Consultation response form

Your response

About the Internet Watch Foundation:

The Internet Watch Foundation (IWF) is a charity that works in partnership with the internet industry, law enforcement and government to remove (with the co-operation of industry) from the internet child sexual abuse images and videos wherever they are hosted in the world and non-photographic images hosted in the UK. The IWF exists for public benefit and performs two unique functions in the UK:

1. We provide a secure and anonymous place for the public to report suspected online child sexual abuse images and videos and;

2. Use the latest technology to search the internet proactively for child sexual abuse images and videos.

The IWF has a Memorandum of Understanding between the National Police Chiefs' Council (NPCC) and Crown Prosecution Service (CPS) that governs our operations. This ensures immunity from prosecution for our analysts and recognises our role as the "appropriate authority" for the issuing of Notice and Takedown in the UK.

Operationally, the IWF is independent of UK government and law enforcement. The IWF also plays a vital role in providing the internet industry with several quality-assured technical services to prevent the spread of known child sexual abuse images and videos online and to stop the uploading of new images in the first place. These include image hashing utilising Microsoft's PhotoDNA, a URL blocking list of live webpages, keywords list, domain alerts, payment brand alerts, newsgroup alerts and simultaneous alerts (for US companies only). Key to this is our trusted relationship with the internet industry which enables us to act as a broker between them and government and law enforcement.

In 2020, the Independent Inquiry into Child Sexual Abuse (IICSA) concluded: "In the UK, the IWF sits at the heart of the national response to combatting the proliferation of indecent images of children. It is an organisation that deserves to be publicly acknowledged as being a vital part of how, and why, comparatively little child sexual abuse material is hosted in the UK."

Our work is funded almost entirely by the internet industry: 60% of our funding comes from our 200 global members which include providers of user-to-user services, search providers, Internet Service Providers (ISPs), Mobile Network Operators and manufacturers (MNOs), social media platforms, safety tech providers, content service providers, telecommunications companies, software providers, domain name registries and registrars and those that join the IWF for CSR reasons.

Our members include some of the biggest companies in the world – Amazon, Apple, Google, Meta, Microsoft, Snap, X (formerly Twitter), and Discord. We also have the largest ISPs and mobile operators in the UK (BT, Talk-Talk, Sky, Virgin Media, the Internet Service Providers Association) and some of the smaller operators within the internet ecosystem who pay as little as £1,040 per annum yet are still able to access all the technical services and tools we have to offer.

The IWF is a charity registered in England & Wales with an 11-person Board of Trustees of which, eight are independent members and three are industry representatives. The IWF Hotline is audited by an independent team, led by a High Court judge, every two years and the report published in full.

Overview-

The Internet Watch Foundation recognises the enormity of the challenge that Ofcom faces in delivering effective regulation that will meet the Government and Parliament's expectations of "making the UK the safest place in the world to go online" and improving the online experiences of UK users.

Ofcom deserves enormous credit and praise for bringing forward its consultation on the illegal content codes so soon after Royal Assent. It has clearly been recruiting expertise from across the online safety sector, technology companies, and civil society that has resulted in the development of a stellar evidence base of how illegal content is manifesting online; particularly in relation to CSE/A.

We also believe it is important to highlight that the UK already leads the world in its response to online harms and CSE/A and want to see these mechanisms built on and enhanced further if we are to truly achieve the aims and ambitions of the Online Safety Act.

There are already effective mechanisms for dealing with child sexual abuse with the Independent Inquiry into Child Sexual Abuse recognising:

"In the UK, the IWF sits at the heart of the national response to combatting the proliferation of indecent images of children. It is an organisation which deserves to be publicly acknowledged as a vital part of how, and why, comparatively little child sexual abuse is hosted in the UK."[1]

INHOPE's inspection of the IWF also concluded that "*not only do we operate to an exceptionally high standard in the UK but its operations and structure in many ways set the standard for other hotlines around the world."*

We have been delighted to play our part in assisting Ofcom by providing evidence in the development of this first iteration of the illegal content codes of practice and we offer our response to this consultation with a view to helping to further strengthen its evidence base and ensure that we are doing everything we possibly can to better protect children online.

If we get this approach right, we believe we have an opportunity to make great strides forward in our vision for an internet free from child sexual abuse.

Our consultation response focuses on the following issues:

1. The need to **simplify** the "consultations at a glance proposal" and **signpost** to organisations who can assist with compliance so small and medium sized business are clear on their obligations.

[1] Independent Inquiry into Child Sexual Abuse: Internet Inquiry Point 29, Page 33 https://webarchive.nationalarchives.gov.uk/ukgwa/20221215030740/https://www.iicsa.org.uk/key-documents/17805/view/internet-investigation-report-march-2020.pdf

2. Ensure a **balanced and proportionate approach** to private communications and End-to-End Encryption that enables **better protection for children** in these environments.
3. Ensure the Code of Practice retains its current measures to tackle CSE/A; **adds Key-word detection** as a tool for CSEA provisions based on evidence already gathered for search mitigation for CSE/A and its recommendation for Fraud, includes measures to tackle the **detection of new Child Sexual Exploitation and Abuse Material**; ensures grooming measures are reliant on **Age Verification**; ensures organisations supporting the delivery of **datasets** to services in scope are well supported; and the **roadmap is updated** to include when future iterations of Codes are expected.
4. **Risk Assessment-** ensure that the regulation focuses on **small but high-risk** platforms; ensure that Ofcom's approach to risk assessment does not just include "large" platforms where a lot of best practice currently exists; extend requirements to train staff in content moderation to **medium sized companies**. **Review the approach to the definition of "large platforms"**, the regulation will likely not capture some of the most popular platforms used by children and **ensure that medium sized businesses are also in scope of training and development requirements for staff.**
5. **Illegal content judgments guidance-** focuses heavily on takedown measures; should be much more focussed at ensuring the content doesn't get there in the first place.
6. **Focus on evidence, emerging harms, future proofing, costs to society vs costs to business.**

   Ofcom has done an excellent job of evidencing harms and their high cost both financially and emotionally to victims and society in Volume 2 of the consultation, but this then feels disconnected from Volume 4 where the focus shifts dramatically to the costs to businesses we believe, somewhat disproportionately. **We recommend that Volume 4 is refocussed with the rights of victims, children and the damage illegal harms cause to society in mind**.

   On **emerging harms, we believe the evidence base is missing further detail on the impact of Generative AI and Extended Reality Technologies**, which are here and now problems, and, in the future, there will be the **impacts of quantum computing** which may already be impacting business decisions of services in scope.

   Finally, we **believe that Ofcom is somewhat constrained in its recommendations based on its requirement for a strong evidence base**. We would like to see a much more pragmatic, precautionary approach to regulation that focusses more on safety by design in the longer term.

Recommendations-

1. **Simplify the 'consultation at a glance' proposals and effective signposting of organisations which can help with compliance-**

This consultation is incredibly detailed, long, and complex and has been a real challenge for organisations with dedicated policy teams and lawyers to respond to. A consultation that people cannot easily understand or take weeks to comprehend is not consultation.

Whilst Ofcom has heavily invested in engaging with the online safety community and companies to explain the consultation, we fear that this will not be enough and much more thought needs to be given to simplify the complexity of this document. Our concern is that small to medium sized businesses in scope of the Online Safety Act, who don't have access to this sort of expertise, need much clearer guidance and assistance in understanding what they are required to do in order to comply with the Act and effective signposting to organisations like ourselves, which can help them to comply with the measures proposed in Volume 4 (the illegal content code of practice).

At the Internet Watch Foundation, we know that we potentially have an extremely important role to play in assisting the industry with compliance through the provision of datasets, namely hashes and URLs. We stand ready to support the industry in the provision of our Hash and URL lists to services in scope as set out by expectations outlined in the Code of Practice.

We believe Ofcom should be signposting services in scope of the legislation to dataset providers who can assist them with compliance. Whilst we recognise Ofcom must be careful in designating certain providers of services, we believe they could consider some form of accreditation for technological solutions based on high quality data provided by organisations like the IWF.

Other suggestions could be to harness best practice from other regulated sectors. For example, in schooling, Ofsted, the independent regulator, cannot direct schools to take certain measures, it is only responsible for inspecting the effectiveness of measures, but it does sign post schools to measures that might help them to meet their regulatory obligations.

A good example of this is the objective Ofsted has set of schools to improve school attendance. In a recent blog on the Department of Education website, Ofsted highlights best practice and resources to assist improved performance, including signposting to schemes run by third sector providers, like Barnardo's.

2. **<u>Ensure a balanced and proportionate approach to private communications and End-to-End Encryption that better protects children and respects victims' rights to privacy-</u>**

We are pleased to see acknowledgement within Volume 2 (the causes and impacts of online harm) that End-to-End Encryption (E2EE) has been recognised as a functionality which poses particular risks, particularly in relation to enabling perpetrators to spread child sexual abuse material, with a reduced risk of detection.

This is well supported by a clear evidence base borne out of police recorded crime statistics[2], and research from the NSPCC has demonstrated that grooming is increasingly becoming a cross-platform harm, with 70 different apps or gaming providers involved in grooming crimes in the year 2021/22 alone.[3] The experiences of victims of these crimes, and the court cases of prolific offenders such as David Wilson also support the significant risk E2EE poses. If Facebook Messenger had been End-to-End Encrypted, it is highly probable that Wilson would have evaded detection and the 500 boys he messaged and the 51 boys he coerced into sending indecent images of themselves, would have highly likely never been safeguarded.

We urge Ofcom to retain this as a specific risk factor, when finalising the response to this consultation.

[2] NSPCC Freedom of Information request shows Meta owned apps including Facebook, Instagram and WhatsApp were used in a quarter of offences where the platform was identified by Police.

[3] https://www.nspcc.org.uk/about-us/news-opinion/2022/online-grooming-crimes-rise/

We are also pleased to see that Ofcom has proposed several "service design mitigations" that apply to both services at high risk of grooming and all large user-to-user services which have a medium risk of grooming, applying to all users under the age of 18.

However, the 10 mitigations proposed on pages 229 and 230 of Volume 4 (the illegal content codes), are absent from their applicability to providers of private communications and end-to-end encrypted services in the "consultations at a glance" summary document.

We would recommend that Ofcom amends its "consultation at a glance" documentation to make it clear that the grooming "safety by design" measures apply equally to providers of user-to-user services, those offering private communications, and end-to-end encrypted services.

We recognise that due to the constraints contained within the Online Safety Act itself under Section 231 of the Act (Proactive Technology) and Schedule 4, Section 13 (4), that any measures proposed by Ofcom:

"*May not recommend the use of technology to analyse user generated content communicated privately, or metadata relating to user generated content that has been communicated privately.*"

We therefore understand that other technical mitigations focussed on the detection of content have not been specifically recommended for private communications. This includes Image Hashing and URL blocking, proposed in Volume 4 (Codes of Practice).

However, we would like to challenge the assumption that appears to have been made that End-to-End Encrypted platforms seem to be out of the scope of automated content moderation requirements on the basis that they are "private".

We believe, this is in direct contradiction to the significant evidence base Ofcom has compiled in Volume 2, which states that End-to-End Encryption is a clear risk factor, particularly in relation to child sexual abuse.

We believe there is a current gap in Ofcom's guidance for providers of private communications services in achieving the Act's aims and objectives. Whilst we recognise that Automated Content Moderation cannot be recommended, **more can and must be done to provide advice and guidance on how private messaging services can be safely designed for children with a greater focus on the delicate balance of rights.**

The right to privacy is not an absolute right and the interplay between privacy and safety is complex.

We believe it is important to balance the approach to Human Rights in this context. The Online Safety Act requires Ofcom to consider freedom of expression (Article 10 of the ECHR) and privacy (Article 8 ECHR), but they are not the only relevant rights as Ofcom notes.

We particularly want to focus our response on Article 8 and Article 3 of the European Convention on Human Rights and Article 19 of the UN Convention on the Rights of the Child.

Article 8 of the European Convention on Human Rights states:

"1. Everyone has the right to respect for his private and family life, his home, and his correspondence."

But it also importantly states:

"2. There shall be no interference by a public authority with the exercise of this right ***except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic wellbeing of the country, for the preservation of disorder or crime, for the protection of health or morals, or the protection of rights and freedoms of others."***

It is therefore important to remember that the right to privacy is a qualified right and not an absolute right. Under Article 3 obligations it states:

"No one shall be subject to torture or to inhumane or degrading treatment or punishment."

Article 19 on the UN Convention on the Rights of the Child states:

"*State parties will take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or* ***exploitation including sexual abuse*** *while in the care of parent(s) or legal guardian(s) or any other person who has the care of a child*."

It is also important to highlight that not only do these obligations apply to state parties when drafting and passing legislation, but these principles also apply to the implementation of such measures.

We urge Ofcom to think carefully about the consequences of designating End-to-End Encrypted services as private communications providers. Such a judgment may have long term unintended consequences which may mean that social media networking sites move towards services they provide to End-to-End Encryption to be classified as "private" either to avoid their obligations under the Act or avoid costly content moderation costs.

Schedule 4, Paragraph 13 (6), requires Ofcom to:

"*Have regard to the degree of accuracy, effectiveness and lack of bias achieved by the accuracy of the technology in question*".

We have seen Ofcom successfully detail how Hash Matching and URL blocking meet these requirements, however, it would also be helpful for Ofcom to take a similar approach to technologies it is going to recommend as part of its enforcement action (yet to be developed) in respect of Section 122 of the Bill, Use of Technology Notices.

We would like to point out that no technology can ever achieve a 100% level of accuracy, so Ofcom must also set realistic, proportionate expectations on the level of accuracy of technologies- we should not let perfection become the enemy of better protections from the spread of illegal content online. We also believe that it is right that Ofcom sets the challenge to companies that where the technology does not currently exist, companies are required to think about developing technologies that do require them to meet the Act's aims and objectives. If the power exists in the legislation, Ofcom must be thinking of ways it can be utilised and services must have means to comply with the obligation.

There are several examples where large technology platforms in scope of this regulation are already using client-side scanning in technical solutions, which they claim do not break encryption or violate privacy rights. Perhaps the best example of this is Instagram's recently announced protections for minors, which enables teenagers to turn on a control which blurs photos of nudity. This is also very similar to the solution Apple has adopted. However, we believe there is scope to go further, based on the expanded protections for child protection Apple announced in August 2021, which they stated in the FAQs had the support of both privacy and child protection organisations. Whilst we recognise Ofcom cannot mandate proactive technology in private messaging it should be encouraging organisations that are within the scope of this regulation to develop technology and systems and process that help to achieve the Act's aims and objectives.

To that end, we would urge Ofcom to discuss with companies as part of the supervision process, what steps they are taking to explore the potential solutions outlined in the technical paper written by Ian Levy and Crispin Robinson, two of the world's leading cryptographers.

We would urge Ofcom to make a public statement that confirms they are exploring Section 122 as one of the enforcement powers it will be seeking to use.

We would request that Ofcom use its evidence gathering powers to ask about developments companies like Apple and Meta have been pursuing so that they can be evaluated.

Ideally, we would like to see further consultation from Ofcom as part of their obligations under Schedule 4, section 13 (6) to define what technologies it is considering as effective to enforce Section 122 of the Bill.

3. **The definitions of content communicated publicly and privately-**

Linked to End-to-End Encryption and private communications, we believe it is important that much clearer guidance is issued around content that is defined as being communicated publicly or privately. Ofcom has covered this as part of its guidance in this consultation under Appendix 9.

Section 232 of the Online Safety Act sets out three statutory obligations for companies to consider which include:

"*How many people from the UK can access the content; restrictions on who may access the content; and the ease at which the content may be shared*."

The guidance in Appendix 9, point A9.14, sets out several User-to-User (U2U) services that would be outside the scope of the proactive technology measures in the codes of practice. This includes email, MMS, SMS, one-to-one aural communications, comments, and reviews on provider content, identifying content that accompanies anyone of these and news publisher content.

We are concerned that a blanket removal of services from the scope of obligations in the code, may result in confusion for services and may lead to services removing the protections they are currently deploying in these services on a voluntary basis.

We would ask that Ofcom amends its guidance to clarify that services would be able to continue using automated content moderation on a voluntary basis but would not be compelled to do so as a result of regulation.

We are also concerned with how Annex 9 of this consultation interacts with previously published guidance from the then Department for Digital, Culture, Media and Sport on 29 June 2021, which sets out "practical steps" that can be taken to improve the safety of your online platform which recommends automated content detection and highlights child sexual abuse and exploitation as a specific harm that could occur in a private messaging environment.

We also need to ensure that content does not migrate from open areas of the internet to channels where the detection of this content becomes more complex and complicated.

As Ofcom makes clear in Appendix 9; content that is initially circulated “privately” may well become “publicly” communicated at some point in the future.

There is a very complicated interplay between content that may have been at first been communicated privately, but then becomes publicly available. This of particular relevance when we consider the explosion of self-generated child sexual abuse imagery, which of course could have been shared between two teenagers, but then leaks when a relationship breaks down and others gain access to that content. This issue has not been fully explored in Appendix 9. The communication of the material publicly may not even be circulated through online service providers- a child’s nude images could be “capped” (or screenshotted), printed, and shared around a school for example.

Other considerations should include, for example, at what point does a group within a platform that is defined to be “private” such as WhatsApp, Telegram, or Signal, all of which are end-to-end encrypted, cross the threshold of circulating content in a “publicly” available way? How many users must be part of a group? How many times does content have to be circulated or onwardly shared before it is defined as having been communicated “publicly”? How should we tackle “pile-ons” of sexual abusers rushing a live stream of a teenager in their bedroom pressuring them into carrying out sexual activity on themselves and capturing that for further onward distribution online?

Linked to the point on end-to-end encrypted communications already raised in the consultation response, we are also concerned about the assumption that seems to have been made that End-to-End Encrypted services are considered by default to be “private communications.”

Whilst we recognise the pragmatic approach Ofcom has tried to take, **we urge Ofcom to think more carefully about what point a threshold is crossed from when a piece of content ceases to be considered “private” and has been “publicly” shared. Ofcom should also consider the rights of victims and children much more carefully in the context of its assessment on Human Rights and Privacy. It should carefully apply the principles of Article 8 and 3 of the European Court of Human Rights and Article 19 of the UN Convention on the Rights of the Child in its guidance- neither of these are specifically referenced in Appendix 9.**

4. **Code of Practice-**

Positive aspects of Ofcom’s proposals:

We are pleased to see that in Volume 4 (the illegal content codes of practice), Ofcom has recommended as part of its proposals around automated content moderation (ACM), hash-matching and URL detection for previously identified child sexual abuse material as part of the obligations.

These measures will be extended to some of the riskiest providers where the thresholds of UK monthly users have been lowered to 700,000 for those at high risk of image based CSAM in their risk assessment and 70,000 UK users for file hosting and storage sites.

For providers of search services, the draft code of practice also recommends search warnings and the deindexing of URLs known to be displaying child sexual abuse material. As is stated in Volume 4, we know from evidence from the National Crime Agency and our own work, that CSE/A content is readily available through providers of large search services in just three clicks.

Ofcom has also recommended ten safety-by-design measures which apply to all users below the age of 18, that have functionalities which put them at medium to high risk of grooming.

The IWF is pleased to see that the proposals in the draft code of practice proposes both a mix of safety by design measures and proactive technologies to tackle both grooming and the dissemination of known child sexual abuse material on services in scope. We urge Ofcom to retain these measures in the final versions of the Codes of Practice and we provide further evidence below that further demonstrates the effectiveness of the measures proposed.

Evidence we have gathered that supports this proposal:

Image hosting sites and cyberlockers continue to be where the IWF removes most of its child sexual abuse content, which supports Ofcom's proposal for lower thresholds for providers where we know the problem is more acute.

(CONFIDENTIAL✂)

INHOPE's 2022 annual report also suggested that Image Hosts had been responsible for a 38% increase in child sexual abuse material distribution. Whilst their report also acknowledges that reports from file hosters had dropped from 26% of CSAM in 2021 to 6% in 2022, they attributed this drop in the difficulty in accessing and reporting premium level accounts on file hosting platforms as both a citizen and hotline analyst, demonstrating that detecting this content is becoming more complex, and hence the need in our opinion for more proactive measures.

The evidence base supports the fact both of these measures are extremely effective at dealing with the issue of known (previously detected) child sexual abuse material.

Effectiveness of webpage (URL) blocking:

In April 2020, during the first month of the Covid-19 pandemic, the IWF alongside just three of its industry members released data which stated that URL blocking had prevented 8.8 million attempts from UK users to access webpages on our blocking list.

In February 2024, one of our members, Converge, who are a fibre broadband and technology provider announced they had blocked almost 12 billion entry attempts to illegal websites, which they stated was a 400% increase on the 1.9 billion attempted entries from the previous year. They, in part, attributed this rise into them adding 198,000 URLs and domains associated with illegal activities, including through its partnership with the Internet Watch Foundation.

Effectiveness of Perceptual Hash Matching:

We believe that the comprehensive evidence base that Ofcom has gathered in respect of the scale of child sexual abuse demonstrates in large part, the effectiveness of Photo DNA and hash matching technologies. The sheer volume of reports to the National Center for Missing and Exploited Children demonstrates hash matching measures accompanied with other industry best practice are extremely effective in detecting child sexual abuse and exploitation content.

(CONFIDENTIAL✂)

Effectiveness of proposals for Search mitigation (warning messages and deindexing CSAM):

A report led by Joel Scanlon of the University of Tasmania published in February 2024, reviewed the effectiveness of the project reThink chatbot a partnership between the Internet Watch Foundation, the Lucy Faithful Foundation and Aylo (the owner of the pornographic website Pornhub). The chatbot has been functional on the Pornhub website in the UK since March 2022 and data was collected until September 2023. This chatbot built on the already successful deterrence messaging campaigns that had been operational on the site since March 2021, directing potential offenders to seek help from the Lucy Faithful Foundation.

The key findings during this evaluation period concluded that 99.8% sessions did not result in any triggering of the chatbot, but that still led to the chatbot being displayed 2.8 million times between March 2022 and August 2023, resulting in 1,656 requests for more information from the Stop It Now services; 490 click throughs to the Stop It Now website, and approximately 68 calls to the anonymous counselling service.

Prior to the launch of the chatbot, warning messages about potential offending behaviour were displayed over 2 million times; with warning messages being triggered over 4.4 million times during the evaluation period.

The report concludes several successful outcomes; there was a significant statistical decrease in the number of searches for CSAM on Pornhub UK; most sessions which triggered the chatbot only did it once; and sessions which did start with the first action being to search for CSAM, did continue to use the site, searched less frequently for CSAM than in sessions where warning messages weren't displayed.

Gaps in Ofcom's current proposals:

Lack of ambition:

We recognise that the draft codes of practice represent a first step in the regulatory journey, but we are disappointed by the lack of ambition contained within the codes. We are concerned that this gets the new regulatory regime off on the wrong footing from the get-go and sends the wrong message to companies in scope, that instead of stretching the limits of what is possible, the approach from Ofcom has been far too safe and risks being perceived as a lack of ambition, by NGOs, the public, and even the politicians who have all lobbied so hard for the legislation.

The Government has continually boasted that this is "world leading legislation" that will "make the UK the safest place in the world to go online." These commitments were first made in the Conservative Party's 2017 manifesto[4], with other measures such as Age Verification to tackle the problem of children accessing inappropriate content such as pornography, being first promised as far back as 2015[5].

A whole generation of parents and children have been promised a safer internet for almost the best part of a decade. Whilst we recognise that the passage of the Act was not in the control of Ofcom, we do believe that there was sufficient time to prepare a more ambitious approach to the codes of practice, particularly for CSEA based on the remarks of its Chief Executive.

[4] Conservative Party Manifesto (2017) Page 77
[5] Conservative Party Manifesto (2015) Page 35

In a letter to Peers dated 17 April 2023, Ofcom's Chief Executive stated in a section entitled: *Phase one, illegal harms codes and including tackling child sexual abuse*:

"We can move very quickly here because this part of the Bill has remained unchanged for quite some time and illegal harms are defined by existing law. The Government's and Parliament's intentions about what they want platforms to achieve are clear."

In a press release heralding the Act's Royal Assent in October 2023, further clarity is provided on what the Government's expectations were:

"The new laws take a zero-tolerance approach to protecting children from online harm."

"The Act places legal responsibility on companies to prevent and remove illegal content."

It also carries quotes from the then Home Secretary, Suella Braverman, who states:

"This landmark law sends a clear message to criminals, whether it's on our streets, behind closed doors or on far flung corners of the internet, there will be no hiding place for their vile crimes.

"Social Media companies will be held to account for the appalling scale of child sexual abuse occurring on their platforms and children will be safer. We are determined to combat the evil of child sexual abuse wherever it is found, and this Act is a big step forward."

Returning to Ofcom's preparations for the impending regulation, Ofcom's Chief Executive's letter to Peers references it was *"well advanced in gathering the necessary evidence, drivers of risk, and the systems and processes available to services to address them."*

The letter also states that at that stage, 104 bilateral teach-ins and roundtables had been held with "extensive" industry engagement. It is therefore disappointing that so much industry best practice appears to have been missed in Ofcom's proposals in the illegal content codes.

We don't believe that the proposals in their current form go far enough or help the Government or Parliament deliver on its promises of a safer internet or our mission of an internet free from child sexual abuse.

Despite this criticism, we do understand there is a need to balance the speed of getting the consultation out in order to ensure that Ofcom complies with Section 43 (11) of the Act which requires Ofcom to submit draft Codes of Practice to the Secretary of State within 18 months of Royal Assent. However, it is clear through conversations both bilaterally and with wider stakeholders that this requirement for speed appears to have been at the expense of getting everything right first time - resulting in gaps.

We also recognise that Ofcom only gained its information gathering powers on 10 January and has been clear in statements made by its senior leadership team that this will be key to further developing the required evidence base for future mitigations.

We believe there are two potential remedies to this approach:

Firstly, we would like to see a couple of fixes to the current codes.

- **We believe that the detection of new child sexual abuse using classifier technology should be recommended as a mitigation immediately**. Its omission is a major oversight, and we know that many of the large services in scope of this regulation are already doing this.

- Secondly, **we would like to see Age Verification measures also added to the grooming mitigations to strengthen their effectiveness immediately**. It is no good recommending safety by design measures for children's accounts if this relies on self-declaration of age that can be easily circumvented, and Ofcom is already consulting on Age Assurance as part of its Part 5 obligations under the Act.
- Finally, **we believe that Ofcom should also be recommending the use of keyword databases for both User-to-User and Search Services, making the most of all available services offered by organisations like IWF**. Keyword detection has also been recommended by Ofcom as a mitigation for fraud, so as a technology, it should be easy to demonstrate that it meets all of the criteria required under the accuracy, effectiveness and freedom of bias requirements.

The second remedial action that can be taken is for **Ofcom to publish an update to its roadmap on when further iterations of the CSE/A Code can be expected**.

We are concerned that if Ofcom continues with its current timetable for implementation the full extent of the regime will not be operational until 2026/27 financial year and we know that there could also be further significant delays with the passage of the secondary legislation that is required with the anticipated General Election which is anticipated to take place in the Autumn of 2024. It is vitally important that further measures to protect children from child sexual abuse are brought forward at the earliest opportunity.

Detection of new Child Sexual Abuse Material:

We are disappointed that Ofcom has chosen not to recommend any measures focussed on the detection of child sexual abuse material that has not previously been identified.

We fear that this sets the regulatory bar too low for a first draft of a code of practice, and many companies within the scope of the regulation are in fact already using classifier technology to detect child sexual abuse material that has not previously been identified and grooming approaches. We do not believe that it is acceptable for this important measure to be left to future iterations of the Codes of Practice based on a lack of available evidence if it is already established best practice within the industry.

Ofcom justifies this decision in Volume 4 on page 8, point 11.15 stating:

"We do not yet have the evidence base to set out clear proposals regarding the deployment of such technologies such as machine learning or artificial intelligence to detect previously unknown content at this time. As our knowledge base develops, we will consider other recommendations on automated content classification in future iterations of our codes."

This is despite the fact this technology has been widely deployed by some of the major platforms in the scope of this regulation and in some cases for quite some time.

In October 2018, Meta's Global Head of Safety, Antigone Davis announced in a blog post that Meta (then Facebook), was investing in new technology to fight child exploitation.

The blog states: "*In addition to photo matching technology, we're using artificial intelligence and machine learning to proactively detect child nudity and previously unknown child exploitative content when it is uploaded. We're using this and other technology to more quickly identify this content and report it to NCMEC and also to find accounts that engage in potentially inappropriate interactions with children on Facebook so that we can remove them and prevent harm."*

Google has published a blog post in partnership with the National Center for Missing and Exploited Children (NCMEC) about how its hash matching API is helping them to de-duplicate reports, improve analysts welfare by not viewing content that has already been identified and therefore prioritising images that have never been seen before. Google also has a content safety API which is used on static images and previously unseen content and helps organisations classify and prioritise potential abuse content for review. According to their website, the API had been used by partner organisations to classify over 6 billion images.

In October 2023, Microsoft published a paper about the possibility of metadata-based detection of child sexual abuse material as a possible response to stemming the rising tide of new child sexual abuse material online. The paper proposed a CSAM detection framework consisting of machine learning tools trained on file paths extracted from a real-world data set of over 1 million file paths obtained in criminal investigations. The paper also boasts accuracies as high as 0.97 while presenting stable behaviour from adversarial attacks previously used in natural language tasks. When evaluating the model on publicly available file paths from common crawl data, they observed a false positive rate of just 0.002, showing the model operating in distinct data distributions maintains low false positive rates.

As far back as 2015, research was being carried out which looked at potential mitigations for grooming using Artificial Intelligence and Machine Learning. A study by Maxime Meyer from the University of Upsalla researched a two-step approach to differentiating adults who were posing as children from real children. The process involved analysing text-based analysis of conversations from all those individuals who had self-identified as children. The report concluded there was a strong evidence base to suggest that it was possible to identify adults who are pretending to be children from actual children and could be used to inform children about the true age of the children they are communicating with.

In January 2020, Microsoft announced it was launching a free tool, project Artemis, which aimed to identify predators who groom children for abuse in online chats.

Lack of age verification to accompany grooming mitigations:

We are concerned that the grooming mitigations proposed on page 229 and 230 of volume 4 currently rely on the self-declaration of age and are therefore extremely easily circumvented by children, by simply lying about their age upon registration.

Whilst we recognise that Ofcom will be dealing with the issue of Age Verification through the next “protection of children” code expected in a couple of months, we don’t believe it makes sense to make recommendations which will claim to have such an impact on the scale of grooming that can be so easily circumvented, particularly because there is such a well established Age Verification industry and Ofcom are currently consulting on Age Assurance measures as part of the Part 5 provisions under the implementation of the Online Safety Act.

We recommend Ofcom introduces Age Verification measures alongside the Grooming measures, to improve their effectiveness.

Safety by design approach:

We also recognise concerns that have been raised about whether the codes have been developed in line with expectations of Government and Peers in the scrutiny of the Bill in the House of Lords.

In a debate in the House of Lords during the passage of the Bill, Lord Parkinson, the Government Minister for the Bill said:

"*The Government have always been clear that the way in which a service is designed and operated including its features and functionalities, can have a significant impact on the risk of harm to a user. That is why the Bill specifically requires providers to ensure their services are safe by design and to address the risks that arise from their features and functionalities.*"

He continued: "*We have tabled new clause 1, which makes it clear that duties on providers are aimed at ensuring services are safe by design. It also highlights obligations on services to extend the design and operation of the service*."

The Government's Online Harms White Paper also places an emphasis on safety by design. In their White Paper response in December 2020 the Government said:

"*Our proposed safety by design framework will set out clear principles and practical guidance on how companies can design safer online products and services.*"[6]

The White Paper also makes clear that the safety by design approach will also apply to all services equally. It states:

"*The Safety by Design framework will be an important step in ensuring that all companies, especially small businesses are equipped with the know-how to effectively embed safety by design of their online products and services, to help minimise the regulatory burdens in the fulfilment of the duty of care.*"[7]

There are international examples of best practice which can be drawn upon when it comes to embedding safety by design. The Australian e-safety commissioner has produced principles, an easy assessment tool for services, resources for investors and financial entities and guidance to the tertiary sector on how to engage all of the relevant constituent parts of a safety-by-design process and we would encourage Ofcom to consider a similar approach to the UK regulation.

Whilst there is some evidence to safety-by-design principles for example, with Grooming mitigations proposed in Ofcom's code of practice, these measures are currently reserved for the largest platforms or those at medium to high risk of CSAM.

We believe that it is a missed opportunity to build on the successes of the implementation of the Age-Appropriate Design Code to ensure that platform have safety "hard wired" in at the start, rather than constantly having to retrofit solutions to illegal content spreading on their platforms.

Provision of data sets to companies in scope of the regulation:

[6] Point 41, page 13, Government's Online Safety White Paper Full Response, December 2020. https://assets.publishing.service.gov.uk/media/5fd8af718fa8f54d5f67a81e/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf

[7] Page 33-34, Government's Online Safety White Paper Full Response, December 2020 https://assets.publishing.service.gov.uk/media/5fd8af718fa8f54d5f67a81e/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf

On several occasions in the consultation document, Ofcom has raised concerns over "*the capacity of database providers*" and "*ensuring that thresholds in guidance remain appropriate*" (Page 90, Page 113 Volume 4).

It has been continuously argued during the passage of the legislation that organisations like the IWF would be vital to the success of the aims and objectives of the regime, yet, formal recognition and agreement on how we help to deliver the regime remains lacking.

It is disappointing to see that this expertise has not been supported, so that concerns over the capacity of providers like us could be addressed before they become potential issues, when services begin to approach us. Whilst we recognise some of that responsibility sits with us and industry, Government Ministers, MPs, and Peers had been clear in their expectations of the involvement and expertise we bring to the effective delivery of the regime.

Speaking at Committee Stage in the House of Lords, Government Minister, Lord Parkinson said:

"There are a number of expert organisations that could play a role in the future regulatory framework, given their significant experience and expertise on the complex and important issue of tackling online child sexual exploitation and abuse. ***This includes the Internet Watch Foundation, which plays a pivotal role in the detection and removal of child sexual abuse material and provides vital tools to support its members to detect this abhorrent content.*** *"*[8]

The former DCMS Secretary of State, Baroness Morgan also stated at Committee stage:

"*We have a world-leading organisation in the form of the Internet Watch Foundation which plays an internationally respected role in tackling child sexual abuse. Any delay in establishing the role and responsibility of an expert organisation such as the IWF, risks leaving a vacuum which is a risk to children.*"[9]

Baroness Kidron was equally unequivocal:

"*When it comes to the IWF, nothing should be left to chance. No warm words or good intentions replace the requirement for its work to be seamlessly and formally integrated into the Online Safety Bill.*"[10]

In one sense, the work of the IWF has been seamlessly integrated into the Bill and its guidance through the recommendation made by Ofcom in this consultation of the inclusion of image hash lists, webpage blocking lists, and the mitigations proposed around search services. However, formally agreement on a public facing MoU with Ofcom has taken over 18 months to negotiate and still isn't in place at the time of responding to this consultation.

We believe will play an important role in delivering the regime because we are the only organisation that provides both an Image Hash list and webpage (URL) blocking list that comply to UK law standards. These lists are high quality, reviewed daily, and recognised as a trusted data

[8] House of Lords Hansard, 16 May 2023, Online Safety Bill, Committee Stage: https://hansard.parliament.uk/lords/2023-05-16/debates/545F4702-E05A-4C12-88A4-9CDD70C115BD/OnlineSafetyBill column 219

[9] House of Lords Hansard, 16 May 2023, Online Safety Bill, Committee Stage: https://hansard.parliament.uk/lords/2023-05-16/debates/545F4702-E05A-4C12-88A4-9CDD70C115BD/OnlineSafetyBill column 226

[10] House of Lords Hansard, 16 May 2023, Online Safety Bill, Committee Stage: https://hansard.parliament.uk/lords/2023-05-16/debates/545F4702-E05A-4C12-88A4-9CDD70C115BD/OnlineSafetyBill column 225

source by our industry members. No other organisation, we believe, offers a webpage blocking list to the same standard of accuracy or an image hash list that has the same level of quality.

It is also important to recognise that there are several potential barriers to scalability of Hashing and URL solutions, which we believe Ofcom will need to resolve through dialogue with organisations like the IWF and other regulatory bodies such as the Information Commissioner's Office and Government Departments.

Firstly, Hashes are considered pseudonymised personal data by the ICO[11], this is because they consider despite the extremely small possibility a hash can be reverse engineered, the fact it could be and could therefore lead to the identification of a person, hashes must be treated in the same way under GDPR as other personally identifiable information.

Secondly, whilst we are supportive of the aims of the regulation to broaden the number of services taking hashes and webpage blocking lists, it is essential that an element of due diligence remains in place for service providers like us. Access to our hash list, URL list and keywords list are currently tightly controlled through strict contractual arrangements which set out how these services may be deployed in accordance with current laws including GDPR. We also conduct strict due diligence checks on companies and individuals wishing to join the IWF as members and take services. We are currently considering what changes we could make to our processes to enable the greater level of demand that is likely to come our way for services and would welcome further engagement from Ofcom and the ICO on these issues.

Finally, there are also costs attached to scaling these services, with uncertainty about the number of organisations that may be creating demand for services. Many of the services directly within scope of the Hashing proposals are likely to be small to medium size file hosting services in the immediate future, which will not generate huge amounts of revenue for the IWF under our current business model and structure, but potentially generate a huge amount of work in due diligence and legal contractual work and obligations as well as monitoring and compliance to ensure that the services are being used appropriately in line with contractual obligations.

We recommend that Ofcom agrees its proposed Memorandum of Understanding with the IWF as soon as possible.

We also recommend that organisations like us are supported to scale by both industry and Ofcom to help achieve the regulatory aims of the regime in terms of the provision of vital services, without this support, the regulation will struggle to achieve its full impact.

Safe Harbor Provision:

Our final comment on the Code of Practice concerns about how they may be interpreted. Some statements in the Code of Practice suggest industry may go beyond their obligations recommended in this consultation, but at present there is nothing requiring them to do so.

On page 8 of Volume 4, point 11.17 it states:

[11] Information Commissioner's Office: Anonymisation: Managing data protection risk, Code of Practice https://ico.org.uk/media/1061/anonymisation-code.pdf Page 79

"Reflecting current best practice, many services may adopt further measures beyond those set out in the codes of practice to protect users against sources of risk that they identify in their risk assessment."

Rather than making this a voluntary measure that companies could take, **we recommend that Ofcom adds to the Code of Practice a requirement on all services in scope to address harms that arise from their risk assessment that are a result of features and functionalities based on best practice, for which Ofcom might not have yet established an evidence base to recommend**. This could be another way of implementing measures to address the detection of CSAM content which has not already been identified, for example, and will also have the added benefit of ensuring the services do not roll back on current best practice through fear of non-compliance- they could use the justification of managing the risk identified in their risk assessment. It could also be an important tool in enabling companies to innovate in response to risks they identify and could also be a positive development in terms of the regulation of new technologies such as Generative AI and Extended Reality technologies and help to future proof the regulation.

The Online Safety Act itself also contains a provision (Section 49) which gives services "safe harbor" from measures contained within the Code of Practice. Services do not need to follow measures contained in the code, provided they can demonstrate alternative measures to comply with the duties in the legislation.

This is set out in the explanatory notes (point 302) accompanying the Clause 49 in the Online Safety Act:

"A provider is not obliged to follow a code of practice; they may instead take alternative measures to comply with the duties in the legislation."

It is important that Ofcom plays close attention as part of its supervisory regime to services who choose to take alternative measures. It could be that some companies wait for supervision before they act, others could choose to take other steps than proposed in the Code, which could potentially be innovative and lead to the identification of best practice.

5. Illegal content Judgments

Much of Ofcom's measures proposed in Volume 5 (illegal content judgments) and the Codes of Practice (Volume 4) focus on takedown measures for content rather than preventing pieces of known child sexual abuse content, for example, going live on a platform in the first place.

They do not consider the use of proactive technology (that are not restricted by S.231 of the Act) nor safety by design measures, which we have covered in our response to the Code of Practice.

This seems to run contrary to the stated aims and objectives as set down by Parliament and in response to New Clause 1 that was tabled to the Bill in the House of Lords, which embedded safety by design as a key principle.

It also runs counter to other Government priorities. In 2020, the Independent Inquiry into Child Sexual Abuse concluded in 2020:

"*No industry witnesses said that it was technically impossible to pre-screen their platforms and services. PhotoDNA is efficient in detecting a known child sexual abuse image once it has been uploaded but its important to try and prevent the image from being uploaded in the first* *place and thereby prevent access. The use of pre-screening or pre-filtering technology should be encouraged to fulfil the Government's expectation that: "child sexual abuse material should be blocked as soon as it is detected. This is a key aspect of the preventative approach that is necessary."*[12]

The Government's response to the Independent Inquiry's recommendations supported this recommendation it stated:

"*The Interim Code of Practice on tackling CSE/A builds upon the voluntary principles which set out the UK Government's expectation that all companies will prevent access to known child sexual abuse material. The first principle is that companies will seek to prevent known child sexual abuse material from being made available to users or accessible on their platforms or services, take appropriate action under their terms of service, and report it to the appropriate authorities. Pre-screening is one means of preventing access, recognising that this threat and response that it requires may vary depending on the type or nature of the service offered.*"[13]

This leaves us in the curious position of interim codes of practice and voluntary principles going much further than what Ofcom has been willing to recommend. We also know from industry transparency reporting that some of the largest platforms are also catching the majority of CSAM content before it goes live on their platforms.

Snap for example in its latest transparency report states:

"In the first half of 2023, we proactively detected and actioned 98% of the total chid sexual exploitation and abuse violations reported here- a 4% increase on the previous period."[14]

Meta also provides information on its proactivity rate, which it claims can be as high as 99%[15]

However, it is important to bear in mind that proactivity is only applicable to known cases of CSAM and is only focussed on the detection of CSAM content to a limited extent. Content that has not previously been reported is much harder to detect and it is possible that even if a platform is deploying tools like Google's CSAI Match to detect potential new CSAM content, that some content goes live on a platform before it can be removed.

Some testimony in the recent filings against Meta in New Mexico acknowledge this claim:

"*Meta knew about the huge volume of inappropriate content being shared between adults and minors they do not know; a 2021 presentation estimated 100,000 children per day received online sexual harassment, such as pictures of adult genitalia*"[16]

It continues:

"*Instagram is well aware that users post on its site, distribute and advertise CSAM. When a user search using known CSAM keywords, Instagram displays "an interstitial alerting the user of potential CSAM content in the results." The Warning Reads: "These results may contain*

[12] Independent Inquiry into Child Sexual Abuse: The Internet (Point 95, Page 48) https://webarchive.nationalarchives.gov.uk/ukgwa/20221215030740/https://www.iicsa.org.uk/key-documents/17805/view/internet-investigation-report-march-2020.pdf

[13] Government response to the Independent Inquiry into Child Sexual Abuse (Point 10, Page 2) https://assets.publishing.service.gov.uk/media/5fa96feae90e0730594deb47/Government_Response_to_IICSA_Internet_Report.pdf

[14] https://values.snap.com/en-GB/privacy/transparency

[15] https://transparency.fb.com/en-gb/policies/improving/proactive-rate-metric/

[16] https://storage.courtlistener.com/recap/gov.uscourts.nmd.496039/gov.uscourts.nmd.496039.36.1.pdf page 95

images of child sexual abuse. Child Sexual Abuse or viewing the sexual imagery of children can lead to imprisonment and other severe personal consequences. This abuse causes extreme harm to children and searching and viewing such materials adds to that harm. To get help or learn how to report any content as inappropriate, visit our help center."[17]

Even though this warning notice acknowledges the illegality of harm stemming from the search result, Instagram still gives the users the option of "see results anyway" and the user is taken to the content Instagram is warning is illegal and harmful rendering the warning notice useless.

When challenged on this at the recent Senate Hearing in the United States by Senator Ted Cruz, Mark Zuckerberg responded by stating:

"*Well, because we might be wrong, we try to trigger this warning, or we tried to, when we think there is any chance the results might be wrong.*"[18]

It is clear through these responses that some services prefer leaving content in place on the basis that "they might be wrong" rather than taking a more "proactive approach" to content removal.

The guidance issued by Ofcom states companies can go further if they wish:

"26.18 states: *"Services are free to take down content above and beyond what is illegal under the Act, so long as they make this clear in their terms of service, and that their content moderation practices result in the timely removal of illegal content as set out in the illegal content safety duties."*

Our concern is that this looks and feels an awful lot like self-regulation based on the terms and conditions services chose to put in place. There is also a warning that over removal of content should not come at the expense of detecting illegal content.

In Chapter 12, of Volume 4, Ofcom also reminds us that: "*It is important to make clear that as a regulator, Ofcom will not take a view on individual pieces of content. Rather, our regulatory approach is to ensure that services have systems and processes in place to meet their duties."*

We are therefore concerned that the overall approach to the illegal content judgments means that there isn't much movement from the current status quo. It is still for companies to make individual judgements on individual pieces of content; there is a lack of focus on how to design systems safely, preventing the spread of known content from ever going live in the first place, and not much focus on the proactive detection of new content through the recommendation to use AI or Machine Learning technologies such as CSAI match in the Code of Practice.

We recommend that Ofcom considers seeking information from services on the systems and processes it has in place to detect known CSEA content and CSEA content that has not previously been detected on its platforms. We recommend a further focus on safety by design and ensuring CSEA content that has previously been detected is prevented from circulating by scanning on upload.

[17] https://storage.courtlistener.com/recap/gov.uscourts.nmd.496039/gov.uscourts.nmd.496039.36.1.pdf Page 102

[18] https://www.techpolicy.press/transcript-us-senate-judiciary-committee-hearing-on-big-tech-and-the-online-child-sexual-exploitation-crisis/

6. Scope and risk- categorisation

Definitions of size vs risk:

During the passage of the Online Safety Act in Parliament there was significant debate on ensuring that the legislation could ensure that it was not only "large platforms" that were in scope of the regulation.

Government Ministers frequently reminded colleagues in both the House of Lords and House of Commons that:

"All platforms regardless of size, are in scope with regard to content that is illegal and content that is harmful to children."[19]

Lord Parkinson was also keen to build on this further to ensure that illegal content and activity could be tackled across a range of services, recognising the cross-platform nature of harms like grooming and child sexual abuse. He stated:

"Whilst I am sympathetic to arguments that we must avoid imposing disproportionate burdens on regulated services....the current scope of the Bill reflects evidence of where harm is manifested online. There is clear evidence that smaller services can pose a significant risk of harm from illegal content, as well as children, as Lady Kidron, rightly, echoed. ***Moreover, harmful content and activity can often range across a number of services. While illegal content and activity may originate on larger platforms, offenders often seek to move to smaller platforms with less effective systems for tackling criminal activity."***[20]

A debate late on in the passage of the legislation saw an important concession to amendments that had been pushed hard in the House of Commons by Sir Jeremey Wright KC MP and Baroness Morgan of Cotes in the House of Lords.

The Government introduced an amendment at Consideration of Lords Amendments in the House of Commons to ensure that the threshold for Category 1 providers would be based not on size **and** functionality but size **or** functionality. This essentially opened an opportunity for Ofcom to not only target its regulatory power on large companies, but also on companies with functionality that made them significantly higher risk of harm.

Whilst we recognise that categorisation is not subject to this consultation and will be further consulted upon by Ofcom at a future date, we do believe that at present, the current definition and thresholds of a "large platform" are simply too high and are not reflective of the debate during the final stages of the Act where amendments were made specifically to cover high harm services.

Point 9.60 of Volume 3 Page 57, Ofcom explains its approach to assessing likelihood and impact. Defining impact Ofcom states:

"For high impact, we propose a user number of more than 7 million monthly UK users. This aligns with how we propose to define a 'large' service, as discussed from Chapter 11, paragraph 11.51. It represents approximately 10% of the UK population, which is similar to the

[19] House of Commons Hansard, 19 April 2023, https://hansard.parliament.uk/commons/2022-04-19/debates/F88B42D3-BFC4-4612-B166-8D2C15FA3E4E/OnlineSafetyBill Column 133

[20] Hansard 2nd May Column 1485 https://hansard.parliament.uk/lords/2023-05-02/debates/C4ADB2FF-C4AE-4BEA-8E30-A341ECF32822/OnlineSafetyBill

definition of very large service taken by the EU in the Digital Services Act. It is also broadly similar to one of the factors feeding into the highest risk category in the Australian social media code."

Whilst we praise Ofcom for attempting to achieve regulatory alignment internationally with other regulators, we are concerned that the 7m+ threshold is too high and will leave several prominent companies outside the scope of many of the mitigations.

For example, Roblox, a platform widely used by nearly 300 million people globally[21], 60% of which are children (under the age of 16) and is currently subject to a class action bought by parents in California may not be fully covered by all of the measures they could and should be under the definition of the Act.

Fortnite, another platform widely used by children, would also be out of scope, with them averaging 4 million monthly UK users- 5% of the total global average of 80 million.

It is also important that companies are transparent about the number of UK users they have on their services. We saw when the Digital Services Act first issue requests for information on the number of users services had that Pornhub disputed they had breached the 45 million monthly user threshold, claiming*:*

"As of 31 July 2023, Pornhub has 33 million average monthly recipients of the service in the EU."[22]

Only to be later designated along with three other commercial adult websites as very large platforms.[23]

Whilst we recognise that the Act was amended late in its passage and this will have had an impact on Ofcom's preparations, we believe it is important that all platforms are truly in scope of this regulation. We remind Ofcom that this consultation focuses on some of the most egregious and serious criminal offences that have a huge impact on society and those who are victims that have to live with the lifelong consequences and therefore **we do not see the need to separate out very large platforms from those small and medium sized platforms that could potentially cause a huge amount of harm.**

We want to see the hashing and URL provisions embedded as widely as possible across industry for the maximum impact to be achieved. Recognising the increased costs to micro, small and medium sized businesses, we could support recommendations that they are given longer to prepare, maybe a period of 12-18 months but if they are medium to high risk of harm, they should be required and in scope of mitigation measures.

Application of Governance and Accountability measures:

In point 7.4 of Volume 3 (Risk Assessment) Ofcom sets out its approach to Governance and accountability measures, explaining that these are reserved for large service providers with more than 7m+ monthly UK Users and 'multi-risk' services as those that identify as medium or high risk for **at least two** kinds of illegal harms in their latest risk assessment.

We believe it is important that if a service is at medium to high risk of being abused to disseminate, distribute, or provide access to large amounts of child sexual abuse that they should be

[21] https://backlinko.com/roblox-users

[22] https://nypost.com/2023/12/20/business/pornhub-blasts-eu-over-new-regulations-on-top-porn-sites/

[23] https://dig.watch/updates/european-commission-designates-pornhub-stripchat-and-xvideos-as-vlops-under-dsa

in scope of governance and accountability measures. We believe good governance; effective risk mitigation strategies and appropriate levels of accountability are all vital components to managing a significant risk to the safety and welfare of children.

We do not believe that you should have to be considered for medium to high risk for “at least two” kinds of illegal harms to be in scope of these measures.

Ofcom also makes several assumptions throughout which suggest that single-risk services cause less harm and therefore mitigations have less benefit:

For example, in point 11.44, Volume 4 (Page 13) Ofcom states:

“We intend these measures to apply to services that face significant risks for illegal harms in general. There is a question over what it means for a service to have such risks. One option would be to recommend these measures to services that have identified as medium or high risk of at least one kind of illegal harm. ***However, where services only identify a risk of a single kind of illegal harm, the benefits of these measures to address all harms will be lower****. This is partly because if services have only identified a single area of risk, the extent of harm will tend to be lower compared to if they have identified a range of kinds of offence where they are high risk.”*

Ofcom also, in our opinion, wrongly assumes that because a service is only at medium to high risk of a single type of harm, that risk is more likely to be better understood across the organisation and will therefore be taking steps to address it.

“If a service was only of medium or high risk for a single kind of illegal harm, the risk is more likely to be well understood across the organisation*, such as the risk of fraud for some marketplace services. This tends to mean the benefits of these measures in terms of improving understanding and consistency of approach are smaller than if there were multiple areas of risk.”*

(CONFIDENTIAL✂)

We therefore recommend that Ofcom changes its recommendation around Governance and Accountability measures to apply to services that are medium of high risk of one kind of illegal harm in their latest risk assessment.

<u>**Training requirements**</u>

We also believe that medium sized companies within the scope of the code of practice should also be held accountable for the measures that require them to train and develop their staff. As we have mentioned previously, we are concerned that Ofcom has set a bar so high in its definition of large platforms, that many medium sized platforms that are medium to high risk or that are popularly used by children will be out of scope of training and development requirements.

Question (Volume 2)	Your response
Question 6.1: Do you have any comments on Ofcom's assessment of the causes and impacts of online harms? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.	*[Is this answer confidential?* ***Partly, Confidential section highlighted in the text.*** **<u>Overview:</u>** It is our view the Ofcom has compiled a thorough evidence base setting out the online CSE/A threat landscape from publicly available sources of information both in the UK and internationally. We are pleased to see that data and research collated by child protection bodies including ourselves, the NSPCC, ECPAT International, NCMEC, Thorn, and many others has been included alongside publicly available law enforcement data and academic research. We would recommend that Ofcom utilises the evidence in Volume 2 in other areas of the consultation more effectively. This is particularly relevant to the societal costs vs. compliance costs for business. Societal costs are referenced extensively in Volume 2 and then in other volumes the focus shifts to compliance costs to business with little thought to societal impact. It should be recognised that there is a regulatory cost to business to mitigate some of the harms that they cause or exacerbate. We also recommend that this section is updated to reflect harms caused by Generative AI and Extended Reality technologies. Whilst there is an acknowledgement, that there is: "*....growing evidence that extended reality technologies are being exploited for the commission of CSAM offences...*" (Volume 2, Page 66), there was little in the footnotes of examples of this growing evidence base. These are harms that are occurring at scale now - and updated versions of the code must take these technologies into account. It is also important to note that the Government Minster, Lord Parkinson confirmed to the Telegraph whilst the Online Safety Act was before Parliament, that "*ChatGPT style chatbots would fall under new online safety laws and content that had been generated and posted on social media by them will be covered by new laws*."

Question (Volume 2)	Your response
	Currently Ofcom’s evidence base on the harms caused by these new technologies is too light and we have provided some evidence of the harms caused in this response. **<u>Generative Artificial Intelligence:</u>** Ofcom states in the Volume 2, Page 6, point 5.6: *“We will monitor harms and regulated services trends and will revise our Register as appropriate. In future we may expand the scope of our risk assessment if necessary. For example, as new technologies develop, and risks to online safety emerge due to the rapid innovation of the sector.* *This may include technologies such as immersive online virtual worlds, augmented realities, and generative artificial intelligence (‘generative AI’).”* The footnote then goes on to explain that the risk register has only partially considered the risk of Generative AI technologies in a *“limited measure”* and that the register considers *“some of these risks.”* Elsewhere in the CSAM risk section in Volume 2 the consultation explains: “*The use of deepfakes in CSAM production is still very new, and the resulting images and videos are hard to identify*.” (Volume 2, Page 77). We would argue that Generative AI is not a future risk, but is very much a risk that requires oversight now, if the problem is not to get any worse. In a one-month period between September and October 2023, the IWF was able to scrape 20,254 AI generated images from one dark web forum. Of the 11,108 images we assessed using human review, we found 2,978 images were illegal either under the Protection of Children Act (1978) or the Coroners and Justice Act (2009). The IWF produced a report ahead of the UK Government’s International AI Safety Summit, which contained several recommendations on how the technology could be better regulated to ensure harm didn’t occur. These recommendations included: • Ensuring the data sets used to create generative AI material could be scrutinised and

Question (Volume 2)	Your response
	validated as clear of child sexual abuse material by expert child safety organisations. - Ensure that protections can be built into closed-source models and that open-source models are open to regulatory scrutiny prior to their release to ensure appropriate risk mitigation strategies are in place. - To ensure companies have in place clear terms and conditions which prohibit users from using their tools to generate CSAM. - That search providers de-index fine tuned models known to be linked to the creation of AI generated CSAM. Since that report, we have also been discussing other mitigations which could include: - App stores being held accountable for enforcing their terms and conditions by removing applications that are known to be used to generate AI CSAM. (CONFIDENTIAL✂) There is further evidence that these images are causing real world harm as the BBC has reported from Spain, where 20 girls between the ages of 11 and 17 had become victims of having their fully-clothed imagery manipulated to depict them without their clothes on, with the police investigating 11 boys for sharing the images within WhatsApp and Telegram groups. A report published by the University of Stanford’s Internet Observatory provides further information as to the extent of the problem. Their report found “hundreds” child sexual abuse images in an open-source dataset used to train popular AI image generation models such as Stable Diffusion. Their research specifically referred to the LAION-5B dataset. **Extended reality technologies (XR):** At the start of 2024, law enforcement announced that it was investigating the first case of digital rape in the Metaverse. The victim was a girl under the age of 16, left distraught after her avatar was gang raped by strangers online. Whilst no physical harm was caused, the psychological trauma and emotional trauma she

Question (Volume 2)	Your response
	suffered, officers claim was equivalent to real world harm due to the immersive nature of the technology. Research published by the NSPCC suggests that 75% of people believe 6–12-year-olds are at major or significant risk of sexual abuse in immersive spaces and that rises to 80% within the 13-16-year-old age range. The University of Manchester also published a paper in 2022, which further breaks down Extended Reality Technologies into three categories: Virtual Reality (VR), Augmented Reality (AR) and Mixed Reality. Encouragingly, this paper highlights many of the risk factors Ofcom has identified in the consultation document, including live-streaming and anonymity, for example, but the research does highlight emerging challenges, such as new ways to abuse and exploit children, the potential normalisation or inappropriate behaviours towards children and challenges for content moderation and enforcement. These challenges will become particularly profound the cheaper and more universally available the technology becomes. The NSPCC estimates that 15% of children between 5 and 10 have used one and 6% use one daily. **Other Relevant information:** Since Ofcom published this consultation, the Vulnerability, Knowledge and Practice Programme (VKPP) has produced a report, which adds further evidence of the CSE/A threat. They analysed over 107,000 crime reports, which discovered that around 75% of offences were committed directly against children around 25% of these offences related to online offences of indecent images against children, with child-on-child abuse rising significantly from around a third, to 50% of offences, further highlighting the changing nature of this crime since the advent of technology. **Industry data:** We also noted that it seemed almost all the evidence Ofcom has used to justify its evidence base for CSE/A has come from civil society organisations, policing, public inquiries, and academia. Whilst all are credible, reliable sources of evidence, we would urge Ofcom not

Question (Volume 2)	Your response
	to forgot about the significant data the industry holds on the CSE/A threat. We appreciate that much of this consultation would have been prepared prior to Ofcom receiving its formal powers, but we would encourage Ofcom to make full use of these powers now that they have been conferred, so that evidence from industry can also be included within this narrative. For example, it would be helpful if Ofcom were able to provide both quantitative and qualitative data and commentary on how much content different platforms were able to prevent from being uploaded to their platforms, the tools, service design, and mitigations they put in place to prevent illegal content from being uploaded and how transparently they reported on these issues. It would be helpful if future evidence bases also scrutinised the claims made in publicly available transparency reports, with information that Ofcom has requested from platforms about the scale and nature of the issues on their services, and what conclusions they were able to draw between service functionalities or similar models, whilst also highlighting best practice.
Question 6.2: Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.	*Is this answer confidential? No* **End-to-End Encryption (E2EE):** We were particularly pleased to see that End-to-End Encryption has been included as a functionality that posed specific risks, in particular relation to the detection of CSE/A. When this factor is combined with the other characteristics of a service and child sexual abuse material, we know that this technology will have a significant impact on harm to children. As is referenced in this consultation, we saw the impact of Meta not scanning for child sexual abuse content on accounts based in the European Union, whilst the temporary derogation was being negotiated. This resulted in a 58% reduction in reports to the National Center for Missing and Exploited Children (NCMEC). We believe that if they are to encrypt their messenger and Instagram direct messaging functionality, that we could see similar such dips in reporting, perhaps larger

Question (Volume 2)	Your response
	drops given that E2EE will be rolled out worldwide and not just EU accounts. **Measuring service size:** Page 11 of Volume 2 states there are two ways Ofcom is proposing to manage size of service. This includes measuring the user base, the number of employees (capacity) feel like good measures to determine size and are very similar to how we currently determine the membership fee for the IWF, which is based on size (determined the way Ofcom sets out) and sector. However, in later volumes of the consultation (Volume 3 and Chapter 11) Ofcom states that a "large" service will be defined as a service which has a user base of over 7 million monthly UK users. Our concern is that most websites that are responsible for hosting large quantities of child sexual abuse material will be missed entirely by the more stringent measures in the proposals from Ofcom, of particular concern is the differing approaches to risk assessment.

Question (Volume 3)	Your response
Question 8.1: Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice? Please provide underlying arguments and evidence of efficacy or risks to support your view.	*Is this answer confidential? No* We have covered this above.
Question 8.2: Do you agree with the types of services that we propose the governance and accountability measures should apply to?	*Is this answer confidential? No* Covered above.

Question (Volume 3)	Your response
Question 8.3: Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?	*Is this answer confidential? No* No further evidence to add.
Question: 8.4: Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?	*Is this answer confidential? No* No further evidence to add.
Question 9.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* We have set out above where we disagree with proposals. To summarise we would like to see: • The definition of Very Large Platforms revisited to ensure more services are caught in scope of the regulation. • We believe governance and accountability measures should apply to all services at medium to high risk of one harm. • Training requirements should be extended to staff in services where they are deemed to be medium to high risk of CSAM.

Question (Volume 3)	Your response
Question 9.2: Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?	*Is this answer confidential? No* Nothing further to add.
Question 9.3: Are the Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service?[24]	*Is this answer confidential? No* Nothing further to add.
Question 10.1: Do you have any comments on our draft record keeping and review guidance?	*Is this answer confidential? No* Nothing further to add.
Question 10.2: Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?	*Is this answer confidential? No* Nothing further to add.

[24] If you have comments or input related the links between different kinds of illegal harm and risk factors, please refer to Volume 2: Chapter 5 Summary of the causes and impacts of online harm).

Question (Volume 4)	Your response
Question 11.1: Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?	*Is this answer confidential? No* *Covered above.*
Question 11.2: Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?	*Is this answer confidential? No* Covered above. We are supportive of measures to: • Detect CSAM with hash matching • Block access to CSAM with URL blocking • Deindex links known to contain CSAM (Search) • Provide warning messages (Search) We believe such measures should apply to all services at medium to high risk of one type of harm.
Question 11.3: Do you agree with our definition of large services?	*Is this answer confidential? No* We disagree with the definition of large services. We have set this out in our response above. With the illegal content measures and Ofcom's ambition to raise the floor, we don't see why there is a need to differentiate between services when it comes to the most egregious forms of online harms. We recommend that Ofcom looks again at this definition to ensure popular platforms used by children are in scope of all of the measures within the code, particularly for CSAM and that Ofcom revisits debates in the House of Commons and House of Lords to ensure medium and high harm small platforms are captured.
Question 11.4: Do you agree with our definition of multi-risk services?	*Is this answer confidential? No* Also covered above, but to summarise, we disagree. We believe Ofcom has not placed enough emphasis on services that are at medium to high risk of just ONE illegal harm. **We recommend that Ofcom amends its definition accordingly.**

Question (Volume 4)	Your response
Question 11.6: Do you have any comments on the draft Codes of Practice themselves?[25]	*Is this answer confidential? No* We have covered this extensively in our response. We recommend the following measures are added: • Keyword detection for CSAM • Use of classifiers (AI and Machine Learning) to detect CSAM content that has not previously been detected • Grooming measures are supported by Age Verification and not reliant on self-declaration of age. • Codes of Practice are amended to require companies to mitigate risks identified in their risk assessment.
Question 11.7: Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?	*Is this answer confidential? No* Nothing further to add.
Question 12.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* *Nothing further to add.*
Question 13.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* *Nothing further to add*
Question 14.1: Do you agree with our proposals? Do you have any views on our three proposals, i.e. CSAM hash matching, CSAM URL detection and fraud	*Is this answer confidential? No* Yes- we agree with the CSAM measures and have provided further evidence on their effectiveness above.

[25] See Annexes 7 and 8.

Question (Volume 4)	Your response
keyword detection? Please provide the underlying arguments and evidence that support your views.	
Question 14.2: Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated ‘publicly’ or ‘privately’?	*Is this answer confidential? No* We believe there is a complex and delicate balance and that this guidance needs further work. We would like to see greater acknowledgement of a victim’s rights to privacy not to have illegal imagery of them spread online. Greater reference also needs to be made to the carefully qualified statements under articles 8 and 3 of the UNHCR and Article 10 of the rights of the child.
Question 14.3: Do you have any relevant evidence on: • The accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services; • The ability of services in scope of the CSAM hash matching measure to access hash databases/services, with respect to access criteria or requirements set by database and/or hash matching service providers; • The costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching[26] for CSAM URL detection; • The costs of applying our articles for use in frauds	*Is this answer confidential? Yes* (CONFIDENTIAL✂)

[26] Fuzzy matching can allow a match between U2U content and a URL list, despite the text not being exactly the same.

Question (Volume 4)	Your response
(standard keyword detection) measure, including for smaller services; and - An effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and any information you have on the costs and efficacy of applying hash matching and URL detection for terrorism content to a range of services.	
Question 15.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add.*
Question 16.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add.*
Question 17.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add.*

Question (Volume 4)	Your response
Question 17.2: Do you have any evidence, in particular on the use of prompts, to guide further work in this area?	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add.*
Question 18.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add.*
Question 18.2: Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add.*
Question 18.3: Are there other points within the user journey where under 18s should be informed of the risk of illegal content?	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add.*
Question 19.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add*

Question (Volume 4)	Your response
Question 19.2: What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?	*Is this answer confidential? No* *Nothing further to add*
Question 19.3: We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive. Are you aware of any other design parameters and choices that are proven to improve user safety?	*Is this answer confidential? No* *Nothing further to add*
Question 20.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? No* *Nothing further to add*
Question 20.2: Do you think the first two proposed measures should include requirements for how these controls are made known to users?	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add*
Question 20.3: Do you think there are situations where the labelling of accounts through voluntary verification	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add*

Question (Volume 4)	Your response
schemes has particular value or risks?	
Question 21.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add*
Question 21.2: Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically: • What are the options available to block and prevent a user from returning to a service (e.g. blocking by username, email or IP address, or a combination of factors)? What are the advantages and disadvantages of the different options, including any potential impact on other users? • How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed? • There is a risk that lawful content is erroneously classified as CSAM by automated systems, which may impact on the rights of law-abiding users. What steps can	*[Is this answer confidential? No* *Nothing further to add*

Question (Volume 4)	Your response
services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?	
Question 22.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? No* *Nothing further to add.*
Question 23.1: Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?	*[Is this answer confidential? No* *Nothing further to add.*
Question 23.2: Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?	*[Is this answer confidential? No* It is important that even if a small or micro business is identified at medium to high risk of being abused for CSAM or grooming that it puts in place mitigations. We remind Ofcom of comments made by Lord Parkinson in the House of Lords, rejecting amendments from Baroness Fox about the need for special treatment for small and mirco-businesses.
Question 23.3: We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?	*[Is this answer confidential? No*

Question (Volume 4)	Your response
Question 24.1: Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard? If not, why not?	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add.*

Question (Volume 5)	Your response
Question 26.1: Do you agree with our proposals, including the detail of the drafting? What are the underlying arguments and evidence that inform your view.	*[Is this answer confidential? Yes / No (delete as appropriate)]* *Nothing further to add.*
Question 26.2: Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?	*[Is this answer confidential? No* *No further comments. In line with comments made at the start of the consultation we believe Ofcom must simplify this guidance for businesses. It is overly complex and is difficult to comprehend.*
Question 26.3: What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?	*[Is this answer confidential? No* *No further comments.*

Question (Volume 6)	Your response
Question 28.1: Do you have any comments on our proposed approach to information gathering powers under the Act?	*[Is this answer confidential? No* It is important that Ofcom recognises the burdens that they are placing on civil society organisations to respond to significant consultations. This consultation is the first of many planned over the next two years to implement the regime. Responding to the consultations takes significant resources from organisations that are not as well-resourced as Ofcom. We urge Ofcom to develop alternative measures to gathering feedback from civil society. Whilst we are proud to have been involved in developing the Codes and responding to the consultation, this has placed significant time and resourcing implications on our organisation and others we work with in the child protection sector. There is also a risk that the child protection and civil society sec
Question 29.1: Do you have any comments on our draft Online Safety Enforcement Guidance?	*Is this answer confidential? No* Impact on voluntary measures undertaken by ISPs and Domain Name providers: As briefly raised by the Internet Service Providers Association (ISPA) in their response to this consultation, both we and they would welcome further information from Ofcom on how it is intending to work with some of the current voluntary infrastructure in place in the UK, through the work of the Internet Watch Foundation in the provision of blocking orders. Currently, ISPs implement the IWF's blocking of CSAM at ISP level and this happens prior to a court order based on the fact the IWF is recognised as the Notice and Takedown body in the UK through our memorandum of understanding with the CPS and NPCC. This is something that many of our members, their trade association want to see continue and four of our largest members BT, Talk-Talk, Virgin Media and Sky collectively cover 95% of the UK broadband market, meaning there is good coverage to them voluntarily blocking child sexual abuse material. We also work closely with Nominet, the .UK domain name registry and other registries and registrars internationally

Question (Volume 6)	Your response
	to provide them with Domain Alerts and other bespoke services to help keep their services free of child sexual abuse material. This is extremely effective with Nominet only suspending 1,193 domains for all forms of criminal activity in 2023. It is vitally important that this voluntary work is enabled to continue. It also helps to achieve the aims and objectives of the recently published voluntary infrastructure guidance from the Home Office. We would welcome further engagement with Ofcom on this subject including, as referenced by ISPA: • Clarity on how our current blocking measures will be impacted (if at all) by Access Restriction Orders. • Will Ofcom look to issue voluntary access restriction orders to ISPs for the IWF's URL list? • What sort of guidance Ofcom is going to offer around the accuracy and efficiency of blocking technologies? • Appeals processes • In addition, we believe that Ofcom needs to consider whether such measures need to be extended beyond ISPs to incorporate other operators of key Internet infrastructure such as content delivery networks (CDNs) and public DNS resolvers. This would ensure that the measures continue to be effective despite changes to Internet protocols that weaken the gatekeeper function of ISPs.

Question (Annex 13)	Your response
Question A13.1: Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating	*[Is this answer confidential? No* Nothing further to add

Question (Annex 13)	Your response
Welsh no less favourably than English?	
Question A13.2: If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.	*[Is this answer confidential? No* *Nothing further to add.*

Please complete this form in full and return to IHconsultation@ofcom.org.uk.