# RESPONSE TO OFCOM CONSULTATION ON GUIDANCE FOR SERVICE PROVIDERS PUBLISHING PORNOGRAPHIC CONTENT

---

**Issue**

We set out here our response to Ofcom's consultation on its draft guidance for service providers publishing pornographic content. This is the guidance that will support regulated services' compliance with part 5 of the Online Safety Act. There are a number of concerns that we raise below that have relevance to those we flagged in our response to Ofcom's Illegal Harms consultation - in particular, the approach to proportionality and the focus on costs. We also set out in our analysis the problematic decision that Ofcom has made to use a similar approach to age assurance to that already contained in the Video Sharing Platform (VSP) regime and the On-Demand Programme Services (ODPS) regime - despite the fact that the Online Safety Act requires a higher threshold – that such measures be "highly effective". This difference in threshold is not reflected in the draft guidance.

**What the Online Safety Act says**

The Online Safety Act has a standalone section (part 5) which places duties on "providers" of pornographic content – that is where pornographic content is published or displayed on the service by the provider of the service or "a person acting on behalf of the provider" – to introduce age assurance measures to prevent under-18s accessing pornographic material on their services. It is therefore regulating the online porn industry rather than social media or other online services that may host pornographic content that is uploaded or shared by users of the service, and therefore classed as "user-to-user" content.

The duties require regulated providers "to ensure, by the use of age verification or age estimation (or both), that children are not normally able to encounter content that is regulated provider pornographic content in relation to the service" (81 (2) and that "the age verification or age estimation must be of such a kind, and used in such a way, that it is highly effective at correctly determining whether or not a particular user is a child" (81 (3)). It also places duties on regulated providers to keep written records; and on Ofcom to produce guidance (section 82), the draft of which is now being consulted upon.

**Parliamentary debate**

It is important to note the policy and legislative history relating to the inclusion of this section in the Act. Part 3 of the 2017 Digital Economy Act introduced a requirement on pornography services (excluding on

demand programme services – separately dealt with under the Communications Act) to ensure that online pornography would be made available "in a way that secures that, at any given time, the material is not normally accessible by persons under the age of 18" (s 14 DEA 2017). It provided for the designation of a regulator to oversee this, along with a variety of enforcement powers. While age verification technologies were implied by the DEA – and the regulator was to be named the Age Verification Regulator – they were not specifically referred to and standards of effectiveness were not identified.

In October 2019 – six months after the Government had published its Online Harms White Paper – the then DCMS Secretary of State Nicky Morgan, announced that the Government would not be enacting part 3 of the DEA:

> "It is important that our policy aims and our overall policy on protecting children from online harms are developed coherently in view of these developments with the aim of bringing forward the most comprehensive approach possible to protecting children.
>
> The government has concluded that this objective of coherence will be best achieved through our wider online harms proposals and, as a consequence, will not be commencing Part 3 of the Digital Economy Act 2017 concerning age verification for online pornography. The Digital Economy Act objectives will therefore be delivered through our proposed online harm regulatory regime. This course of action will give the regulator discretion on the most effective means for companies to meet their duty of care. As currently drafted, the Digital Economy Act does not cover social media platforms." (Written Statement 16 October 2019)

The draft Online Safety Bill, published in May 2021, made provisions to repeal the Digital Economy Act part 3 but did not extend the provisions for protecting children from pornography in the Bill beyond social media sites. Part of the justification for this was that many pornography sites had user-to-user (U2U) functionality so would be covered by the provisions in the Bill. Following pre-legislative scrutiny of the draft Bill, during which many representations were made about the lack of coverage for commercial pornography sites and the likelihood that those that *were* covered by virtue of having U2U functionality would simply disable that functionality to avoid the need for compliance, the Joint Committee on the draft Online Safety Bill concluded that: "the Bill does not provide sufficient protections for children, including failure to capture all pornography sites" (p22).

In its response, the Government agreed to incorporate "a standalone provision into the Bill requiring providers who publish or place pornographic content on their services to prevent children from accessing that content. This addresses the concerns that have been raised about a gap in scope, and ensures that all services that would have been captured by both Part 3 of the Digital Economy Act and all the user-to-user and search services covered by Online Safety Bill will be required to protect children from pornography. This new duty will be enforced by Ofcom with providers being subject to the same enforcement measures as services subject to the safety duties." The text of Part 5 appeared in the Online Safety Bill as introduced in May 2022.

During the Bill's passage, the provisions in this part were amended as a result of significant campaigning and pressure on the Government, particularly in the Lords. The main amendments, introduced by the Government at Lords Report, included:

- the expansion of the scope of "regulated provider pornographic content" to include that displayed on a part 5 service by means of "an automated tool or algorithm", so covering AI-generated porn (s. 79(2)(b));
- the insertion of the requirement on regulated services to use "age verification or age estimation (or both)" (s. 81(2)) – rather than using "for example, by using age verification" – in their duty to ensure that children "are not normally able to encounter content that is regulated provider pornographic content";
- the requirement, at s 81 (3), that "age verification or age estimation must be of such a kind and used in such a way that it is highly effective at correctly determining whether or not a particular user is a child";
- that Ofcom's guidance on these duties must include "examples of kinds and uses of age verification and age estimation that are, or are not, highly effective at correctly determining whether or not a particular user is a child" (s 82(2)); and that it "may elaborate" on principles, including that "age verification or age estimation should be easy to use", "should work effectively for all users regardless of their characteristics or whether they are members of a certain group", and "interoperability between different kinds of age verification or age estimation".

Introducing the amendments to tighten up the requirements vis-à-vis age verification and age assurance – having come under significant pressure in previous debates, particularly from Baroness Kidron and Lord Bethell – the DCMS Minister Lord Parkinson said: "These amendments will also ensure that there is a clear, privacy-preserving and future-proof framework governing the use of age assurance, which will be overseen by Ofcom. Our amendments will, for the first time, explicitly require relevant providers to use age verification or age estimation to protect children from pornography. Publishers of pornographic content, which are regulated in Part 5, will need to use age verification or age estimation to ensure that children are not normally able to encounter content which is regulated provider pornographic content on their service." (Online Safety Bill - Lords Report stage - 6th July 2023 - col 1429)

Parkinson went on:

> "Providers covered by the new duties will also need to ensure that their use of these measures meets a clear, objective and high bar for effectiveness. They will need to be highly effective at correctly determining whether a particular user is a child. This new bar will achieve the intended outcome behind the amendments which we looked at in Committee, seeking to introduce a standard of "beyond reasonable doubt" for age assurance for pornography, while avoiding the risk of legal challenge or inadvertent loopholes.
>
> To ensure that providers are using measures which meet this new bar, the amendments will also require Ofcom to set out, in its guidance for Part 5 providers, examples of age-verification and age-estimation measures which are highly effective in determining whether a particular user is a

> child. Similarly, in codes of practice for Part 3 providers, Ofcom will need to recommend age-verification or age-estimation measures which can be used to meet the new duty to use highly effective age assurance. This will meet the intent of amendments tabled in Committee seeking to require providers to use measures in a manner approved by Ofcom."

[In advance of Ofcom's consultation on the OSA's children's duties, given that the age verification techniques used for those duties also will need to meet the standard of highly effective, it is worth noting that Parkinson also said:

> "Similarly, in codes of practice for Part 3 providers, Ofcom will need to recommend age-verification or age-estimation measures which can be used to meet the new duty to use highly effective age assurance. This will meet the intent of amendments tabled in Committee seeking to require providers to use measures in a manner approved by Ofcom." (Hansard - 6th July 2023 - Col 1430)]

**Ofcom's proposals**

Ofcom sets out its proposals to implement these duties in its consultation document, with the draft guidance published as a separate annex. We know from conversations with organisations in our network that there are a number of specific concerns with the proposals, including the lack of specificity as to what "highly effective" means and the risk that, in not specifying this at the outset of the regime, the industry will comply with what is a much lower bar than that intended by the legislation and will then settle at that baseline in years to come.

Ofcom has set out that "currently, we do not have sufficient evidence as to the effectiveness and potential risks of different age assurance methods to recommend specific metrics for assessing whether or not any given age assurance method or process should be considered highly effective" (4.12) … "Furthermore, as the age assurance industry is still nascent, with improvements and new solutions likely to emerge over time, we consider it would not be appropriate at this time to set a base level or score which service providers must ensure their age assurance method or process meets for each of the criteria. We also want to allow space for important innovation in the safety tech sector. For these reasons, we are not proposing specific metrics that the age assurance process should achieve for each of the criteria." (4.13)

Instead, the draft guidance (at section 4) sets out how regulated providers can use age assurance to deliver their duties under the Act and Ofcom will use evidence from their written record to judge whether they are compliant or not.

In place of recommending specific types of technology, Ofcom sets out (at figure 4.1) criteria that age assurance methods should fulfil to be "highly effective", including that it is "technically accurate", "robust", "reliable", and "fair", with examples of the type of age assurance used in other contexts (open banking, photo-ID matching, age estimation, etc) that could be highly effective. It is notable here that they also include the possibility of "other methods that fulfil each of the criteria". This, Ofcom argues, "affords service providers a degree of flexibility in how they comply". This is a markedly different

approach to the prescriptive approach taken in the illegal harms consultation proposals, which we discuss below.

**Analysis**

We set out in our response to the illegal harms consultation our concerns that Ofcom was focusing too much on reducing costs to companies in its decisions on "proportionality" or otherwise; and taking too prescriptive an approach to recommending measures in the code of practice – only including those specific technologies that have met a sufficiently high evidence threshold and not focusing enough on outcomes. To some extent, we have similar concerns with the approach taken here too, particularly as regards the need for the measures taken to be highly effective. This is a threshold that is not present in other systems implementing age verification requirements (On-Demand Programme Services, Video-Sharing Platforms (VSP) and the defunct DEA regime, see above). We cover these in the sections below, along with some further observations.

Measures vs Outcomes

In this draft guidance, Ofcom is taking a more outcome-focused approach than it does in the illegal harms consultation. As the consultation document says at A1.17, "In developing our proposed guidance, we have exercised a degree of discretion in setting out specific expectations on what service providers 'should do' to fulfil their obligations. We have limited our use of discretion to the extent we considered necessary to clarify to services how they can comply with their duties. We also consider that these expectations are proportionate. They are the minimum steps we expect services should take to comply with their duties**. Moreover, the principles-based approach gives providers flexibility to determine which age assurance method(s) best suit their needs and to pursue cost-effective approaches which can be adjusted over time.** This should benefit all regulated services as it allows them to future-proof their systems and processes, and to respond to their user base and technical developments over time in the most cost-effective way for them". (A1.17)

While this is on one level very welcome, Ofcom does not provide sufficient criteria by which it will measure those outcomes and/or the providers' compliance with their duties. Ofcom's arguments about the "nascent" age verification industry (see above, though we also note age verification in some form or other has been required under the Communications Act for more than a decade) do not justify not having an output level score (especially in relation to technical accuracy). There is a difference between recommending a particular tool (which Ofcom in our opinion rightly is not doing) and measuring effectiveness of any tool. If the concern is that any one tool could not be effective enough, techniques could be used in combination with other tools. Ofcom's narrow approach means that it is precluding the potential effectiveness of combinations of techniques that might lead to the same outcome.

We note that Ofcom provides criteria describing different aspects of effectiveness. While we agree with these aspects, they do not in themselves provide a definition for highly effective. While we appreciate that there may be challenges in specifying a metric by which to judge "highly effective" age assurance technologies, there would be no reason why Ofcom could not specify a metric for each of their criteria that would indicate that the method adopted – and/or the implementation and enforcement of that method – by the regulated provider is "highly effective". If, in practice, the application of that age

assurance method falls below the metric specified, the written record could then be used by Ofcom to determine whether providers had used their best efforts and/or acted in good faith to ensure its effective implementation and identify those providers who had done neither. Ofcom however say that they are not doing "setting a base level for score" so because of the "nascent" age assurance industry and because they want to "allow space for important innovation in the safety tech sector". In our view, metrics related to Ofcom's criteria (rather than types of technology) would not preclude innovation in this field.

Focus on costs

In table A.1.1, which compares the costs and benefits impacts of the guidance on stakeholders, Ofcom admits that it has taken the minimum approach to delivering its duty in producing the guidance along with reducing the potential costs for stakeholders:

> "For age assurance to be highly effective at correctly determining whether a user is a child and to achieve the objective that children are not normally able to encounter regulated provider pornographic content on the service, it needs to fulfil each of the criteria. Further detail on the rationale for the proposed guidance is in paragraphs 4.11-4.13. **These are the minimum expectations required to enable Ofcom to fulfil its duty to provide guidance on compliance with the Part 5 duties, and for service providers to fulfil their obligations under the Act.** Our approach provides service providers with the flexibility to determine how they implement age assurance, rather than requiring them to implement a specific kind of age assurance, or achieve specific accuracy metrics results, for example. **This flexibility should benefit all regulated services as it allows them to future-proof their systems and respond to their user base and technical developments over time in the most cost-effective way for them.**

At para 2.32, Ofcom concludes that "based on the information currently available, our proposed guidance on the age assurance duties is proportionate as it clarifies our expectations of what services should do to comply, while retaining appropriate flexibility for providers to do so in the most cost-effective way." We note, however, that while Ofcom's approach as a regulator should be guided by the principle of proportionality, the obligation on providers in s 81(2) is not subject to a specific proportionality requirement – and this is by contrast to the position in relation to the Part 3 safety duties.

In the context of the long history of this particular regulatory intervention – from the passing of the Digital Economy Act in 2017 through to the repeal of its provisions to impose age verification requirements on pornography providers in 2019 and then the lengthy time taken for the passage of the Online Safety Bill – this focus on cost-effectiveness is at odds with the reality of the industry these provisions are aimed at. The voluntary introduction of age-verification measures across the online pornography industry has never been an option. Indeed, the Government's Online Safety Bill impact assessment cited research by the BBFC into the adult industry which suggested that "the current lack of age assurance - even when the industry has stated its willingness to adopt these technologies - **appears to be the result of competitive concerns and the potential commercial impact if this requirement is not mandatory across all services**. It is therefore important that the child safety duties and pornography provision together apply to all pornographic content accessible to UK users."

It is also at odds with both evidence on the impact and prevalence of harm arising from children's access to online porn and the increasing ease with which ever younger children find it online.

Evidence on the impact on children was detailed in the which cited a number of short and long-term impacts on children, including negative body image, impact on sexual attitudes and sexual violence and aggression towards women and girls – one study found that 10-15 year olds who consumed violent pornography were six times more likely to be sexually aggressive than those who did not consume it. The Impact Assessment concluded that "While it is not possible to monetise the impact of underage exposure to pornography, it has a clear and significant effect on children's attitudes and behaviours."

On the ease of access, a report from the Children's Commissioner last year found that "a quarter of 16-21-year-olds first saw pornography on the internet while still at primary school …by the age of 13, 50% had been exposed to it."

Regulatory and legislative links

The Online Safety Act is not the first time Ofcom has had to deal with age verification , under the ODPS regime under Part 4A Communications Act and the VSP regime in Part 4B. Section 368E(4) Communications Act specified that an on-demand programme service must take appropriate measures to ensure that any "specially restricted material" (which includes legal pornography (BBFC categories 18 and R18); pornography that is contrary to the criminal law is not permitted on these services) is only made available in a manner which secures that persons under the age of 18 would not normally see or hear it. Section 368E(4A) requires that measures be proportionate to the potential of the material to harm the physical, mental or moral development of those under 18. There is no requirement that the measures be "highly effective" - a contrast to the OSA.

The VSP regime also envisages that those under 18 should be protected from the same risk of harm (by reference to the same categories). The VSP regime provides (in Sch 15A Communications Act) a list of possible measures – including age verification. Ofcom notes that whether a measure is appropriate depends on whether it is practicable and proportionate – taking into account the type of harm, the characteristics of those being protected, the size and nature of the service and the rights of users. (See Ofcom VSP guidance para 2.35 here.)

The measures should be implemented in such a way as to carry out the relevant purpose (s 368Z1(2) Communications Act). Ofcom describes effective implementation as having the aim "to prevent users from encountering harmful material, potentially by reducing the prevalence of it ... continued occurrence of harmful material appearing on a platform may suggest that a platform has not taken appropriate measures or has not implemented them effectively". (Ofcom VSP guidance para 4.5). Ofcom further notes that measures should be effective, easy to use, transparent, fair and evolving. Ofcom further stated that "if a VSP has restricted material on its service that is of a pornographic nature, providers should have a robust access control system that verifies age and prevents under-18 from accessing such material" and that "the chosen access control measure(s) should be effective in preventing access to that material for under-18s". (VSP Guidance para 4.110 and 4.117)

**We might note the consistency of Ofcom's approach to the issue of age assurance, which on one level makes sense. Problematically, however, the underlying legislative provisions differ**. The existing ODPS

and VSP provisions expressly note that measures should be proportionate to harm caused – the OSA does not (though the rights of users should be taken into account generally); the harm here is accepted by the OSA's schema. There is in the VSP a recognition that the tools should be effective. Yet, the OSA requires a higher threshold – that they be "highly effective" and this difference in threshold is not reflected. The guidance for the Part 5 services and the use of the same criteria (e.g. fairness and robustness) is one further distinction between the VSP regime and the Part 5 regime. The VSP regime explicitly says that pornography which is contrary to the criminal law should not be on the service at all; there is no equivalent provision as regards Part 5 providers. This lack of content controls underlines the importance of access controls – and the need for highly effective measures.

We note Ofcom's concern about not interfering unnecessarily with adult's access to legal pornography content, but remind Ofcom that not all content on Part 5 services is automatically legal (e.g. Aylo has been fined for carrying content derived from sex trafficking and has insufficient safeguards to guard against image based sexual abuse (here)). In terms of disruption to the user, we note that the Gambling Commission has suggested that their existing rules "which allow operators to verify age and identity via background checks that are effective in the vast majority of cases and are minimally disruptive to the customer."

**Recommendation**

We hope that Ofcom will consider the points made above urgently, particularly given that there will be a read across to the Online Safety Act children's code measures with relation to age assurance (and on which Ofcom will be consulting shortly) and the emphasis that the Government, via the Pornography Review, is placing on the measures in the OSA to deal with many of the issues relating to online pornography.

**Online Safety Act Network**

**March 2024**

**Contact: maeve@onlinesafetyact.net**