

Common Sense Media

TO: Ofcom

FROM: Common Sense Media

DATE: 4 March, 2024

RE: [Consultation](#): Guidance for service providers publishing pornographic content

CONFIDENTIALITY:

Per Ofcom's consultation response form, the whole response below is not confidential. Responses may be attributed to Common Sense Media.

✂

RESPONSE:

Common Sense Media is the leading nonprofit organisation dedicated to improving the lives of all children and families by providing the trustworthy information, education, and independent voice they need to thrive in the 21st century (see more below).

We are pleased to submit these comments in response to Ofcom's age assurance consultation for service providers publishing pornographic content. Common Sense supports Ofcom's efforts to protect children's safety while ensuring their privacy, and we offer constructive suggestions to achieve this balance below.

Common Sense emphasises in response to the consultation that age assurance technologies and methods are evolving quickly. Where the Online Safety Act requires age assurance, such as for service providers publishing pornographic content online, Ofcom's guidance must reflect and encourage that evolution so as to prevent service providers from stagnating their age assurance systems and incentivize improved practices. This updated guidance will ensure that industry protects children using the best-available methods, including with input from civil society and other experts.

More specifically, our responses to the consultation:

- Highlight the need for multiple age assurance methods in certain circumstances,
- Note circumvention risks to some of Ofcom's proposed highly effective age assurance methods,
- Emphasise that age assurance methods must be accessible to consumers in all socioeconomic positions, and
- Recommend that Ofcom establish an innovation forum to ensure platforms and providers regularly review ways to strengthen age assurance methods, in consultation with civil society.

Question 3: Do you have any comments on our proposed guidance in respect of the kinds of age assurance which could be highly effective? If you consider there are other kinds of age assurance which have not been listed that you consider could fulfil the proposed criteria, please identify these with any supporting information or evidence.

Confidential? – N

Common Sense Media offers three comments with respect to the proposed methods of age assurance considered to be highly effective.

First, if the goal is highly effective age assurance, Ofcom should consider requiring that at least two methods of age assurance be used at once. At present, several of the methods described in the guidance as ‘highly-effective’ only show considerable efficacy when combined with other kinds of verification methods, though the technology continues to improve. For example, industry leaders in biometric age estimation (including traditional face scanning and emerging technologies like vein pattern recognition) currently rate their products as having a margin of error of roughly ± 1.4 years for users aged between 13 and 19.¹ That means that a 17 year old could be determined to be anywhere from 15.6 to 18.4 years old—insufficient for highly-effective age verification on its own, especially for those publishing adult content. Indeed, where biometric age verification has been implemented now, there is typically a requirement for a second kind of verification.² To determine whether a user is 18, systems are set to biometrically determine if a user is at least 25 to account for margin of error, then require a second kind of age verification if users are biometrically determined to be 24 or younger.

Second, Common Sense emphasises the privacy concerns associated with many of the listed methods. While all age assurance methods require giving up some amount of personal information about users, methods such as credit card or bank verification may present special concerns since they require disclosing financial information. We don’t think those concerns invalidate these as effective methods for age assurance, however, we would strongly support adding more privacy-sensitive options to the list of highly-effective methods. For example, offline age verification³—wherein some kind of “scratch card,” or physical token, is sold in stores that are already equipped to verify customer age (like liquor stores or pharmacies) and then registered online or on a third-party verifier app with the adult’s email address—can represent a highly effective method that presents lesser privacy concerns since little identifying information is saved in any system.⁴ We don’t mean to imply that scratch cards represent a silver bullet solution, rather point to it as an example and encourage Ofcom to strongly consider greater research or consultation in the area of privacy-protective age assurance measures.

¹ *Facial Age Estimation white paper*, Yoti (15 Dec., 2023), <https://www.yoti.com/blog/yoti-age-estimation-white-paper/>.

² Charles Hymas, *AI face-scanning technology to be rolled out at supermarkets to check age of shoppers*, The Telegraph (24 Jan., 2024), <https://www.telegraph.co.uk/news/2024/01/24/ai-face-scanning-technology-supermarkets-age-alcohol-id/>.

³ Sarvesh Mathi, *What Are The Different Age Verification Methods Available And Why Are They Problematic?*, Medianama (11 Jan., 2023), <https://www.medianama.com/2023/01/223-online-age-verification-solutions-privacy-issues/>.

⁴ *Online age verification: balancing privacy and the protection of minors*, CNIL (22 Sept., 2022), <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.

Finally, as mentioned above, we think the guidance must do more to incentivize companies to “do better” and raise the standard for protecting children online. As written, the proposed guidance seems only to require that companies employ the best age assurance measures currently available. Common Sense is concerned that in doing so, Ofcom is, albeit unintentionally, creating a negative incentive structure for companies. Rather than keeping pace and evolving with technological innovations, companies may be encouraged to stagnate their age assurance methods so as to meet only the minimum threshold provided by the guidance.

The spirit of this concern—that implementation of the OSA could set the bar too low for industry compliance and “reinforce the status quo, which the legislation was intended to improve”—has also been raised to Ofcom by a number of civil society groups in the context of mitigating illegal harms.⁵

We thus recommend that Ofcom make clear its expectations for service providers to stay abreast of new age assurance methods and technologies and implement them in a reasonably timely manner. And, relatedly, age assurance methods not explicitly listed as highly-effective may well be determined to be so in the future. Service providers can and should strive to continue evolving and doing better, and should not be limited to currently available technology. Ofcom could make it more clear that other non-enumerated methods may be considered highly effective, which could enable and propel companies to continue developing more effective and privacy protective age assurance methods.

Question 5: Do you have any information or evidence on the extent of circumvention risk affecting different age assurance methods and/or on any steps that providers might take to manage different circumvention risks for different methods?

Confidential? – N

Several of the proposed age assurance methods are susceptible to circumvention. Common Sense recommends that Ofcom include a list of possible or common circumvention methods in their guidance, so as to put service providers on notice and encourage development of preventative tactics. While many circumvention methods are curable through technology or design features, the existence of many of these circumvention risks further justifies our above suggestion that in situations where highly-effective age assurance is desired, service providers should be required to operate more than one age assurance method.

Credit Card Checks: Of the methods described in the guidance as highly effective, this method presents the largest circumvention risks.⁶ Children may be able to access parents’ cards without their knowledge, or may have authorised cards under their parents’ accounts which don’t require them to be 18.⁷ While some solutions exist to solve the first problem—for example,

⁵ Online Safety Act Network, *Ofcom’s Illegal Harms Consultation: Emerging Concerns*, <https://www.onlinesafetyact.net/uploads/osa-network-ofcom-illegal-harms-sign-on-feb-2024.pdf>

⁶ *Age verification: Striking the balance between security and privacy in bid for children’s online safety*, Biometric Update (20 Mar., 2023), <https://www.biometricupdate.com/202303/age-verification-striking-the-balance-between-security-and-privacy-in-bid-for-childrens-online-safety>.

⁷ *Can I add my child to my credit card?*, GoHenry (18 Feb., 2024), <https://www.gohenry.com/uk/blog/financial-education/can-i-add-my-child-to-my-credit-card>.

requiring users to verify the precise amount of an instantly-refunded charge would prevent kids from using a purloined parents' credit card to pass age verification—very little can be done about a child whose parents permit credit card usage.

Indeed, this problem has borne out in the U.S. since the passage of the Children's Online Privacy Protection Act in 1998. Since its enactment, which required age assurance for children under 13, credit card verification has become both the most common and the *most circumvented* method of age assurance in the U.S.—with reports showing that as many as 1 in 5 children have access to a credit card that they can use to circumvent the check.⁸

VPN Circumvention: The use of virtual private networks allows children to change the digital location from which they access content—thereby circumventing country-specific or location-specific age gates. In the UK alone, 23% of minors say they have the ability to use this technology to bypass age verification.⁹

Other Technological Workarounds: In addition to VPN circumvention, a range of technologies exist that enable children to access age-restricted content, including: torrenting media content, using proxy websites or servers, using a TOR browser, or even accessing the 'dark web.' Recent surveys show that as many as 25% of children aged 14-15 and 33% of children aged 16-17 report knowing how to use these tools to circumvent age assurance.¹⁰ And these services are often hard to identify, decentralised, and designed to evade law enforcement such that they are difficult to design around or counter.

That these circumvention risks defy easy solutions shows the need for more development in this area, and lends credence to a requirement for service providers to use multiple age assurance methods in cases where high assurance is needed. A multiple age assurance methods approach is also consistent with recent ICO guidance, which found that waterfall techniques—the practice currently used with biometric technologies of setting multiple age buffers and requiring more strict verification of users closer to 18 —provide high levels of confidence and solve some circumvention concerns.¹¹

Question 6: Do you agree with our proposed guidance that providers should consider accessibility and interoperability when implementing age assurance? Please provide any information or evidence in support of your views.

Confidential? – N

Common Sense agrees that providers should consider accessibility and interoperability when implementing age assurance, but we believe the guidance should go further than merely encouraging providers to consider the accessibility of age assurance methods. Rather, Common

⁸ The State of Play: Is Verifiable Parental Consent Fit For Purpose?, Future of Privacy Forum 11 (June 2023), <https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf>.

⁹ Young people, Pornography & Age-verification, BBFC 56 (Jan. 2020), <https://www.revealingreality.co.uk/wp-content/uploads/2020/01/BBFC-Young-people-and-pornography-Final-report-2401.pdf>.

¹⁰ *Id.* at 56.

¹¹ Age Assurance for the Children's Code, Information Commissioner's Office 10-11 (15 Jan., 2024), <https://ico.org.uk/media/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code-1-0.pdf>.

Sense recommends that the guidance make consideration of the accessibility of an age assurance method mandatory for service providers.

We acknowledge that the fairness criterion, as currently written, creates a mandatory consideration that age assurance methods are fair across different racial, gender, sex, disability, and age lines. Common Sense notes, however, that certain age assurance methods may be inaccessible to various users for reasons that are not directly related to the above—and not necessarily formally protected classes. For example, financially disadvantaged individuals may not have access to certain forms of identification, a functioning camera with high enough resolution to perform a biometric scan, or a credit card/bank account. This accessibility concern extends beyond the criterion required to be considered under fairness.

While accessibility is considered by the guidance, it is listed merely as an “additional principle for providers to consider.” Common Sense believes that an age assurance method’s accessibility is a core consideration in determining whether or not to use it, and therefore supports inclusion of accessibility as a mandatory, and not merely an additional, concern for providers.

Conclusion

Common Sense Media believes that meaningful regulation is critical to our broader mission of protecting children in the digital world. Moreover, strong global collaboration among regulators, civil society, and tech industry is particularly key to address common pain points such as age assurance that can help successfully enforce child safety policies. To that end, we applaud Ofcom’s global engagement, regulatory progress to date, and investment in ample resources to help address these complex challenges.

As Ofcom considers ways to incentivize age assurance innovation, we recommend that Ofcom establish an innovation forum to ensure that platforms and providers regularly review ways to improve age assurance methods. The regulator would play a key role in both facilitating a space for tech companies to collaborate and engage, as well as hold platforms accountable for progress. Ideally this forum should include civil society voices who can bring practical expertise in youth experiences online, relay real time challenges with age assurance, or even bring children and parents to the table.

Finally, Common Sense recognizes that Ofcom is undergoing a number of consultations regarding the Online Safety Act, and we encourage Ofcom to remain vigilant about consistency in this process. Ofcom should also consider the extent to which its guidance is consistent with the recently published opinion from the Information Commissioner, which evaluates in detail the effectiveness of several of the proposed highly effective age assurance methods.¹²

Common Sense Media is grateful for the opportunity to respond to Ofcom’s online safety consultation regarding age assurance and service providers publishing pornographic content. As a trusted global brand for children and families, we look forward to helping bring American and global perspectives to consideration as Ofcom develops essential regulatory guidance, standards, and tools to improve children’s lives around the world.

¹² *Id.*

About Common Sense Media UK

Common Sense is an independent nonprofit organisation dedicated to helping children thrive in a rapidly changing world. The organisation is based in San Francisco with regional offices across the U.S. We launched our first international office in the UK in 2019, a registered charity (also Common Sense Media, 1188840), through which we rate, educate, investigate, and advocate for the safety, privacy, and well-being of children in the UK and globally.

Common Sense Media achieves its aim to create a more healthy, equitable, and empowering future for children in the following ways:

RATE: Through our parent platform, Common Sense Media, we provide independent ratings and reviews of various forms of media.

EDUCATE: Through Common Sense Education, we share our Digital Citizenship curriculum with millions of teachers across the world to increase media literacy and shape digital citizens, as well as offer tips to families and communities as they navigate media and technology.

ADVOCATE: We advocate and raise awareness to drive policy and industry changes that protect the safety, wellbeing, and privacy of children in the digital world, including the UK, EU, and USA.

INVESTIGATE: Our team conducts independent research to provide parents and caregivers, educators, health organisations, and policymakers with reliable, independent data on young people's use of media and technology and its impact on their physical, emotional, social, and intellectual development.

For more information, visit <https://www.commonsense.org/>.