Consultation response form

Please complete this form in full and return to AgeAssuranceCfE@ofcom.org.uk.

Consultation title	Call for Evidence: Statutory reports on age assurance and app stores
Full name	Matthew Sinclair
Contact phone number	
Representing (delete as appropriate)	Organisation
Organisation name	Computer and Communications Industry Association (CCIA)
Email address	msinclair@ccianet.org

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how Ofcom handles your personal information and your corresponding rights, see Ofcom's General Privacy Statement.

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? Delete as appropriate.	Nothing
Your response: Please indicate how much of your response you want to keep confidential. Delete as appropriate.	None
For confidential responses, can Ofcom publish a reference to the contents of your response?	N/A

Your response

Question	Your response
Section A – Age Assurance **Question 1**: How have regulated service providers used age assurance for the purpose of compliance with the duties set out in the Act?	Confidential? – N In accordance with the duties at ss.12(3)-(7) OSA, service providers have adopted proportionate systems and processes satisfying the requirement to implement age assurance that is highly effective at correctly determining whether or not a particular user is a child. Service providers are focused on complying with the requirements set out in the Codes of Practice and Ofcom's guidance on highly effective age assurance. Ofcom should ensure it is taking a proportionate approach to assessing compliance with these requirements: as recognised in the Act and Ofcom's guidance, service providers need to ensure that processes as a whole are highly effective, rather than focusing on individual examples of child users circumventing age assurance processes. We welcome Ofcom's recognition (for example, at the House of Lords Communications and Digital Committee) that the implementation of age assurance methods cannot be 100% accurate at identifying child users in the UK who are using the service. Ofcom should therefore ensure that it appropriately recognises the good faith systemic compliance efforts of service providers, especially in light of a provider's particular risk profile, and should avoid focusing on individual instances where child users circumvent age assurance processes. Furthermore, where service providers are using other tools as part of the age assurance process to mitigate the risk that children encounter age-sensitive material (for example, parental controls), this should be taken into account when assessing the effectiveness and proportionality of the age assurance process.
Question 2: How effective has the use of age assurance been for the purpose of compliance with the duties set out in the Act?	Confidential? – N No response

Question	Your response
Question 3: Has user privacy, cost, or any other factor prevented or hindered the effective use of age assurance, or a particular kind of age assurance, for that purpose?	Confidential? – N Collecting additional personal data from users, in particular children, inherently creates privacy concerns. Requiring services to consider this risk (as envisaged in the earlier additional safety measures consultation) does not give companies a practical way to mitigate the impact on privacy and data minimisation. Depending on how they are implemented, many of the current age assurance measures risk undermining the privacy and security of users. While companies have worked to respond to the duties set out in the Act and subsequent guidance, issues remain, in addition to and often compounding those privacy concerns, including: accessibility risk for those unable to prove their age (including users who could comply, but are not willing to incur the burden); large-scale circumvention possibilities undermining the effectiveness of the measure; and whether the application of highly effective age assurance to illegal content matches the legislative intent. In particular, we consider that the current obligations and guidance do not sufficiently emphasise the need to minimise the collection, use and monitoring of user data. This issue is particularly acute where the data being assessed is that of a child. Where a parent has appropriately confirmed the age of a child user, no further processing of the child's data should be necessary to determine whether or not they are a child user. Alongside, or in the alternative, the use of parental controls to protect children against harmful content should be included as a way in which relevant lower risk services can comply with the child safety duties. Permitting the use of parental controls as a method by which children can be prevented and protected from encountering Primary Priority Content and Priority Content enables compliance with the requirements of the Act, while minimising the negative impact on child users' rights, and would avoid the need to prohibit child users from accessing the service altogether. Furthermore, what constitutes an effective age assurance process on one service may differ from what is effective on another. Ofcom should therefore recognise that service providers are themselves likely to understand

Question	Your response
	best how to deploy age assurance on their products. Rather than relying on a standardised approach to determine whether there has been effective implementation of age assurance processes, Ofcom should engage with service providers to understand the nature and characteristics of their service that may affect whether age assurance has been implemented effectively on that particular service. Ofcom should also recognise the difficulty for service providers in minimising the friction involved when introducing age assurance processes, to ensure a seamless user experience. Service providers themselves will be most keenly aware of how and at what point to introduce age assurance to avoid disproportionately impacting the user's experience of the service, and to reduce the chance of them looking to circumvent the age assurance process or leaving the service (and the associated implications for freedom of expression).
Section B – App Stores **Question 1:** What role do app stores play in children encountering: a) user-to-user content that is harmful to children; b) search content that is harmful to children; or c) regulated pornographic content **In answering this question, please provide any rationale and evidence where available. To help inform your response, you may wish to consider the role the following categories play in children encountering such content, including:** • App review and approval process • App store age ratings • Design and functionality of the app store for child	Confidential? – N In many cases, the role of app stores themselves in children encountering harmful content is indirect and limited. (a) Harmful user-to-user content can occur and has occurred in settings which are primarily intended for children, online and offline. When harmful user-to-user content is encountered in a particular app, that therefore often does not mean the app store has provided users with access to an inappropriate app; rather, mitigation takes place within the app itself. (b) Content harmful to children discovered on the web, e.g. sites featuring inappropriate content, does not involve users downloading any apps. No app store controls could therefore plausibly prevent users finding such content. (c) Pornographic content is already excluded from the most popular app stores as a category.

Question	Your response
accounts/devices (e.g., discovery and navigation) • Safeguards to protect children from harmful content (e.g., parental controls, setting and enforcement of terms of service).	
Question 2: To what extent do app store providers currently use age assurance? **Please describe any age assurance methods applied at the app store level (e.g. during account creation, purchase approval, or app/content access), including the purpose(s) for which they are used.** • Where relevant, explain how age assurance applied at the device or operating system level interacts with app store mechanisms. • Where possible, provide evidence or examples of how effective these current processes are in ensuring children cannot access harmful content.	Confidential? – N App stores may establish age with an appropriate level of assurance at account set-up, for example through self- or parental attestation of age, credit card verification, and/or AI-driven age assurance solutions. Some app stores then use that age to set certain default settings and robust parental controls. These voluntary tools help parents make choices over how their children download apps. Given that content inappropriate for children is generally not allowed under established terms and conditions (see response to Q1), parental controls also target other features (e.g. how much time children are spending using apps), along with what content is being accessed. All else equal, regulatory measures that undermine the responsiveness of app store developers to consumer demand for parental controls, forcing them to respond instead to compliance exercises, would be a step backwards. For example, over-restrictive blocks and/or mandatory default restrictions could undermine effectiveness by causing parents to turn off parental controls entirely.
Question 3: What other protective measures and policies currently exist at the app store level to protect children? How effective do you consider they are?	Confidential? – N App store operators work to address risks to users (including but not limited to children) through a thorough review process. This includes: • Reviewing apps to reject or remove those that are malicious, exploitative or otherwise violate terms and conditions.

Question	Your response
	• Marking apps with age ratings to enable parental oversight. • Excluding content falling into certain categories, e.g. many app stores do not accept apps that contain pornographic content and will exclude them at that review stage. • Putting technical limits on app operation that prevent users being exposed to certain risks. • Marking apps as not suitable for children and enabling parental controls. • Enhanced developer verification processes. • Allowing parents to approve or decline a child's downloads or in-app purchases. • Providing additional user support tools. These controls vary, but enable parental and user choice, with many of the most popular app stores providing controls that respond to user demand for safety and security.
Question 4: Do you think that children's online safety would be better protected from the content types listed in Section B, Question 1 by: a) greater use of age assurance; b) particular kinds of age assurance; or c) other measures, at the app store level? **You may wish to consider the categories listed beneath Section B, Question 1 when identifying potential protective measures.** **You may also wish to consider the potential barriers or risks to implementing age assurance, particular kinds of age assurance, or other measures at the app store level.**	Confidential? – N Protecting children from online threats requires constant vigilance and effort by all players in the ecosystem. The best way to help parents and developers meet these challenges is generally by focusing on parental controls to help provide an age-appropriate experience for children (e.g. allowing parents to set up child accounts with the correct age, which enables appropriate default settings). There is also wider work that can be done to educate users (and promote digital literacy). This helps protect children while also minimising the amount of sensitive personal data that needs to be shared. Features should be designed around privacy, and users should always be in control of their data. Generally speaking, the Digital Trust & Safety Partnership "Age Assurance: Guiding Principles and Best Practices" report[1] lays out five guiding principles for age assurance: • Identify, evaluate and adjust for risks to youth to inform proportionate age assurance methods, as part of implementing safety-by-design.

[1] https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf

Question	Your response
Please provide your rationale for your views, and evidence where available.	● Account for risks to user privacy and data protection as part of development, implementation, and ongoing assessment of age assurance approaches. ● Ensure assurance approaches are broadly inclusive and accessible to all users, regardless of age, socioeconomic status, race, or other characteristics. ● Conduct layered enforcement operations to implement age assurance approaches. ● Ensure that relevant age assurance policies and practices are transparent to the public, and report periodically to the public and other stakeholders regarding actions taken. Many of these principles would need to be implemented differently at the app distribution level, vs the app or website level. Age assurance implementation should be designed to optimize both effectiveness and user experience. Different technical approaches may be appropriate for different contexts, and regulatory frameworks should enable innovation while ensuring appropriate child protection. User privacy and data protection risks are created whenever a service is required to share age-related data with other operators, including app stores (versus doing so as part of a voluntary interaction, where they have discretion to take such risks into account). Any age data sharing requirements should also address the risk of user frustration. For example, users might become frustrated if they cannot verify their age (for whatever reason) and they cannot tell whether the app store or the individual app or website level is better placed to help them fix the issue. Responsibility for user safety should be appropriately shared among app developers, service providers, app stores, and parents/guardians. Individual services are often best positioned to manage their content and user experiences and can implement safety features, as they understand their users and the risks associated with their services. However, app stores may also be positioned to give developers appropriate tools to better understand

Question	Your response
	their users, while still protecting the privacy of those users. If Ofcom were to assess that additional app store-level age assurance was necessary and proportionate to the impact on user privacy and freedom of expression, and considering requiring app stores to implement age assurance, any obligations should be: (a) Limited to the same obligations as existing regulated services in respect of determining whether a user is a child or an adult: it would be not only disproportionate but likely technically infeasible to require app stores to detect the specific age / age group of a child user. There are no clearly established or widely accepted technologies that enable service providers to identify children of different ages. Furthermore, children are much less likely than adults to hold accredited identification documents, and have limited other ways in which they can prove their age. In any event, requiring children themselves to go through age verification has significant privacy implications. (b) Risk-based: only app stores at medium or high risk of content harmful to children should be required to adopt age assurance. This would be in line with the approach taken in the EU under the Digital Services Act. Existing measures that app stores already take to protect children, such as parental controls, should be taken into account when assessing risk. (c) Designed with sufficient flexibility to allow providers of app stores to implement methods that continue to protect privacy and support data minimisation: we are concerned about proposals that threaten user privacy by requiring companies to build tools that would share sensitive personal information about any user who wants to download an app or access the internet. Any

Question	Your response
	obligation on app stores should clarify that compliance does not require the collection of sensitive information about children, and should entrust parents to provide the age of their child when establishing a child's account. Ofcom should therefore focus its age assurance efforts on ensuring that parents who establish an account for their child are adults. (d) Based on further engagement with providers on the way in which age assurance at the app store level interacts with age assurance carried out by apps: Ofcom should permit flexibility as to how age information is transmitted between app stores and apps, and as to how app stores implement their responsibilities. Any obligations imposed should be done with user control in mind, for example, parents should be empowered to decide whether the age range of their child is shared with developers.

Please tell us how you came across this consultation.

- ☐ Email from Ofcom
- ☐ Saw it on social media
- ☐ Found it on Ofcom's website
- ☐ Found it on another website
- ☐ Heard about it on TV or radio
- ☐ Read about it in a newspaper or magazine
- ☐ Heard about it at an event
- ☐ Somebody told me or shared it with me
- ☐ Other (please specify)

Please complete this form in full and return to AgeAssuranceCfE@ofcom.org.uk.