verified with Google, and then it came up saying 'sign in with Google' and it just logged me in and didn't ask for a password... The reason I didn't like it is that I can't remember where or when the first time was when I had to put in my password"* – **Omar, father of Rana (15)**

A few parents considered the effectiveness of the initial age assurance method used when it came to thinking about their children using this method.

> *"Regarding the kids, I suppose it depends on how strict, how rigorous the standards are for the one, then if it is quite rigorous then that would transfer to another and that would be OK"* – **Julie, mother of Sam (15)**

Age Assurance methods comparison

The table below shows a high-level comparison of what parents and children thought of the different age assurance methods explored in interviews and focus groups.

	Self-declaration	**Hard Identifiers**	**Behavioural Profiling**	**Parent/Guardian confirmation**	**Facial Image Analysis**
Overview of perceptions	Accuracy Effort Effectiveness Risk	Accuracy Effort Effectiveness Risk	Accuracy Effort Effectiveness Risk	Accuracy Effort Effectiveness Risk	Accuracy Effort Effectiveness Risk
When is it appropriate?	When used as a 'starting point' which is then verified by stronger age checks such as facial recognition, ID checks or fingerprint. If used on an ongoing basis to confirm it was the same person trying to log in, or for online activities perceived to be less risky (such as social media or video streaming).	For traditionally 'risky' and age restricted activities, for example where spending money is involved, and when used along with facial recognition to confirm a person's identity. Appropriate for situations where offline hard identifiers were required, like purchasing tobacco and gambling.	More appropriate as a secondary 'background check' on some online websites, such as video platforms, gaming and social media. Inappropriate as the principal mechanism for estimating age due to not being perceived as accurate enough.	Most appropriate at service sign-up or download. Most appropriate for social media, video streaming and video games where parents already used flexibility in their oversight. Less appropriate for traditionally age-restricted services/items that parents felt were always inappropriate for children and did not require their judgement.	More appropriate on online platforms where age sensitivity was viewed as less significant, such as streaming platforms, and for some, social media platforms. Inappropriate for activities perceived as being inappropriate for children if not used alongside a photo identification check.

How did people think about circumventing it?	Parents using their own date of birth when creating their child's accounts (was done intentionally by some parents). Randomly selecting a date of birth or changing the year of birth to give an age that is older than the age of the child.	Using someone else's passport or a fake ID to get around this age assurance method.	Children may attempt to act older than their age to manipulate the system.	Children using separate accounts or email addresses to confirm their own activities online. Children gaining confirmation from an older friend or contact who pretends to be their parent/guardian.	Using the face of an older friend or relative. Using images or videos from the internet or from other media.
Concerns raised by parents and children	Self-declaration was ineffective or "pointless" because of the ease for children to say they were older than they were. Adults could pretend they were younger than they were and gain access to platforms that were meant to be child only spaces, or interact with other child users more easily. Data privacy when their date of birth was given alongside other information about themselves.	Could feel invasive due to the amount of information on a passport (e.g., address). Inconvenience for adults accessing 18+ content who feel uneasy about sharing this information in a taboo space. Elderly or less digitally active people may not be able to access the technology required to upload or scan hard identifiers. This could limit them from engaging with certain content, unless alternative options or support was provided to upload hard identifiers.	The data being collected would be used for purposes other than age assurance. Private or personal information may be collected if all online activities were tracked. User's online behaviours may not necessarily reflect their age. There is a risk that people are incorrectly profiled and therefore their experience is inappropriately tailored.	It could create tensions in families where children had separated parents, if different parents had different rules about what they were happy to let the child have access to. These measures might exclude children in care from online activities if their guardians were not available or happy to confirm their ages. Friends' parents could be more liberal with permissions than others and children could be left out. Where parents and children share devices, some thought it would be easy for children to give themselves permission.	The technology would not accurately infer user's ages, particularly younger users. It would create a lot of hassle for adults who appeared younger than their age. It would not work effectively without being used alongside a hard identifier verifying the image-takers identity. Sharing images of oneself or one's children felt intrusive, even if this was less so than for other age assurance technologies discussed.

Questions	No questions were raised about self-declaration as it was something they were familiar with.	How would it work for those without ID? Would they be able to use different types of ID that felt less risky (e.g. driving license, birth certificate)? What information will be stored and how long will the data be stored for? How will the data be kept secure? How would using a hard ID on a one-off basis work? What would they then use on different occasions?	What information would it collect? How else would this information be used? What kind of behaviours is it using to estimate age? Is it a human reviewing the data or AI? (Note: if it was an AI reviewing the data, people felt more comfortable due to not being 'judged' by someone and the perceived risk of someone using that data for nefarious reasons being lower)	How would the technology establish a relationship between children and their parents/guardians? How would this work for children whose parents are separated and may have different opinions on what is appropriate for their child? How would this work for adults for whom asking permission from their parents seems inappropriate?	Would you need to use photo ID as well for this to work? How accurate is the technology? What do you do if it infers the wrong age?

Summary of overarching attitudes towards age assurance methods:

- Most parents said they would rather invest time in using a more effective method at the start than having to repeatedly use a less effective method at multiple touchpoints.
- Generally, parents felt that the effort required for an age assurance method should be proportionate to their perception of potential risks.
- The ideal age assurance method seemed to be a combination of methods that were stronger when first signing up for or accessing a platform, or setting up a device, and which they did not have to do on an ongoing basis. Parents felt a combination of using a hard identifier followed by facial image analysis for verification would be effective.
- Parents' current behaviour showed that they were sometimes helping their children to circumvent measures, and so it can be expected that a good proportion of parents may continue to do this.
- Parents were specifically helping their children to circumvent measures for activities deemed to be less 'risky', such as social media and gaming, as they do not currently see the rigid age restrictions here as meaningful, compared to more traditional age restrictions, such as gambling and pornography.

Summary of attitudes towards individual age assurance methods:

- Parents and children both perceived **hard identifiers** to be the most effective method for protecting children online, and this was their preference for traditionally 'risky' activities.
- However, children preferred **self-declaration** for sites they wanted to access or were already using, as they saw it as easy to circumvent.
- Both parents and children had concerns about sharing the information contained within hard identifiers with platforms and were more confident if a secure **third party** processed these.
- Parents and children had doubts about how effective **facial image analysis** would be, and some felt uncomfortable with the idea of their faces being used in this way.
- **Behavioural profiling** was unpopular due to perceived inaccuracy. Some had concerns about data privacy risks, which were not perceived to be "worth the risk" given the perception of low accuracy.
- **Parent / guardian confirmation** was liked by parents as a method that gave them the most control and flexibility. However, some had concerns about how it could work in practice and the ease of circumventing it.

Section 3
How do families currently approach parental controls and monitoring?

This section covers the current approaches parents are taking to try and keep their children safe online, and the reasons behind these.

This provides further context for understanding families' feedback around age assurance methods, which were informed by the oversight and control measures parents already had in place.

Most parents maintain flexibility when it comes to overseeing their child's online activities

Parental oversight often came with room for conversation and negotiation, recognising that they will not always be able to "have control" over what their children see and do online. Therefore, many families were using communication and compromise as important components in their decision-making.

Parents preferred to talk to their children about issues as they arose and to use these as opportunities for them to learn and grow. This reflected parents' approaches to other restrictions, such as flexibility around watching films with age classifications together as a family or being given small amounts of money to manage.

Because of this preference for gradually introducing children to different experiences, rigid age restrictions often did not feel appropriate. As explained below, a child's age was not the only factor at play when parents decided what their child should and should not have access to but also the child's maturity, and the parent's perceptions of risk on the platform among other considerations. As such, parents preferred to use their own judgement to determine what was or was not appropriate for their child within the limits they were able to control.

Parents' current use of monitoring techniques include either measures on their devices or wider relationship-based measures

Parents used a wide range of oversight methods for their child's online activities, ranging from apps and rules to investment in open communication.

Communicating with the child	Listening/watching children use their devices	Changing settings on devices or accounts	Checking the child's devices
Asking their child about their online life and activities	Being friends with or following their child on social media to observe what they are posting	Using parental control apps or settings	Checking devices as an agreement when the child got the device
Making themselves 'open' for their child to approach them and trusting their child will talk to them if they have problems	Being in the same room their child is using a device in or leaving doors open so parents can hear who their child is talking to	Parents helping to set-up their child's accounts, privacy settings and the age at which they are registered	Checking devices without their child knowing

	Observing mood and behaviour changes after using online devices	Using the parent's email address when signing up to provide oversight of activity/permissions	

Examples of parents using these oversight methods include:

Communicating with the child

> *"I think it's about knowing your child and about making sure that the lines of communication are open and they feel like they can talk"* – **Lianne, mother of James (14)**

Nikola, mother of Amin (16)

Nikola used to have parental controls on their Wi-Fi system. As her 16-year-old son Amin got older, she felt that he had become more mature and trusted him to use the internet without these restrictions in place, even if this meant accepting she had less knowledge or control over his activities.

"I would love to think that I know things based on observation, seeing what he's doing and the platforms he's chatting to people on and what he uses with me, but not everything. I'm not checking his phone deliberately like I used to before... when they were younger, I would definitely check in and see a lot more because they used to play in our communal areas rather than in their own room but now they spend time in their own rooms"

Listening / watching children use their devices

> *"My parents and sister follow me on everything. When I was like 13 or 14 I sometimes hid them from my Instagram story or something. But now I'm almost 17 so I don't hide them from anything anymore and they see everything I post and it doesn't bother me too much"* – **Marcy (16)**

> *"If he has a dip in mood or is being really quiet and withdrawn; I've noticed he's been on his phone and I've asked, 'has anybody said something horrible or have you seen something that's upset you?"* – **Julie, mother of Sam (15)**

10-year-old **Polly**'s parents could hear her use the Xbox in her room and felt that they would notice if she was experiencing anything negative or having conversations with or disclosing information to strangers. Polly often used her phone and tablet in the family living room, which also meant her parents could keep watch over her online activities.

Changing settings on devices or accounts

Many parents in the sample were using parental control apps to monitor and restrict their children's online behaviour. These had functionalities relating to the content children could access, the time they could spend on their devices and location tracking. For example, parents were able to restrict access to websites and apps, require parental permission to visit or download websites and apps, view and set limits on screen time, view their child's search history, block certain content and search terms, and track their child's device location.

Parents using parental control apps

Karla was using a parental control app to monitor her 12-year-old son and 8-year-old daughter. Karla generally used this software to monitor the apps they were downloading and required her son to gain permission should he wish to download additional apps. Karla also liked the feature of tracking his location whenever he was going out. She did not know she could check the amount of time her 12-year-old son **Jack** spends online and on different platforms but discovered this during the interview.

Omar was using a different parental control app, which involved both him and his daughter **Rana** having the app on their mobile phones. He used this app to monitor his daughter's online activity, restricting what she could search and setting notifications for when she tried to search for restricted content.

"Once you put that app on a phone, it goes into the background so she can't see it or delete it. It tells you what she's searching, what social media apps she's using, how long she's using for, and then you can actually put time limits on" –

Omar, father of Rana (15)

Parents using their own details when creating their child's accounts

Amy, the mother of **Imogen** (13), allowed her daughter to set up social media accounts with her friend in the month prior to her 13th birthday. Once Imogen had done so, Amy checked to make sure her settings were at the highest privacy settings possible, and that her registered age – though inaccurate – was registered at the age of a 13-year-old and not an adult.

10-year-old **Harley's** father, **Steve**, used his own email address and created a password Harley did not know when setting up Harley's gaming account. Steve could then check on who Harley was befriending and messaging online, and then ensure Harley knew these contacts in real life. In addition to this, by setting his own password on this account, Harley was unable to download games or make in-game purchases without first asking his dad for permission. Steve used the same strategy across Harley's other gaming accounts, which meant he could ensure Harley's age was registered in such a way that prevented him from communicating with strangers in-game.

Checking the child's devices

"From the moment they got their phone they know I could ask to have access it whenever I wanted to. I don't [check his phone] as much as I used to because I don't have to. But if he's in a negative mood I will check what they've been looking at" – **Focus group, mother of 14-year-old boy**

"I do take the opportunity to check their phones, I don't want to create a big deal out of it, it's just a welfare check, I don't want to make them feel bad" – **Lucy, mother of Alex (11)**

"I check his phone twice a week maybe. I'll go down through Snapchat, through his history and everything... He doesn't know" – **Karla, mother of Jack (12)**

Parents had a higher level of oversight when they were more aware of the potential risks of being online

Parents often raised contact by adult strangers online as a concern, and to a lesser extent, the content their child could come across

The most notable concern for parents was strangers, particularly adults, interacting with or attempting to befriend their children online. There were concerns about adults pretending to be younger than they were, and/or manipulating children by pretending they were the same age in order to befriend them online. For many parents, oversight of their children's online use was intended to ensure they were only interacting with people they already knew.

> *"Safety in general. I know that now at school they teach kids about online safety. But in general you hear people would be contacted online or that kind of thing, then just when you hear those stories, you just worry that will happen to your own child"* – **Focus group, mother of 11-year-old girl**

Kim, mother to **Polly** was concerned about adult strangers attempting to join games with children online:

> *"The people that come into parties and try to join games, you know that they're not children, you can tell by the way they talk that they're not children. But the kids don't get that conversation. They don't sit there and think, 'I'm talking to a grown up here'"* – **Kim, mother of Polly (10)**

In general, parents had some concerns around content considered to be age-inappropriate or harmful. This concern often included accidental exposure to content (such as when scrolling through social media platforms) or being sent or shown content by friends. Parents were particularly concerned about their children seeing sexually explicit content as well as violent content and swear words.

A few parents were more worried about their child being bullied or intimidated online, such as in group chats, or having negatives posts being made about them.

The child's gender, previous negative experiences and parental understanding of platforms were the most influential factors on parents' perceptions of risks

Across the sample, there were a range of differences in household types and socioeconomic backgrounds. This included the child's birth order in the family (youngest, middle child, oldest), whether the household was single or co-parent and the socioeconomic conditions of the household. However, there was no clear relationship between these differences and how families perceived online risks. Instead, the factors that played the largest role in parents determining how risk was perceived were as follows: gender of the child, previous negative experiences online, and parental understanding of how platforms operate.

Gender

One of the most common differences in risk perceptions was linked to the gender of the child. In general, parents were more concerned about the risks that their daughters may experience, whilst sons were seen as generally being less at risk online.

Parents' concerns about girls being online were mainly focused on body image and exposure to images and videos that may negatively shape their self-perception. Some parents were concerned about their daughters gaining unwanted negative attention from others online, for example, sexual attention.

Though parents were less concerned about the risks their sons might encounter online, they were still often worried about their sons' behaviour online, for example, spending lots of time gaming or being exposed to sexual and/or violent content.

Previous negative experiences

Parents often did not think about online spaces being risky until something happened either to their child, to someone they knew, to themselves whilst growing up, or after reading about cases in the press. Parents frequently did not have restrictions until they became aware of a risk as a result of a negative situation.

For example, **Bonnie** took away her daughter **Ella's** (10) mobile phone after an incident where playing an online game introduced Ella to an older male; their conversation moved to a different social media platform where the user shared inappropriate messages with Ella. . Bonnie previously trusted her children to tell her if they saw anything that upset them online. As a result, Bonnie gave Ella a watch that only allows her to make calls to approved contacts and tracks her location.

Understanding of platforms

Parents' knowledge and understanding of the online platforms their children used played an important role in their perceptions of risks online. Across the sample, most parents were aware of the platforms their child was using but did not always understand the features or things their child could do on different platforms. This included aspects such as age restrictions, if you were recommended content, how they could contact other users, or the content they could engage with. When some parents found out what their child saw, they became concerned about their child using these platforms.

"I don't know how the algorithm works, it's so random… you see silly dances, people doing inappropriate things. I just don't think it's age appropriate for young children to be watching" – **Nubia, mother of Kali (8)**

"They were on TikTok, I didn't know what it was, and then [daughter, 8] came in, saying she saw something she didn't like. So we did get rid of those… I thought it was just kids' stuff" – **Cara, mother of Harley (10)**

Some parents based their understanding of platforms on their own experience and what was common for their age, rather than what was more common to children.

"Instagram is fine because it's just a picture sharing site. But maybe I let them make me think everything is fine on there…" – **Bonnie, mother of Bea (13)**

"Zack has Snapchat and TikTok but I haven't let him have Facebook because that's the 'big one' of social media" – **Lara, mother of Zack (10)**

Some parents had limited knowledge of the minimum age restrictions of platforms – some thought they knew but were incorrect or could only guess an age range. **Leela**, **Rishi's** (17) mother, admitted she was not sure what age restrictions social media platforms had and assumed it was for children over 16-years-old.

These perceptions and partial understandings about the potential risk of a platform meant that some parents were happy to set up children's accounts using their own information – including their age. Parents were often unaware that that online platforms may be tailoring content based on the age provided or giving them access to certain features only accessible to adults.

When parents were prompted to think about this in interviews, some expressed concern at the potential implications of giving a platform a false age for their child, and therefore being treated as an adult user, such as Lucy:

"I think I set his TikTok up with my email address, it probably has my age on it too. That's actually a problem isn't it? The algorithm might be treating him like a 42-year-old. That's food for thought" – **Lucy, mother of Alex (11)**

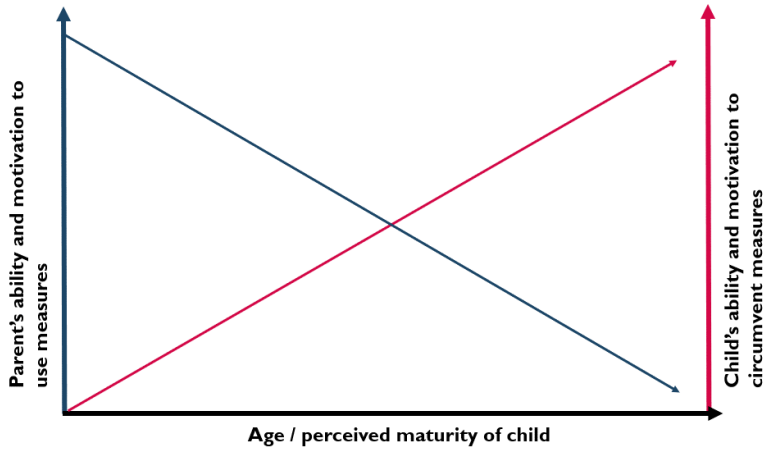
Tensions exist between attitudes towards age assurance methods and the real-world practicalities of parenting

As introduced in the first section, parents and children were displaying behaviours around online safety that could be at odds with more inflexible age assurance methods.

Whilst parents wanted their child's experience online to be safe, in practice they gave children opportunities to take risks depending on perceptions of their maturity. In this way, parents hoped to encourage positive and open relationships with their children that would help them grow independent, resilient, and responsible with age. Parents tended to prioritise communication, negotiation, and flexibility in the kind of activities their children were currently taking part in online, over rigid or more strict parental controls.

There are tensions between what parents may want in terms of parental controls, and what they are willing to compromise on if it means that they will have a better relationship with their child or maintain other restrictions that they see as more important.

This tension changes as children get older, with implications for age assurance in terms of how it shapes parents' desired level of involvement in their child's activities. The graph below is an illustration of how a parent's motivation to restrict their child's online activities decreases as the child gets older or is perceived to be more mature, while the child's ability to circumvent measures increases.



As children get older or are perceived to be more mature, parents' motivation and ability to restrict their online activities or introduce parental controls decreases

As children's social lives become increasingly mediated online, parents did not want their children to be left out of online activities their peers are allowed to take part in. Parents also did not feel there was as much risk for older children compared to when they were younger, as they become more responsible and mature as they grow up.

Parents expressed that it takes more effort to set up and maintain controls that children cannot circumvent as their children's technological know-how increased with age. Having strict controls could also create tensions and arguments between parents and children. Given the importance of trust in parent-child relationships as the children get older, parents preferred to avoid arguments and to 'pick their battles' in order to avoid damaging the relationship they had with their child.

Meanwhile, children's motivation and ability to overcome parental rules increases as they get older

As children grow up, they become more curious about what's happening online and want to be more involved in online communities and activities. Children also become increasingly savvy online and better able to get around parental restrictions, such as downloading VPNs or setting up secret accounts.

Children want greater independence from their parents and become more concerned about keeping their online lives, including their social interactions, private from their parents. Along the lines of social interactions, children also begin receiving more peer pressure to be doing the same things as their friends.

Children were able to circumvent parental rules and controls by:

1. **Gaining access to parental accounts, settings or parental control apps** – this often included children using their parents' devices to give themselves permission to do activities on parental control apps.

There were several examples of children who found ways to avoid or circumvent their parents' oversight of their online activities by using their parents' devices or information to set their own permissions.

For example, 12-year-old **Jack** had figured out his mum, **Karla's**, password for his online gaming account after she had entered it in front of him. He remembered it and would routinely use it himself to download games without her permission.

Other children would use their parents' devices when they were not looking to override the limits that they had set using parental control apps. For instance, one 16-year-old girl from the focus groups, **Laura**, would use her parents' tablet to override the screen limits they had set on their parental control app.

Similarly, when 14-year-old **David's** mum, **Kerry,** had been away from her phone, he took the opportunity to copy down the access code he required from a parental control app to download new applications and mobile games on his phone.

2. **Creating new accounts online to avoid surveillance** – such as when parents followed them on social media.

15-year-old **Rana** had agreed with her dad, **Omar**, that he would no longer use parental control apps so long as he was able to keep an eye on her online activities by befriending her on the social media platforms she used. Despite this, Rana created additional accounts that her father was unaware of. Eventually Omar realised this was happening through word of mouth from other family members but accepted there were limits to what he could control.

3. **Changing their IP address to avoid controls on their Wi-Fi settings.**

One mum of a 17-year-old boy, **Jordan**, from the focus groups had a number of family settings and controls in place, including parental controls on their home network. Jordan had set up a VPN to get around these controls. Though his mother was aware of this, Jordan suggested that there was little she could do.

Similarly, **Rishi** (17) had downloaded an application on his phone which enabled him to change his phones IP address to circumvent the screen time limits his parents had set. Rishi had learned this from his friends at school.

Other 16 to 17-year-old boys from the focus groups were also aware of VPNs and their ability to bypass parental restrictions on devices and networks.

Leela, mother of Rishi (17)

Leela had regulated much of what her son, currently 17, could do offline and online. She had strict routines and used a parental controls app to set up screen time limits for different apps and to block his phone so he could not connect to the Wi-Fi after 9pm. She also took her son's phone and laptop to her room to ensure he was sleeping early. When Rishi turned 16, Leela stopped taking his phone and laptop overnight.

"I stopped taking his phone and laptop overnight to start giving him some responsibility cause he's going to be 18 soon. But also, he has to learn by himself. I can't shield him all his life, can I?"

At the same time, Rishi learned from a friend how to get a VPN to connect to the Wi-Fi in the evening at home, and at school where the network was blocked. Leela found out about this and acknowledged there was not much she could do to stop him, as he was becoming more knowledgeable on ways to get around her rules.

Section summary:

- Most parents were flexible when it came to overseeing their child's online activities (e.g. restricting some activities but not others, sometimes helping them circumventing age restrictions).

- The measures used by parents ranged from stricter device-level controls or parental control apps to less rigid, relationship-based methods such as communicating with their child about their online activities or observing them using their devices.

- Parents generally had a higher level of oversight where they were more aware of the potential risks online. Other factors, such as the child's gender, perceived maturity and having had negative experiences online shaped parents' attitudes towards online risks and safety.

- There are tensions between parental involvement in online safety and the practicalities of maintaining control. As children get older, parents' ability and motivation to introduce online safety measures decreases, whilst children's ability and motivation to overcome these increases. This has important implications for age assurance as it shapes parents' desired involvement in their children's online activities.

Section 4
Conclusions

Overall, parents felt that services should have age assurance measures, but these could sit in tension with their desire for control and flexibility over what their children do online

While all parents wanted their children to be safe online, they also wanted them to grow up and learn how to handle risks independently. They wanted their children to avoid reaching a sudden point in time at which they reach a certain age and could do anything they wanted to online without restrictions, instead preferring to maintain flexibility when it came to overseeing their child's online activities. This means that parental oversight often came with space for conversation and negotiation, which could sit in tension with the concept of age assurance and age assurance measures.

Across the sample, there were a range of differences in household types and socioeconomic backgrounds. This included the child's status in the family (youngest, middle child, oldest), whether the household was single or co-parent, and the socioeconomic conditions of the household. However, there was no clear relationship between these differences and how families perceived online risks. Instead, the factors that played the largest role in parents determining how risk was perceived included: gender of the child, previous negative experiences online, and parental understanding of how platforms operate.

Age restrictions do not always feel meaningful, so many parents were allowing, and even facilitating, their children to circumvent current age assurance measures

Many parents did not understand the logic behind some of the current age restrictions for online platforms, and their preference for flexibility meant that rigid age restrictions often did not always feel appropriate. Some parents had a limited understanding of what could happen to their children online, and therefore did not always see the potential risks as carrying much severity. This meant they tended to want more robust measures for traditionally age-restricted activities, such as gambling, pornography and the buying of age restricted goods, but less robust measures for social media, gaming, and video sharing platforms.

Most children and parents were aware of how easy it is to circumvent current age assurance methods on social media and gaming platforms and had experiences of doing so. It is critical that age assurance methods align with the type of oversight parents want. If not, there is a risk that parents will support children in circumventing these methods.

Generally, parents felt that the effort required for an age assurance method should be proportionate to their perception of potential risks

When accessing social media, gaming, and video sharing services, which tended to be perceived as less risky, children preferred self-declaration whilst parents often preferred parental confirmation. However, parents and children leaned towards "tougher" measures, such as hard identifiers, for traditionally age-restricted activities (such as gambling, accessing sexual content, banking, buying age restricted products, and on some occasions, downloading age restricted games) as hard identifiers were seen as the most effective method and proportional to the risk.

For accessing social media, gaming and video sharing platforms, children preferred self-declaration, due the perceived ease of circumvention and desire to be able to access these platforms. Parents often preferred parental confirmation due to the perception of control and flexibility. Parents and children often felt less comfortable with the idea of sharing hard identifiers with these platforms.

Both parents and children reflected on accuracy, effectiveness, effort, and risk as important factors when thinking about age assurance methods

These four themes came up from the depth interviews as important factors parents and children reflected on, which were later explored more deliberatively in focus groups and used to probe what parents and children found more relevant.

When it came to using age assurance methods, some families were concerned that age assurance could introduce significant frictions for parents and children. Parents and children wanted minimal effort when using the platforms day-to-day. However, they did not mind investing effort upfront or on a one-off basis as long as it meant the method would be more effective.

Many doubted the accuracy and efficacy of many of the age assurance methods and could think of many ways to circumvent the methods. Some raised doubts about how worthwhile the process of age assurance would be for the methods they saw as less effective. It was felt that age assurance needs to be effective to be worth the effort required.

Some raised privacy concerns around sharing data with platforms for age assurance

Some parents and children raised concerns about sharing their data with online platforms for age assurance, particularly in relation to hard identifiers and behavioural profiling data. The level of concern seemed to depend on which organisations the data would be visible to and, in the case of behavioural profiling data, whether it was being reviewed by a human or an AI. However, it seems there is a trade-off between the accuracy of an age assurance method and how comfortable parents and children felt in taking data sharing risks, as many agreed that hard identifiers were the preferred method for accessing platforms they perceived to be the most risky.

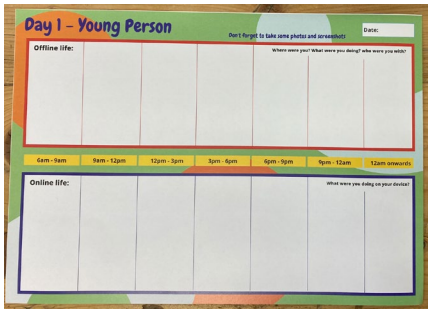
Annex: Methodology and sample detail

Media diaries & in-home interviews

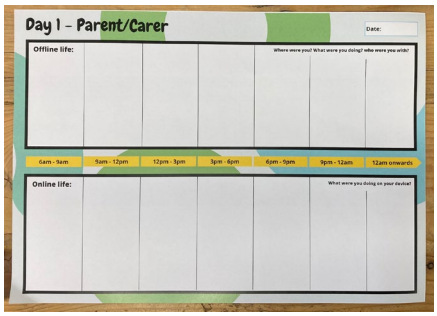
Method

Eighteen families participated in the media diaries and in-home interviews. All families taking part in the research were asked to complete a 'media diary,' where an allocated researcher asked the parent and child to record their online and offline activity over the course of three days. Families were asked to send accompanying screenshots of their most common online activities and photos of the devices they used during the three days. Families were also asked to send a short (two to three minute) video introducing themselves.

The media diaries and accompanying activities were used to provide researchers with an initial understanding of the different families taking part in the research and to prompt parents and children to reflect on their online media use prior to arranging the in-home interviews. In addition to its introductory function for both researchers and families, the pre-task was designed with the objective of capturing background information around the daily lives of parents and children and how online media use interacted with other activities across the day.



Example of child media journal



Example of parent media journal

In-home interviews were arranged to take place in the homes of participating families following the completion of their media journals and an introductory phone call with the researcher conducting the interview. Home visits lasted approximately four hours. These visits included two separate interviews: one with the parent and one with the lead child, as well as an hour of 'observation' during which the researcher was able to learn more about family relationships and communication at home.

In-home interviews were designed to:

- Gather contextual insights around family dynamics, approaches to parenting and parental oversight of online media use
- Better appreciate how age assurance technologies would fit into existing family practices
- Understand and appreciate the drivers behind current parental oversight measures and children's attitudes and behaviours on social media and other online platforms
- Triangulate differences in perspective and practices of parents and their children
- Explore attitudes around the existing and potential provision of age assurance technologies online

Interviews were semi-structured, in which several areas were explored with both parents and children, including:

- Family life
- Parenting, rules and responsibilities
- Children and parent media use
- Media use oversight by parents
- Attitudes and opinions around existing age assurance methods
- Attitudes and opinions toward potential age assurance technologies

To support the interviews, researchers used visual stimulus to prompt discussion and explain concepts to respondents. For example:

- Logos of social media platforms and other platforms that age assurance may take place on
- Visual representations explaining each age assurance method
- Scenarios in which adults and children may need to assure their age

To note: researchers asked more generally about the platforms and services respondents used and then probed on these platforms collectively. Researchers did not ask questions relating to age assurance about specific platforms but instead probed around the platforms and services parents/guardians and children had stated they used.

Sample

Overall, eighteen families participated in the in-depth interviews. The families that took part were sampled across a variety of criteria to ensure a diversity of experiences. Below is an overview of the core sampling criteria and the spread across these criteria achieved in the research.

Age of the child taking part in the research:

- 5 x 8–10-year-olds
- 4 x 11–12-year-olds
- 6 x 13–15-year-olds
- 3 x 16–17-year-olds

Family size and composition: the families interviewed reflected a variety of different household compositions and family arrangements. These included single-parent, co-parent and step-parent households, as well as families in which the children split their time between two households. Similarly, the number of children and the nature of relationships between siblings varied across families.

Ethnicity and religious practice: families interviewed included those of a variety of ethnicities, including seven Black, Asian and Minority Ethnic families. In addition to ethnic diversity in the sample, families also represented a variety of religious affiliations, including Islam, Catholicism, Judaism and Sikhism.

Location: families interviewed were based in locations across the UK, including England, Wales, Scotland, and Northern Ireland which reflected a spread of rural, suburban, and urban areas.

Socioeconomic background (MRS Social Grade 'ABC1' system) based on the standard National Readership Survey definitions[6]: families reflected households with a chief income earner in a range of occupations and earning a range of incomes:

Grade	Types of job	Families in sample with grade
AB	Higher or intermediate managerial and professional	7
C1/C2	Supervisory clerical, junior management/skilled manual workers	8
DE	Semi-skilled, casual, unemployed	3

Financial vulnerabilities: seven of the families involved in the research were at risk of financial vulnerability, as indicated by access to free school meals, universal credit, or healthy start vouchers.

Physical or mental health conditions: four of the families included in the research had parents with physical or mental health conditions that affected their daily activities in such a way to limit their ability to work full-time. Four of the children interviewed also had physical or mental health conditions that were being professionally managed.

[6] https://www.mrs.org.uk/resources/social-grade

Parental oversight: half of the families involved in the research were assessed as having 'medium to high' oversight and half 'low to medium' oversight. This was based on a recruitment questionnaire that included self-reported indications of parental concerns, worries, and practices around monitoring and controlling their child's online media use.

Child's primary device usage and online activity: families interviewed included a range of child device usage, including those where children spent less than two hours a day using a device to those where children typically used a device for more than six hours a day. Families also included a variety of device and activity preference, across gaming, social media, and video streaming.

Deliberative Focus Groups

Method

Focus groups were designed to further explore objectives from the in-home interviews and the different themes that emerged from these visits. The focus group methodology was designed to more deliberatively explore previous knowledge and initial attitudes towards different age assurance methods. This included exploring the views of parents and children around the different trade-offs such technologies might involve in practice, such as the privacy, accuracy, efficacy, and effort to use different technologies in different scenarios and by different groups in the population.

Both parent and child groups followed the same structure. The focus groups began by exploring respondents current understanding or past experiences of age restrictions and age assurance technologies, as well as general perceptions around the use of age assurance technologies. They then proceeded to explore individual age assurance technologies, prompting responses and debate around the trade-offs of each and individual respondent's preferences in different scenarios and situations. Throughout the groups, private responses were encouraged. So too were questions and concerns that respondents had in relation to the different technologies they were introduced to.

Sample

Eight focus groups were conducted, four with parents of children of a variety of ages and four with children at different ages. A total of seventeen parents and twenty-three children took part. Parents and children were recruited separately and did not overlap with those included in the in-home interviews.

Parallel sampling considerations were used as those in the in-house interviews. As such, the parents and children reflected a range of backgrounds, including family size and composition, ethnicity, socioeconomic group, location, parental oversight and child media usage.

The parent focus groups were organised around the age of their children and included four groupings:

- Parents/guardians with children aged 8 – 10
- Parents/guardians with children aged 11 – 12
- Parents/guardians with children aged 13 – 14
- Parents/guardians with children aged 15 – 17

These groupings were chosen in order to better appreciate the way children's age may influence attitudes and practices around parental oversight – including parental strategies and concerns around children's online activities – as well as opinions of different age assurance technologies and their proportionality in different circumstances.

The children's groups were organised around both age and gender, these groups included:

- Boys aged 13-14
- Boys aged 16-17
- Girls aged 13-14
- Girls aged 16-17

Children were recruited as pairs of friends. These groupings were chosen in order to ensure that children taking part would feel comfortable to take part in discussions around online media use and age assurance technologies.

The selected age brackets were chosen to reflect different experiences, with 13-14 being the minimum age at which children can join social media platforms whilst adhering to community guidelines and 16-17 reflecting an age where children typically prefer greater independence as they grow into adults.