AVPA

Age Verification Providers Association

Written evidence submitted by the Age Verification Providers Association (OSB0122)

Response to your call for evidence Online Safety Bill

Thank you for the opportunity to contribute evidence to inform your Joint Committee's pre-legislative scrutiny of the Online Safety Bill.

Children are at the heart of society's concerns about online safety, but unless we know which internet users are children, we cannot provide them with the additional protections they deserve; equivalents to measures we already consider essential in the real world.

This Bill provides further impetus to the Age Verification sector's work to establish the foundation of a safer internet for children – namely, a general, well-regulated and convenient mechanism to allow online services to know the age or age-range of their users *without* the need for those users to disclose their full identity.

Summary of our submission

- The Bill's scope is too narrow because it was designed to address only social media. Without amendment to the scope and altering a major exemption, **pornographic websites will escape regulation entirely**. To avoid this, Parliament should:
  - Add a third category of sites in scope to include all sites with content considered harmful to children (with or without user-to-user services)
  - Exclude sites in this new category from the "limited functionality services" exemption
- The Secretary of State should publish a draft list of *Primary Priority* and *Priority* Content to allow for meaningful scrutiny of the Bill in context.
- The Bill should regulate to promote an independent, privacy-protecting, standards based, open, competitive and interoperable age verification sector as a foundation for a safer internet for children
- Parliament should add a 6 month time limit for the laying before it of the suite of codes of conduct and statutory guidance to avoid the risk of 2-3 years delay while this is perfected by the Secretary of State and Ofcom.
- Enforcement powers should be amended to enable them to be applied at scale to 1.3 million adult websites without an individual application to the Court for each of them.

The Age Verification Providers Association is a global trade body which represents over 20 of the main technology suppliers who have invested in the development of age assurance solutions to support the implementation of age restrictions online. The UK has led the way in developing age verification, innovative age estimation solutions, and international industry standards. Our members already perform millions of accurate, privacy-preserving, independently audited and standards-based online age checks every year. AV technology works.

Will the proposed legislation effectively deliver the policy aim of making the UK the safest place to be online?

Not as initially drafted. The scope of the Bill reflects only the initial target of social media and search, so will not include harmful sites if they do not allow the user-generated content that characterises social media platforms and has been used as the basis of the Bill's definition of scope. This is major loophole.

Will the proposed legislation help to deliver the policy aim of using digital technologies and services to support the UK's economic growth? Will it support a more inclusive, competitive, and innovative future digital economy?

To some extent yes, but with important caveats. As the trade body for a fast-growing sector whose work involves helping organisations comply with regulatory requirements, the AVPA welcomes further clarification of the regulation in this area.

In terms of our field of age assurance, the UK remains the leading jurisdiction globally, despite the government's arguably[1] illegal decision to refuse to implement Parliament's will when it came to Part 3 of the Digital Economy Act 2017 (which the Online Safety Bill seeks to repeal). This new Bill could allow the UK to resume that leading role, creating substantial export opportunities for the UK 'safety-tech' sector. However, the omission of pornographic content from the scope of the Bill represents a huge missed opportunity to consolidate the UK as a world-leader in safety-tech. So, whilst we welcome the Bill in principle, it leaves important areas out of scope, is long overdue, and is likely to be subject to further delays, and as such any benefit to the UK's future digital economy risks being lost.

Are children effectively protected from harmful activity and content under the measures proposed in the draft Bill?

The Bill will also not offer *any* protection to children before its measures are being fully and vigorously enforced by Ofcom. The timing of implementation is a great concern, with your own Committee's deliberations being only the beginning a very lengthy process.

Prevent a 2-3 year implementation delay by adding deadlines to the Bill so Ofcom must

[1] The High Court gave permission in July 2020 for a judicial review of the decision to abandon Part 3 of the DEA on the basis it was arguable (under the Fire Brigade's Union precedent) that ministers may decide *when* to implement legislation but not *whether or not* to do so at all. The case was settled when HM Government committed to repealing Part 3 within the Bill now before the Committee for scrutiny, ensuring Parliament retained its power to decide what is and it not law in this respect.

prepare codes of practice relating to the additional duties applicable if the service is likely to be accessed by children within six months of Royal Assent.

Our experience of the thorough Ofcom process for developing guidance suggests there could be a very long delay before the new law is implemented and fully enforced unless statutory deadlines are included in the primary legislation. Ofcom is expected, only after Royal Assent to avoid legal challenges, to issue a Call for Evidence, then draft proposals for consultation, including Codes of Conduct in relation to each of the duties; these then need to be agreed by the Secretary of State and laid before Parliament, with delays possible for amendments or objections at any stage. Realistically, this could easily become a 2-3 year process before duties apply, and typically enforcement will only be implemented in a staged fashion; from monitoring, to supervision and eventually to regulatory action adding a further grace period before the regulator shows its teeth.

We are not criticising the rigor with which Ofcom apply themselves to their duties; rather we are recognising the urgency of the problems this Bill is designed to address, and arguing that the regulator should not let the best be the enemy of the good, or perfection trump speed. Clearly the guidance, codes of conduct and other output from the regulator will need to evolve over time, not least to address changes in technology, but putting a 'good enough' regime in place quickly needs to be ensured within the legislation. The risk otherwise is of the same degree of delay that beset Part 3 of the Digital Economy Act and still affects the Audio Visual Media Services Directive which has been law for almost a year but for which Ofcom's guidance is still not complete.

The Bill needs to be amended to prevent the best delaying the good, requiring Ofcom to complete a first version of the relevant codes and guidance within six months; with of course the opportunity to improve on them in future. Technology moves too fast to ever expect such documents to be either perfect or enduring.

Apart from the general scope issue already outlined above, there is also the question of what harms will be defined by the Secretary of State as Primary Priority or Priority Content. While Parliament will be given the opportunity to approve these schedules, debating the Bill without a draft list of these harms will fetter the ability of the legislature to consider sensibly the impact of the legislation. It is like being asked to assess the deterrent impact of revised sentencing guidelines without knowing to which crimes they will apply.

The Secretary of State should issue a draft schedule of Harmful Priority Content before the Bill is introduced to Parliament.

Does the draft Bill make adequate provisions for people who are more likely to experience harm online or who may be more vulnerable to exploitation?

Our primary focus is on children, who are inherently more likely to experience harm online. We argue that knowing whether an internet user is a child or not is a critical foundation for all forms of online child protection, and is also necessary to preserve the freedoms of adults who must otherwise be treated as if they are children.

This does not, however, require all internet users to share their full identity to the websites and services they are accessing. **The essence of online age verification is the ability to prove your age without disclosing your identity.**

Is the "duty of care" approach in the draft Bill effective?

This approach has the ability to be a generalisable legal route to applying proportionate protections across a wide variety of sectors. But the Bill has been drafted to limit the application of some or all of the duties it creates, with wide-ranging loopholes. There may be merit in a more inclusive approach to all online services, particularly those "likely to be accessed by children", to mirror the definition in S123 of the Data Protection Act (the Children's Code) and then applying specific exceptions where Parliament accepts these are merited.

Does the Bill deliver the intention to focus on systems and processes rather than content, and is this an effective approach for moderating content? What role do you see for e.g. safety by design, algorithmic recommendations, minimum standards, default settings?

There is a risk that the regulator the Bill creates is a paper tiger. It may write codes of conduct, issue guidance, make representations, but without the ability to take enforcement action in relation to specific complaints, find its impact mitigated. For example, with approximately 1.3 million pornographic websites, mostly based overseas, Ofcom needs broad administrative powers to cut off their access, and the services upon which they rely for payments, search, hosting and advertising so it presents a credible threat to non-compliant sites. The present enforcement mechanism would overwhelm the court system just to deal with adult websites.

Service restriction orders and access restriction orders must be applicable to unnamed services which meet stated criteria, so Ofcom can apply to the court for a general order applicable to multiple services – enforcement requiring a separate order for each service does not scale sufficiently. The current enforcement mechanism would require the regulator to apply to the court for an order for each of some 1.3million pornographic websites, which is clearly not a practical proposal. While there is an argument for retaining judicial oversight of the process as a whole, an amendment designed to allow for largescale enforcement action is critical. The risk otherwise is that regulators only tackle the largest sites, based on a misplaced logic of "risk-based regulation" which does not work when the internet offers such vast choice and the immediate ability to switch from one site to another. Traffic will rapidly divert to smaller sites which are out of sight of the regulator unless there is systematic, comprehensive enforcement to deliver a level playing field for all regulated sites on day one. The British Board of Film Classification took this to heart as they prepared to enforce the Digital Economy Act, and were discussing innovative automated mechanisms for assessing compliance at scale, and triggering comprehensive enforcement action well beyond the leading sites.

How does the draft Bill differ to online safety legislation in other countries (e.g. Australia, Canada, Germany, Ireland, and the EU Digital Services Act) and what lessons can be learnt?

The Bill is complementary to other EU legislation in respect of age verification. We are developing, as part of a European Commission funded programme, an interoperable network of age verification and parental consent providers. The euCONSENT network will facilitate the implementation of GDPR (digital age of consent) and the Audio Visual Media Services Directive, as well as provisions in this Bill, and other future EU legislation wherever there is a policy objective to protect children differently from adults online. This network will be online before the Bill becomes law, offering a convenient and ubiquitous AV solution, delivered by an open and competitive market of interoperable providers.

Independent, standards-based, regulated online age-verification is also being considered by countries as far apart as Australia, Canada and India.

Does the proposed legislation represent a threat to freedom of expression, or are the protections for freedom of expression provided in the draft Bill sufficient?

Narrowly speaking, those who cherish freedom of expression have nothing to fear from the age verification required in the Bill, provided it is managed through independent, regulated third parties so users do not need to share personally identifiable information with the websites and platforms they are accessing – AV providers simply confirm to those sites if a user meets their age requirements, yes or no, without sharing their full identity.

Content in Scope

The draft Bill specifically includes CSEA and terrorism content and activity as priority illegal content. Are there other types of illegal content that could or should be prioritised in the Bill?

Revenge porn and non-consensual pornographic content may merit further consideration for priority treatment, particularly given the evidence that children are increasingly being persuaded, often by other children, to create and post content.

Earlier proposals included content such as misinformation/disinformation that could lead to societal harm in scope of the Bill. These types of content have since been removed. What do you think of this decision?

The impact of misinformation/disinformation on children is more acute than on adults, in general, because they are less able to spot it, and have less knowledge against which to balance it. At a time when we are, for example, giving 12-15 year olds the ultimate decision about whether to get vaccinated against Covid-19, then misinformation has the potential to be extremely harmful to their physical health; while there are many examples of issues with mental health caused or exacerbated by online content viewed by children. This again reinforces the need to review the scope of the Bill, and to ensure have sight of a draft list of Priority Content to give context in which to consider the Bill's real-life effectiveness.

Are there any types of content omitted from the scope of the Bill that you consider significant e.g. commercial pornography or the promotion of financial scams? How should they be covered if so?

Commercial pornography represents a significant omission from the scope of the Bill. At the time the Bill was initiated, ministers fully expected Part 3 on the Digital Economy Act 2017 to take care of the risks to children, and the indirect impact on women and girls, from the ubiquitous availability of online pornography. These risks are deeply concerning and must be urgently addressed. Each year commercial pornography continues to be unregulated, a new generation of children gain unfettered access to all pornographic content on the internet, no matter how extreme - often featuring violent, non-consensual, and/or unrealistic content that contributes permanently to the formation of children's perceptions of sex and relationships.

We have seen the impact of this on male violence towards women and girls in a recent report eventually published by HM Government in response to the Women and Equalities Committee, if the Committee requires evidence beyond their own instinctive knowledge that our children should not be exposed to this disturbing content a moment longer.[2] (It is worth noting that recent efforts in France to introduce regulation for pornographic websites took the form of a successful amendment to a bill on domestic violence.)

With the government deciding in the summer of 2019 to abandon Part 3 of the Digital Economy Act 2017 ahead of the general election, this Bill also seeks to repeal that legislation. **Ironically, the only mention of 'pornography' in this Bill which the former Secretary of State told the High Court would be an improved replacement for the DEA, is when the word is used to repeal Part 3.**

The former Secretary of State perhaps recognised the difficulty his successor would have in persuading either House to repeal legislation it has waited 4 years to see implemented, with a Bill that does not explicitly address it, when he confirmed to the DCMS Select Committee that he was open to extending the protection offered by the Bill to Children during pre-legislative scrutiny, provided this was congruent with the Bill's approach.

We are proposing, in agreement with all the leading children's charities, church groups and campaigners that the Bill is amended to create a category of services which would be within scope by virtue of containing content harmful to children, irrespective of whether or not they offer user-to-user services.

Scope of the Bill
To (i) user-to-user services and (ii) search engines, Parliament should add:
(iii) all services which include content designated in regulations made by the Secretary of State as **primary priority content** that is harmful to children or **priority content** that is harmful to children (whether or not the services allow for user-to-user functions).
Services in scope under type (iii) will be subject to the same duties as (i) and (ii) already set out in the Bill, including the additional duties applicable if the service is likely to be accessed by children.

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/976730/The_Relationship_between_Pornography_use_and_Harmful_Sexual_Attitudes_and_Behaviours-_literature_review_v1.pdf.

This would ensure that websites which included not only pornographic content, but perhaps also sites dedicated to promoting anorexia ("pro-ana" sites), "Incel" sites and others which might not have any user-generated content but are covering topics that the Secretary of State will be defining as priority content, are still obliged to apply the new duties of care.

The "**Limited functionality services**" exemption should be removed, or not apply to the new type (iii) services we suggest adding to scope.

This is because, as drafted, a porn site which produced all its own porn would be exempt from the Bill. The same logic could apply a site on anorexia that produced its own content. A well-intended exception designed to protect small online retailers may be an Achilles Heel.

What would be a suitable threshold for significant physical or psychological harm, and what would be a suitable way for service providers to determine whether this threshold had been met?

While we are not the most authoritative voice to define a threshold for significant physical or psychological harm, we would like to highlight the fact that any informed answer to the question "what constitutes a significant physical or psychological harm?" requires knowledge of the age of the person who is faced with the potential harm. Content that represents a minor psychological harm for adults may well represent a significant psychological harm for children. Given there exists today technology to determine the age of a user of the internet with a relatively high degree of accuracy, ready to be rolled out across diverse contexts, the omission of specific reference to online age verification technologies (as we are increasingly seeing in various legislation around the world) appears to be a missed opportunity in this draft.

We commend to the Committee the Age Assurance (Minimum Standards) Bill [HL] Bill presented to the House of Lords by Baroness Kidron which the AVPA has fully endorsed, and which might be sensibly incorporated into the Online Safety Bill.

Are the definitions in the draft Bill suitable for service providers to accurately identify and reduce the presence of legal but harmful content, whilst preserving the presence of legitimate content?

As discussed above, limiting the scope of the Bill to sites with user-to-user services creates an enormous loophole.

The draft Bill applies to providers of user-to-user services and search services. Will this achieve the Government's policy aims? Should other types of services be included in the scope of the Bill?

As discussed above, any site likely to be accessed by children should be in scope.

The draft Bill sets a threshold for services to be designated as 'Category 1' services. What threshold would be suitable for this?

This should be a qualitative rather than a purely quantitative threshold.

Services which include content designated in regulations made by the Secretary of State as **primary priority content** that is harmful to children will be subject to the same duties as Category 1 Services, including the additional adult risk assessment duties.

For these harms which are deemed the most serious, it is proportionate to extend the duties placed on the service to include those designed to protect adults as well as children which will apply to the largest global platforms – this measure is to introduce a test of harm as well as simply size in applying these additional requirements.

Will the regulatory approach in the Bill affect competition between different sizes and types of services?

As far as Age Verification is concerned, it is widely available through a highly competitive market, with an ever-growing range of methods, so need not be the preserve of only larger sites. An age check costs pennies not pounds, and need only be completed annually for most low and moderate risk situations, with the same check then re-usable many times over without the need for the user to dig out their passport or take a selfie repeatedly.

Algorithms and user agency

Are there any foreseeable problems that could arise if service providers increased their use of algorithms to fulfil their safety duties? How might the draft Bill address them?

Age estimation is a form of age verification which relies on artificial intelligence to estimate the age range of an online user. This technology is generally developed with machine learning techniques, where computers are given examples of data associated with a user of a known age, and then look for patterns to apply to users of unknown ages.

Any re-drafting of the Bill in this area needs to avoid throwing the baby out with the bathwater, by restricting the ability to use algorithms to estimate age. However, where data is gathered, analysed and stored for the purpose of age estimation, it should not then be used for other purposes without a proper legal basis under GDPR. The ICO is aware of the potential for it to inadvertently limit the use of age estimation if restrictions on the use of data, particularly sensitive personal data, are applied too narrowly. The ICO is taking legal advice on whether the public interest provisions of the Data Protection Act 2018 enable age assurance to be conducted without additional consent which will be published imminently.

Existing UK GDPR is sufficient to protect the privacy and data of users, so there is no obvious need for the Bill to replicate such protective measures. Regulators and auditors will need to remain vigilant that the existing law is observed.

The role of Ofcom

Is Ofcom suitable for and capable of undertaking the role proposed for it in the draft Bill?

We welcome the designation of Ofcom as the regulator, and note that since this was announced, a number of well-regarded experts from across the field of online child

protection have been recruited to join the growing team preparing for this responsibility. We should also put on record their proactive engagement with the AV industry already, well in advance of their role in this field being formalised by the Bill, but we remain concerned about the time required to move from Royal Assent to active enforcement no matter how well-prepared Ofcom is, or what ministers may wish to see as a timetable. Indeed, Ofcom have been clear that their processes cannot be concatenated, and to do so puts them at risk of losing subsequent enforcement cases.

There may be merit in priority elements of the Bill being commenced on an accelerated timetable set out in the body of the legislation, such as urgent needs to address terrorism, CSAM and extreme pornography.

Are Ofcom's powers under the Bill proportionate, whilst remaining sufficient to allow it to carry out its regulatory role? Does Ofcom have sufficient resources to support these powers?

It is important that in protecting the independence of the regulator, there is not the potential for it to choose to ignore the will of Parliament, by either refusing to enforce certain provisions in the law, doing so without speed and energy, or applying inappropriately minor penalties. We have been disappointed that another regulator, the ICO, has not taken any action to protect the widespread abuse of children's data by pornographic websites, for example, even when presented with clear evidence that children access such sites, and that they consistently and obviously process their personal data in order to serve them with even more harmful content. The ICO has argued this is a matter for the new online harms regulator, but given the timescale before this Bill will be enforced is at least 2-3 years, the Commissioner exercising her discretion in this way is a missed opportunity, and leaves the ICO regulating websites selling children's toys more rigorously than those showing the use of sex toys. Such anomalies must not be facilitated by the new Bill's mandate to the regulator.

Finally, but importantly, Ofcom should be given powers (similar to the ICO under Schedule 5, Data Protection Act 2018) to approve certification schemes relevant to demonstrating conformity with the Online Safety Bill, Codes and Guidance issued under it. This was a power which was omitted from the Digital Economy Act, making it difficult for the BBFC to introduce a certification scheme to provide reassurance to the public about data privacy and security, and ultimately leading to criticism from the House of Lords Committee[3].

To facilitate an effective co-regulation approach through the creation of assurance schemes, and independent audit and certification of age verification providers and other suppliers of technology which supports delivery of the Bill's objectives, provision is required in the Bill for Ofcom to approve such schemes if it determines they would be beneficial.

Thank you for the opportunity of contributing to the work of the Committee. We are at your disposal to provide further evidence, in writing or in person.

[3] Thirty-ninth Report of Session 2017–19 - Joint Committee on Statutory Instruments - House of Commons (parliament.uk)

Yours sincerely,

Iain M. Corby

Executive Director
Age Verification Providers Association

About the AVPA

As an association, we work to:

- Inform and educate the public, industry, and media, on age verification solutions and technology.
- Promote a positive image of effective age verification and the age verification industry.
- Represent the industry to regulators and law makers for the advancement of best practice, socially-responsible age verification policy.

The AVPA was formed in 2018 from organisations involved in the UK's Digital Policy Alliance age verification working group, and created and in response to a need for a uniform voice for of the industry.

The AVPA is governed by a representative Board drawn from its member organisations.

22 September 2021