Age Verification Providers Association
557B Wandsworth Road, London, SW8 3JD
[✂]

Online Safety Team
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

By email: IHconsultation@ofcom.org.uk

23rd February 2024

Dear Sir or Madam

Response to consultation: Protecting people from illegal harms online

The Age Verification Providers Association is a global trade body representing suppliers of privacy-preserving age assurance solutions, including both age verification and age estimation. We set out below our narrowly-focused response to the above consultation, confining our comments to matters relevant to our members and within our sphere of specialist knowledge.

Consultation title	Protecting people from illegal harms online
Full name	Iain Corby
Contact phone number	[✂]
Representing (delete as appropriate)	Organisation
Organisation name	The Age Verification Providers Association
Email address	[✂]

Confidentiality

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

Assessment of the causes and impacts of illegal online harms

In the real world, it is relatively easy to know when you are dealing with a child, and indeed to estimate the approximate age of the child and adapt accordingly. A consequence of anonymity and pseudonymity online is that, without taking specific action, the age of the user is not known.

This is an important aspect to any analysis of the causes and impacts of online harms, and is not addressed explicitly in the preamble. It would provide useful context for measures recommended later in the documentation if this was clearer in the assessment.

Ofcom's approach to proportionality is excessively economic: to avoid imposing undue costs on companies. While the Act requires regulated services take a "proportionate" approach to fulfilling their duties, and indeed requires Ofcom to look at resources, Ofcom is also required to look at the severity of harm when weighing the need for action. Even the smallest site with negligible revenue could do great harm without applying basic protective measures and must not be given a free pass – or given the impression it has one which in places this guidance does, if inadvertently.

The following comments relate to Table 1 Measures proposed for U2U services in the "Consultation at a Glance" and are referenced accordingly.

Governance and Accountability

No. 1 Ref. 1: We agree that either a named person or an overall governance body should carry out an annual review to record how the service has managed the risk of illegal harms.

No. 4 Ref. 3D: We argue that a large service with a specific risk should carry out Internal monitoring and assurance function to assess independently the effectiveness of measures to mitigate and manage the risks of harm, reporting to a governance body or an audit committee. It does not seem to be logically defensible that the number of risks would affect the degree of governance for risk as a whole. Large services will generally have internal audit functions already in place, and these can be directed to review the management of specific risks without a disproportionate impact.

Content Moderation

No. 9 Ref. 4B: We also propose that a smaller service with a specific risk should be required to adopt Internal content moderation policies, having regard to the findings of risk assessment and any evidence of emerging harms on the service. It does not seem to be logically defensible that the number of risks would affect the degree of management of the risk.

No. 9 Ref. 4C & 4D: Smaller services with a specific risk relating to content moderation should also have targets for content moderation functions and prioritise content review in line with multi-risk services. Similarly, if the specific risk that applies to the service is one that is mitigated by content moderation, staff should have training and materials to identify and take down illegal content.

Automated Content Moderation

No 14-16: In addition to hash matching, there should be a requirement to apply automated age assurance to detect potential newly generated CSAM. This would flag content where anyone depicted in the content appears to be under 18 – it may be that the algorithms test for an age above 18 determined by their expected accuracy e.g. 21, to reduce the risk that they miss detecting any minors to <0.1%.

This would have to operate in conjunction with age verification for all performers in adult content, so where a person in the content is flagged as appearing to be under 21, there is evidence available to confirm they are in fact 18 or older. That would also drive more comprehensive consent records, as performers would usually, unless they are under duress, they would need to consent to supply the requisite evidence for such an age check.

Without these changes, the guidance creates a major loophole in the regime, allowing a performer who is 18+ to create an account and then give the use of it to a child who will potentially secure a higher revenue stream. The guidance also ignores the risks presented by newly created Child Sexual Abuse Material by requiring checks against only hash databases of known CSAM. Given the growth in self-generated CSAM, and CSAM created under duress by children, and knowing that we have technology that is proven to be able to flag a huge proportion of such material for manual review and removal, this major vector for illegal harms should not be ignored.

Default settings and support for child users

No 28-29 Note d: These measures are only recommended for a service which ii) has an existing means of identifying child users. This deprives children on services which do not happen to have yet implemented any form of age assurance, perhaps even only self-declaration, of protection from grooming.

This creates a perverse disincentive to U2U platforms to introduce age assurance of any kind, as to do so will impose these additional protective requirements.

If this loophole is retained, which we hope it is not, then the phrase "existing means of identifying child users" needs to be rewritten and clarified.

i. The term "identifying" is misleading as it could imply that the platform must only comply with these requirements when they have knowledge of the full identity of children that use it. A better phrasing would be "has an existing means of knowing which users are under 18 years old"
ii. That then needs to be clarified, so could continue "through:
    a. Self-declaration of age by users
    b. Age assurance (age verification or age estimation using biometric or behavioural indicators)
    c. Profiling of users for the purposes of marketing or advertising which treats them as minors for this purpose
    d. The nature of the service appealing mainly to minors
    e. [Evidence that a significant number of minors in the UK use the service]
    f. [Complaints from users that minors are being groomed through the service]

Enhanced User Control

No 31-33 9A, 9B & 9C: These protections should also be in place for child users by default, including for smaller services where there is a specific risk, along with the requirements to prevent grooming No. 28 & 29.

Thank you for the opportunity to shape this world-leading guidance.

Yours faithfully

Iain Corby
Executive Director