# 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** | Stephen Tulip |
| **Contact phone number** | 07732375155 |
| **Representing (delete as appropriate)** | Organisation |
| **Organisation name** | ACT \| The App Association |
| **Email address** | stulip@actonline.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?** | Yes |

## Your response

| Question | Your response |
|---|---|
| **Section A – Age Assurance**<br>**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<br>Many of ACT \| The App Association's small business members host their apps on regulated service providers such as the Apple App Store and the Google Play store. While the stores themselves are better positioned to describe their full efforts to comply with the requirements of the Online Safety Act, ACT members know that there are a number of age assurance measures already in place. App developers must currently indicate the age appropriateness of their apps when distributing through one of these stores or be subject to removal. App stores also provide robust parental controls. |
| **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<br>NA |
| **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<br>ACT members are concerned that policies requiring age assurance at the app store level with follow-on obligations for individual apps on those stores have problematic implications for both user privacy and cost. The vast majority of apps are general audience apps that do not host user-generated content or content that is inappropriate for a child. Requiring them to process notices from the app store that a specific user is a child, for example, raises data privacy concerns, as business that would otherwise have no knowledge of whether any user is a child would now have to collect that data. This leads to potential increased compliance costs, which we discuss further below. |

| Question | Your response |
|---|---|
| **Section B – App Stores**<br>**Question 1:** What role do app stores play in children encountering:<br>a) user-to-user content that is harmful to children;<br>b) search content that is harmful to children; or<br>c) regulated pornographic content<br>**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:**<br>• App review and approval process<br>• App store age ratings<br>• Design and functionality of the app store for child accounts/devices (e.g., discovery and navigation)<br>• Safeguards to protect children from harmful content (e.g., parental controls, setting and enforcement of terms of service). | Confidential? – N<br>As discussed above, app stores already provide age ratings as part of the approval process for apps and already provide robust parental controls to limit a child's account from accessing inappropriate content. However, it is important for policymakers to understand that app stores are not the same as social media platforms, and not all apps are social media apps. Indeed, most apps have nothing to do with social media.<br>Social media, where users generate vast amounts of content, some of which is potentially inappropriate for children, and where that content is directed to users algorithmically, carries a higher risk of exposing children to inappropriate material than the vast majority of other apps, which are often for more narrow uses and do not contain user-generated content at all.<br>ACT members are concerned that policies drafted with the kinds of harms in mind that are more or less unique to social media will cause significant unintended burdens for the entire app ecosystem. Making app stores the sole defence point for age verification is also ill-fitting because many social media companies are also websites; preventing children from downloading a social media service's app will not prevent a child from accessing the service via browser.<br>ACT also believes that potential harms caused by social media are better dealt with at source, rather than passing the burden of age verification to the millions of small businesses that are hosted on online marketplaces.<br>ACT urges Ofcom to consider where demonstrated harms occur before placing burdensome requirements on the vast array of apps that have no relation to those harms. |
| **Question 2:** To what extent do app store providers currently use age assurance?<br>**Please describe any age assurance methods applied at the app store level (e.g. during account creation, purchase approval, or app/content** | Confidential? – N<br>An important benefit of app stores for small businesses is data holding. A company can have a general audience app popular with children and never have to collect or hold any information about the age of identity of their users and subscribers, as that information remains with the store. This is a boon for user privacy. |

| Question | Your response |
|---|---|
| **access), including the purpose(s) for which they are used.**<br>• Where relevant, explain how age assurance applied at the device or operating system level interacts with app store mechanisms.<br>• Where possible, provide evidence or examples of how effective these current processes are in ensuring children cannot access harmful content. | Changes like those about to go into effect in parts of America, like Texas's App Store Accountability Act, fundamentally change this dynamic by requiring app stores to inform app developers of the age of their users via flags. As discussed below, this weakens user privacy and puts developers in a difficult compliance position with regard to existing laws.<br>As mentioned previously, much of the harmful content that Ofcom and the public are concerned about is on social media platforms that can easily be accessed by browsers.<br>Social media companies reportedly have detailed knowledge of the age, behaviours, and even vulnerabilities of their users (https://www.business-humanrights.org/en/latest-news/meta-allegedly-targeted-ads-at-teens-based-on-their-emotional-state/ ) and so are perfectly placed to protect their young users from harm on an ongoing basis as the harms grow and evolve. |
| **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<br>The guidelines impose additional requirements (see section 1.3 of the Apple App Review Guidelines), prevent certain actions such as outside links (for example, to a website) and in-app purchases without a parental gate.  Parental gates, while not perfect, are a mechanism that prevent kids from accidentally choosing options that may not be appropriate, requiring parent intervention to proceed. Kids' apps also are not allowed to send personal identifiable information to third parties. There are also strong restrictions on any behavioural advertising.<br>In addition, the App Review Guidelines contain a number of privacy protections that apply to people of all ages but are particularly important when it comes to information about children. For example, mechanisms that prevent tracking users across multiple apps, as well as data security requirements. Dark patterns are also not allowed and will result in rejection of the app when detected.<br>While no measures can provide air-tight guarantees, these restrictions and requirements seem to be largely |

| Question | Your response |
|---|---|
|  | effective in protecting children's data from being harvested and preventing children from being tricked in actions that would require parental permission. Many older children can figure out how to circumvent parental gates, but the gate still provides a marked barrier, and it is nearly impossible to come up with a test that only parents can pass. It may be possible for bad actors to work and hide techniques from app review and activate certain features after the app has been approved but this is deceptive and probably illegal behaviour that would probably be best be addressed by law enforcement. |
| **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:<br>a) greater use of age assurance;<br>b) particular kinds of age assurance; or<br>c) other measures, at the app store level?<br>**You may wish to consider the categories listed beneath Section B, Question 1 when identifying potential protective measures.**<br>**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.**<br>**Please provide your rationale for your views, and evidence where available.** | Confidential? – N<br>ACT urges Ofcom to consider requirements that are more specifically tailored to the kinds of harms children face online rather than applying them to all apps regardless of purpose or content. Despite seeming like they would impose a burden that falls only on the app stores themselves, app store-level mandates are also a significant cost for apps who use those stores. Small businesses who maintain apps will be required to modify their app to interface with whatever new process for age verification alerts the app stores create. And that's before considering how such policies would interact with other existing privacy laws in the UK and abroad. For general audience apps operating in both the UK and the United States, app store age verification procedures could put them out of compliance with the United States' Children's Online Privacy Protection Act (COPPA) by giving them "actual knowledge" of child users, which triggers COPPA's more significant requirements. Some have estimated that such compliance could range from £45,000 to £219,000 (https://www.americanactionforum.org/insight/coppa-2-0-the-costs-of-layering-on-liability/) |

**Please tell us how you came across about 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.