5RIGHTS FOUNDATION

Consultation: Guidance for service providers publishing pornographic content

5Rights Foundation, consultation response
March 2024

Summary

Pornographic content is exceptionally harmful to children, with more than half becoming exposed to it before they reach the age of 13.[1] This is enabled by non-existent or extremely weak age assurance – with only 37% of the top 100 pornographic services offering age assurance; and all but one only requiring self-declaration.[2]

We welcome Ofcom's work to produce this guidance on age assurance and Part 5 duties so soon following the Online Safety Act coming into force. This guidance will be a crucial feature of the online safety regime and will help protect children from harm online. However, given the clear legislative aim of this duty – to ensure child are not normally able to access pornography – there are gaps Ofcom must address.

Services must be supported to understand if they are firmly in scope of this duty so they can act accordingly. The guidance currently leaves the scope undefined, leaving providers to make the case that they do not meet the 'significant UK user' threshold themselves. This could lead to a large loophole for services to not comply, where they have a small overall user base or where they deem that their UK user base is small in proportion to global user base. Ofcom must align the 'significant' threshold with the ICO's definition used for the Age Appropriate Design Code (AADC)[3] to maintain regulatory alignment. In principle, if a service knows via internal data or independent research that any child accesses it service then it must be in scope. Ofcom must also provide more clarity for services that provide gen-AI models to create pornography but do not necessarily publish the content – such as nudify apps – and ensure they are firmly in scope.

As the age assurance sector continues to grow and develop we support Ofcom's general approach to not prescribe a specific method. However, with this approach Ofcom's criteria for what constitutes 'highly effective' age assurance must be water-tight. As there are no legal definitions for 'technically accurate', 'robust' and 'reliable', Ofcom must look to accepted standards to underpin the judgement of being 'highly effective'. Standardisation bodies ETSI, ISO and the Institute of Electric and Electronic Engineers (IEEE)[4] have, or are currently carrying out, work on this area which Ofcom should

[1] Children's Commissioner (2023) *'A lot of it is actually just abuse': Young people and pornography*
[2] BBFC (2023) *Functionality of online pornography services: A BBFC research report for Ofcom*
[3] ICO (2020) *Age Appropriate Design Code*
[4] IEEE Online Age Verification Working Group

consult. Ofcom should also draw on the work of euCONSENT[5] and work of CEN-CENELEC.[6]

All current age assurance systems require the use of some personal data, yet 'privacy-preserving' is not noted as a factor within the proposed criteria. Ofcom must mandate that services have privacy and security of data built into their processes, and must include 'privacy-preserving' and 'secure' in their judgements to build confidence and trust for all users.

Record keeping is central to enforcement of these duties. The guidance sets out that providers will have to record a great deal of likely sensitive data. Rather than refer them to guidance from the ICO, Ofcom must take on more accountability and build obligations regarding the GDPR and the AADC into a service's record keeping duties.

Overall, the guidance is brief on how Ofcom will enforce this duty and concentrates on internal processes over outcomes. While it may be a challenge to set a threshold for how accurate age assurance methods should be, as no system is yet perfect, Ofcom risks allowing services to be compliant simply because they have an age assurance method in place that meets their criteria. Ofcom should instead measure compliance on whether the method has achieved the intended outcome – that children are not normally able to access pornography. This could be done through recording how many children have been prevented access to the service measured against either internal research or independent research on how many children are currently accessing the service without age verification in place. Services could also look to reporting and complaints data, in addition to commissioning independent research.

The guidance is unclear on how providers will be compliant. Ofcom could support providers by giving detail in the guidance on how they will be assessed against the criteria and outcome by setting out its own internal testing systems.

Consultation response

Consultation question 1: Do you agree with our proposed guidance on scope? If not, please provide any information or evidence in support of your views, including descriptions of services or content where you consider it is unclear whether they fall within the scope of Part 5.

The proposed guidance for condition 1 (regulated provider pornographic content is published or displayed) and condition 2 (the service is not exempt) are, in our view, in line with the legislative intent of this part of the Act and provide adequate direction. However, condition 3 (the service has links to the UK) is too vague and does not provide

[5] euCONSENT
[6] CEN-CENELEC (2023) Workshop agreement CWA 18016, *Age appropriate digital services framework*

clarity for services. This could risk creating a loophole for smaller services, leaving children at risk of viewing pornographic content.

Significant number of UK users

We are concerned that Ofcom has not defined the threshold for what constitutes a 'significant number of UK users.' Instead, the guidance adopts a trust-based approach where providers "should be able to explain their judgement" offering little clarity as to the basis for it.

Ofcom must provide more clarity on the exact threshold in line with the legislative intent of the Act. Leaving this undefined could allow services to deem themselves out of scope based on a small overall user base or proportionally small UK user base based on their global user base. Typically, providers are not transparent with regards to the size of their user bases. The ICO's definition for "significant" in the threshold used as part of the AADC sets a low bar and we would encourage Ofcom to follow this to maintain regulatory alignment.[7] In principle, if any child can access a commercial pornography service, it should be in scope.

Ofcom should set a low bar for meeting these criteria. This is crucial, given that these are the only criteria determining whether a service falls into scope of their duties. The Online Safety Act states requires that "children are not normally able to encounter" pornographic content,[8] with ministers emphasising throughout the passage of the Act that smaller platforms would not be exempt from the regime.[9] Ofcom must ensure that the guidance means children cannot access pornographic content.

Consultation question 2: Do you have any comments on how our proposed guidance applies in respect of pornographic content created by generative-AI services within the scope of Part 5? Please provide any information or evidence in support of your views.

Ofcom must provide greater clarity to how this guidance will apply to all gen-AI spaces that host technology which allow users to create pornography. For example, it is not clear that services which provide the models for users to create this content, but do not necessarily publish the content on the service, would be in scope. So called 'nudify apps', for example, are of growing concern and have been found to be used by children.[10] There are also websites which do not exclusively allow for the creation of gen-AI pornography, but supply models for the creation of all types of content.[11] Ofcom must provide clarity that these services would also be in scope and would be expected to have age assurance measures in place, given the severe risk they pose to children.[12, 13]

---

[7] ICO (2020) *'Likely to be accessed' by children: FAQs, list of factors and case studies*
[8] 81(2) in the Online Safety Act 2023
[9] Lord Parkinson of Whitley Bay, Online Safety Bill, Report (5th Day)
[10] Daily Mail (2023) *AI-powered 'Nudify' apps that digitally undress fully-clothed teenage girls are soaring in popularity*
[11] See: Civitai
[12] Fortune (2023) *'Nudify' apps that use AI to undress women in photos are soaring in popularity*
[13] Euronews (2023) *Naked deepfake images of teenage girls shock Spanish town: But is it an AI crime?*

Consultation 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.

We agree with Ofcom's overall approach of not prescribing a particular method for age assurance but believe the criteria against which methods are judged must be made stronger, underpinned by best practice and existing standards, in addition to measuring compliance against whether it has met the intended legislative aim – preventing children from accessing pornography.

Best practice and age assurance standards

While the criteria established by Ofcom in the guidance are a good start, there is no legal definition of 'technical accuracy', 'robustness' or 'reliability'. Services must be required to demonstrate the effectiveness of their method with data. Ofcom's criteria and must also be underpinned by existing standards.

There are an existing set of interdependent and interconnected common standards considered best practice for the use of age assurance. These are reflected in technical standards developed or currently in development by International Standardisation Organisation, the European standardisation bodies ETSI and CEN-CENELEC,[14] and other international organisations such as the Institute of Electric and Electronic Engineers (IEEE).[15]

These common standards make clear that age verification measures must:[16]

- Adhere to data minimisation in order to be privacy-preserving, only collecting data that is necessary to identify the age, and age only, of a user
- Protect the privacy of users in line with GDPR and the Age Appropriate Design Code[17]
- Be secure and prevent unauthorised disclosure or safety breaches
- Provide routes to challenge and redress if the age of a user is wrongly identified
- Be accessible and inclusive to all users, particularly those with protected characteristics
- Be effective in assuring the actual age is over 18

We note that the guidance fails to reference the AADC in particular, which the Act specifically says Ofcom must have regard to in relation to age assurance in Schedule 4:

---

[14] CEN-CENELEC (2023) Workshop agreement CWA 18016, *Age appropriate digital services framework*
[15] IEEE Online Age Verification Working Group
[16] CEN-CENELEC (2023) Workshop agreement CWA 18016, *Age appropriate digital services framework*, Section 5 and 8; ICO (2020) *Age Appropriate Design Code*; Federal Trade Commission (2020) *Complying with COPPA: Websites and Online Services Directed to Children, including mixed audience sites and services*
[17] ICO (2020) *Age appropriate design: A code of practice for online services*

> *"In deciding whether to recommend the use of age assurance, or which kinds of age assurance to recommend, OFCOM must have regard to the …relevant standards set out in the latest version of the code of practice under section 123 of the Data Protection Act 2018 (age-appropriate design code)"*[18]

Outcomes-based approach

We agree with Ofcom's non-prescriptive approach regarding age assurance methods but argue that the guidance should be clear that compliance is measured on the outcome of any such method used.

Minister Lord Parkinson of Whitley Bay during the passage of the legislation was clear that these measures were "designed to ensure that children are prevented from accessing pornography"[19]. This is the core intended outcome with respect to the Part 5 duties, and should be Ofcom's focus in setting out guidance.

However, the guidance as currently drafted suggests that Ofcom could be satisfied that a service has complied with its Part 5 and age assurance duties if the method in use meets its set criteria, none of which show that it has successfully prevented children from accessing pornography. The focus on measuring if services have "cho[sen] an appropriate kind (or kinds) of age assurance" and if they have "implement[ed] it in such a way that it is highly effective at correctly determining whether a user is a child" neglects to include that it has achieved that purpose. Even if a strong method of age assurance had been applied correctly, services still have a duty to ensure it is achieving the intended outcome.

Ofcom must be clear that, while services have the freedom to use the most appropriate method or methods for its business, they will be held to account based on the outcome. This can be done by providing clarity what thresholds for efficacy Ofcom will be using. This could also be demonstrated with information on how many children have been successfully blocked from accessing the service, measured against external evidence of how many children currently access pornography websites (without age verification in place). Ofcom should also urge providers to carry out independent research and surveys of how many children access their service.

Consultation question 4: Do you agree that service providers should use the proposed criteria to determine whether the age assurance they implement is highly effective at correctly determining whether or not a user is a child? Please provide any information or evidence in support of your views.

As set out in our response to question 3, there are a suite of examples of best practice and international standards that Ofcom should judge the application of age assurance against in order to meet the legislative aims of the Act.

Ofcom's proposed criteria must include the following criteria:

Privacy-preserving

---

[18] Schedule 4 in the Online Safety Act 2023
[19] Lord Parkinson of Whitley Bay, Online Safety Bill, Report (1st Day)

5Rights is extremely concerned that the criteria does not reflect that age assurance methods must be privacy-preserving. During the passage of the Act, the Minister was clear that:

> *"Part 3 and 5 providers will need to have regard to the importance of protecting users' privacy when putting in place measures such as age verification or estimation. Ofcom will be required to set out, in codes of practice for Part 3 providers and in guidance for Part 5 providers, how they can meet these duties relating to privacy."*[20]

Data protection and age assurance are intrinsically connected, and are a matter for both Ofcom and the ICO. On this basis we would expect Ofcom to set out how it intends to uphold data protection within this duty through closer working with the ICO, rather than referring services to guidance from the other regulator.

Any system of privacy-preserving age assurance will need to ensure that it minimises the processing of data, retains data for the shortest time possible, and does not reuse, sell or share the input or output data beyond providing the result. In order to process data, the GDPR[21] requires a legal basis along with a clear purpose for processing it – in this case in order to carry out an age assurance check. Privacy-preserving, in the context of age assurance, is a method of performing the process that does not lead to any more personal information being stored than the single piece of data required as output data. In the case of age assurance, this could include a specific age, date of birth or age range.

We are concerned that the criteria does not refer at all to the AADC, which the Act says Ofcom must have regard to. At all times the AADC requires that the best interests of the child should be a primary consideration when designing and developing online services 'likely to be accessed' by a child,[22] including in the use of any data, however minimal, that is retained or gathered.

The vast majority of technical means for performing age assurance checks can be done in a way that preserves privacy.

Ofcom must make clear that privacy will be at the heart of the age assurance duties in the regime by placing this as a core facet of what constitutes 'highly effective' age assurance. The criteria must include that age assurance must:

- Only use necessary information for establishing the age of the user, and delete this data once it has confirmed age
- Not store data for other purposes or aggressively collect data
- Ensure higher protection for children as per the standards of the AADC (Section 123 of the Data Protection Act 2018)[23]

---

[20] Lord Parkinson of Whitely Bay, Online Safety Bill, Report (2nd Day)
[21] ICO (2020) *UK GDPR guidance and resources*
[22] ICO (2020) *Age Appropriate Design Code – Principle 1: Best interests of the child*
[23] Section 123 if the Data Protection Act 2018, *Age-appropriate design code*

Secure

The criteria must reflect that age assurance systems should uphold data protection duties on data security to support trust and robustness in the system.

As set out above, age assurance necessitates providing some data to the service that a user is trying to access. Accessing or attempting to access a Part 5 service specifically can be highly sensitive, and is a particular privacy issue to users. Service providers have an extremely poor record on data security. Meta[24], X (formerly Twitter)[25] and TikTok[26] have all fallen foul of vulnerabilities in their systems which have left millions of users' data in the hands of hackers. Commercial pornography services have also been compromised by data hackers.[27] Data security is a key principle of the UK GDPR, and the ICO states that services processing personal data must do so "securely by means of 'appropriate technical and organisational measures'."[28]

Ofcom must include this as part of the criteria for a 'highly effective' age assurance system. In order to deliver on this criterion, providers will have to ensure that they limit storage of any personal data both in quantity and time. For some services, they may store no data all once the age assurance has been provided, nor even technically process any data. For instance, ensuring that all the assurance process takes place on the user's device, without transmitting any data beyond the require age assurance, is one such method. Beyond being a benefit for the individual, this also ensures that no central database of identity linked to online activity is ever created.

Route to redress

Ofcom must ensure that the criteria includes a route to redress mechanism for age assurance. A key criteria of highly effective age assurance is 'fairness', which Ofcom contends may not always be achievable due to the permanent risk of false positives. No age assurance system is perfect and, while this is in development, Ofcom should require services to offer a system of redress to allow adult users to challenge where they may be blocked from services they have a right to view. This would help build overall confidence and trust in the system.

Consultation 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?

Circumvention is a key risk for the reasons set out in the guidance.

---

[24] Forbes (2022) *Meta fined for 2021 data breach as millions of Twitter users' data also leaked*
[25] The Guardian (2023) *Hackers reportedly leak email addresses to more than 200 m*
[26] France24 (2023) *EU fines TikTok €345 million over child data breaches*
[27] Cybernews (2024) *MyFreeCams Hacked: 2 million user records stolen from top adult streaming site and sold on hacker forum*
[28] ICO (2020) *A guide to data security*

As well as the more traditional methods of circumvention, we are concerned about AI-driven circumvention. A recent report by 404 discovered a website which helped users to create fake online identification by creating an AI tool, demonstrating that this technology is already widespread.[29] We would urge Ofcom to reflect this as a key risk for services to be aware of in choosing their preferred method for age assurance.

Consultation question 8: Do you agree with our proposed guidance on the record-keeping duties? Please provide any information or evidence in support of your views.

Record keeping and transparency are important components of this regulation.

Record of outcomes and compliance

We agree with Ofcom's guidance on information services regarding the written record requirements relating to age assurance, however privacy-preserving measures must be included in the record. Given this will be a key tool for measuring compliance, services should also be required to keep records of the outcome of any such methods used. As set out in a previous response, evidence of how well a system is working could set out figures on how many children have been blocked from accessing the service measured against the numbers of children we know access them and complaints and reporting data of where children may be uploading content. This would be in keeping with the legislative aims of the Act, and incentivise services to pursue more innovative measures for age assurance.

The guidance does not currently include how 'fairness', 'robustness', or 'reliability' or 'technical accuracy' will be measured. Ofcom should provide either thresholds or information on how they will test this. This will support services to understand what they should be aiming for in terms of outcomes.

Consultation question 9: Do you have any comments on our proposed approach to assessing compliance with the duties on service providers who publish or display pornographic content, including on the proposed examples of non-compliance? Please provide any information or evidence in support of your views.

Overall, we find that this section is very brief and does not include the detail nor threshold to support services in complying with this duty.

No threshold set for compliance: We support Ofcom's general non-prescriptive approach given the pace of the development of this technology. However, this does not preclude Ofcom from setting out expectations and thresholds for the intended outcomes of the methods used. Without thresholds, services will not know what to aim for. This could have the perverse incentive of allowing some services to defend a lower threshold, rather than aiming for a higher standard. The guidance would benefit from more detail on how services can meet the expected bar with regard to successful outcomes.

Lack of clarity on how services will be tested: The guidance does not provide clarity on how compliance will be judged against the criteria. Ofcom should provide more detail on

[29] 404 Media (2024) *'Neural Network' fake ID site goes dark after 404 Media investigation*

what factors will be taken into account when determining if an age assurance approach is robust, reliable, and fair. Ofcom could do this by setting out its own testing approach so that services ensure their own testing strategy meets this bar.