Written evidence submitted by the Internet Watch Foundation

IWF response to the DCMS Online Harms and Disinformation Sub Committee Inquiry into the draft Online Safety Bill

Organisation responding: The Internet Watch Foundation (IWF)

Address: Internet Watch Foundation, Discovery House, Chivers Way, Vision Park, Histon, Cambridge, CB24 9ZR, UK

1. Introduction-

1.1. The Government has set out its ambition to make the UK the safest place to go online and has continually reiterated that it wants to ensure that, through the forthcoming Online Safety Bill, the highest possible protections are in place for children.[1]

1.2. The Government's full response to the Online Harms Consultation, published in December 2020, made it clear that it envisaged a new regulatory landscape where Ofcom would have to work in partnership with those already working in this space. The full Government consultation response stated:

"The Government will work with Ofcom to ensure that the regulator is able to work effectively with a range of organisations. This will be delivered through a range of means including, co-designation powers, memorandums of understanding, forums and networks."[2]

1.3. We agree that this collaborative approach to regulation is important, because it is vital that Ofcom has a good technical understanding of the harms that it is regulating, can build upon existing effective relationships and ensures that its use of powers is appropriate, proportionate and doesn't disrupt decades of successful collaboration between industry and civil society that has seen the UK become a global leader in child online safety.

1.4. The IWF believes that we have a strong contribution to make to the new regulatory environment based on our hard-earned reputation as an effective, trusted partner of Government, law enforcement and industry. In 2020, the UK's Independent Inquiry into Child Sexual Abuse concluded that IWF is a "genuine success story" and that we "sit at the heart of the national response to combating the proliferation of indecent images of children." The report concluded: "The IWF deserves to be publicly acknowledged as a vital part of how and why comparatively little child sexual abuse is hosted in the UK".

1.5. The IWF has therefore worked with its industry partners to develop a model to enable IWF to play an active part as an independent expert in the new regulatory process whilst maintaining its vital collaborative role with the industry.

1.6. We were therefore disappointed not to see any information contained in either the Bill or the explanatory notes accompanying the legislation on how the Government's vision of a collaborative regulator would be achieved. There is no mention of how co-designation could be achieved, what the criteria may be and how this would all work in practice.

---

[1] DCMS Select Committee- https://committees.parliament.uk/oralevidence/2185/pdf/ Q.18

[2] UK Government's Full Response to the Online Harms White Paper Online Harms White Paper: Full government response to the consultation - GOV.UK (www.gov.uk) points 3.27-3.33

1.7. ***Through this submission, we would like to see the pre-legislative scrutiny committee seek further clarity from the Government and Ofcom detailing the process for which organisations like the IWF could be appointed as co-designated bodies for CSE/A.***

1.8. ***In addition, we call on the Government to publish a timeline setting out when some of these decisions may be made and further details on how it intends to fund the organisations responsible for enforcing and implementing the regulatory regime.***

1.9. The Government also further stressed the importance of international collaboration, in its full Government response to the Online Harms White Paper it stated:

"Furthermore, Ofcom will play a critical role in enforcement across borders and will rely on its good relationships with its international counterparts to facilitate obtaining information from other jurisdictions, and to achieve a degree of international regulatory alignment."

1.10. We would like to draw the committee's attention to the large amount of global collaboration that already exists for the detection and removal of child sexual abuse imagery. Where the IWF locates imagery that is hosted outside of the UK, we work with other hotlines, law enforcement and industry internationally to have that content removed.

1.11. Last year (2020), the IWF was responsible for ***57% of the data submitted*** through the International Association of Internet Hotlines (INHOPE) database and the tools and services we offer the industry to block access to this imagery – whilst we are waiting for it to be removed or preventing its upload – are deployed globally including in the US, Philippines and Africa.

1.12. We also operate reporting portals in 49 (inc UK) different countries, which gives 2.5 billion people a secure an anonymous place in their own local language to report suspected CSAM.

1.13. We believe it is also important to draw the committee's attention the fact that any US based companies in the scope of this legislation, already have existing mandatory reporting obligations through US legislation which requires them to report any instances of suspected CSAM to the US-based National Center for Missing and Exploited Children (NCMEC). It is vitally important that what the UK is proposing for mandatory reporting, in sections 205-215 of the impact assessment accompanying this draft Bill, doesn't unnecessarily duplicate these mechanisms for US-based companies already reporting to NCMEC or require them to pay to establish a function they would not use in the UK through a regulatory levy.

1.14. ***We believe for the reasons set out above it is important for the proposed online safety regime in the UK to build upon these existing effective mechanisms and not duplicate other international reporting structures and co-operation which already exists in this space.***

1.15. In this submission, the IWF proposes five areas where we believe we can assist Ofcom and play our part in furthering online safety in the UK. For the past five years, we have been working with specialist regulatory lawyers and other legal advisors to establish a model which would see the IWF develop a new regulatory arm to carry out several distinct functions for Ofcom, whilst maintaining our independence and relationship with our members.

1.16. We believe we are well placed to assist Ofcom with developing the code of practice for CSE/A, monitoring compliance with the code of practice, assisting with investigations (or skilled person reports), mandatory reporting and transparency requirements.

1.17. Included within the key recommendations of our response are several areas where we feel the legislation could require further improvements. Particular areas the committee should focus its time and attention on include the definitions of harm contained within the Bill, the lack of information on how the regime will work in practice, the lack of age verification

measures for adult websites and the complexities of key enforcement mechanisms contained within the Bill such as the Use of Technology Notices.

2. Scope of the response-

2.1. The Internet Watch Foundation's (IWF) remit is distinct and deliberately limited to tackling illegal content, specifically online child sexual abuse material (CSAM) hosted anywhere in the world and non-photographic images of child sexual abuse hosted in the UK. For this reason, our response to the draft Online Safety Bill is specific to this area of expertise.

2.2. As an acknowledged leader in tackling the global threat of child sexual abuse images and videos on the internet, this response is made in the best interests of combating this global criminality for those who have been abused and had their suffering compounded by having their imagery shared online. We believe it is important to acknowledge that any changes in legislation proposed through the Online Safety Bill will only work with the cooperation of industry, and the IWF – with its strong industry relationships – can play a unique brokering role with those companies in scope.

2.3. We have consulted our independent Board and 160+ Members in producing this submission. This includes Internet Service Providers (ISPs), search engines, Mobile Network Operators, and manufacturers (MNOs), social media platforms, content service providers, telecommunications companies, software providers and those that join the IWF for CSR reasons. Our members include some of the biggest companies in the world – Amazon, Apple, Google, Facebook, Microsoft – as well as the largest ISPs and mobile operators in the UK and some of the smaller operators within the internet ecosystem who pay as little as £1,040 per annum yet still access every benefit and service we have to offer. We will also continue to discuss our future role in the new regulatory framework with them in addition to the Government, Parliament and the newly appointed regulator, Ofcom, in the coming months.

2.4. We welcome the Government's plans to introduce new online safety legislation in the UK. We have already responded comprehensively to both the Internet Safety Strategy and Online Harms White Paper and would like to acknowledge the consultation opportunities already provided by Government Departments in shaping this draft Bill. We are pleased to have the opportunity to further contribute to the newly proposed regulatory framework through this period of pre-legislative scrutiny and in response to this call for evidence by the Committee. Dealing with these issues online is challenging, complex and we believe it is right that the Government carefully constructs its new online safety laws by enabling technical experts and others to input into crafting this legislation and improving it further.

2.5. We have been clear from the outset that this legislation must be effective from day one, particularly within the area of our expertise which is dealing with child sexual abuse online. It is within this spirit of ensuring an effective regulatory regime, that builds on current best practice and further improves outcomes for children that we offer our submission to the Committee.

3. About the Internet Watch Foundation-

3.1. The IWF is a UK charity that works in partnership with the internet industry, law enforcement and government to remove from the internet (with the co-operation of industry) child sexual abuse images and videos wherever they are hosted in the world and non-photographic images[3] of child sexual abuse hosted in the UK.

- We exist for public benefit and perform two unique functions in the UK: We provide a secure and anonymous place for the public to report suspected online child sexual abuse images and videos, and;

[3] Non-Photographic Images include cartoons, drawings, computer generated imagery (CGI) and other non-photographic depictions of child sexual abuse that are deemed to have breached sections 62-69 of the Coroners and Justice Act (2009).

- We use the latest technology to search the global internet proactively for child sexual abuse images and videos, then work with partners to get them removed.

3.2. In addition, the IWF has established reporting portals – places to anonymously and safely report online child sexual abuse imagery – in 49 countries around the world, serving 2.5 billion people.

3.3. There is 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 Takedown Notices in the UK. Operationally, we are independent of UK Government and law enforcement but work closely with both.

3.4. 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 upload of 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.

3.5. Our work is funded almost entirely by the internet industry: 90% of our funding comes from our members with the remaining 10% of our funding coming directly from the European Commission's Connecting Europe Facility. Fortuitously, despite this funding from the EU ending in December 2021, it will then be replaced in full until March 2025 by Nominet, who are a world leading domain name registry based in the UK and responsible for administering the .UK domain.

3.6. The IWF has previously received additional Government funding for specific projects and is open to further diversifying its funding mix in the future.

3.7. We are 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 biennially by an independent team, led by a family court judge, and the report published in full.

4. Summary of Recommendations-

4.1. ***Through this submission, we would like to see the pre-legislative scrutiny committee seek further clarity from the Government and Ofcom detailing the process for which organisations like the IWF could be appointed as co-designated bodies for CSE/A. In addition, we call on the Government to publish a timeline setting out when some of these decisions may be made and further details on how it intends to fund the organisations responsible for enforcing and implementing the regulatory regime.***

4.2. ***Given the reasons set out in our introduction, we believe it is important for the proposed online safety regime in the UK to build upon these existing effective mechanisms and not duplicate other international reporting structures and co-operation which already exists in this space.***

4.3. ***Further information from the Government and Ofcom on how it plans to partner with an already under pressure charitable sector and fund some of these outsourced activities would be helpful.***

4.4. ***The more harms the Bill seeks to cover, the greater the level of support we believe Ofcom as a regulator will need.***

4.5. ***We would urge the pre-legislative scrutiny committee to give greater thought to the use of technology notices.***

4.6. ***It is our view that the proposed designated body for the Mandatory Reporting requirement for CSE/A content can only be performed by law enforcement, the IWF or a mixture of the two organisations.***

4.7. ***Any changes to proposed Codes of Practice, particularly for reasons of "Government Policy" could have significant risks to the independence of Ofcom as a regulator. We believe any changes proposed by the Secretary of State should be subject to extensive engagement with industry and Parliament.***

4.8. ***The Secretary of State will have the power in relation to CSE/A offences to specify relevant offences. However, we believe it is important that the definition of illegal content remains narrowly focused on CSAM and Counter Terrorism (CT) content to ensure the focus of the legislation remains on those most egregious harms.***

4.9. ***The IWF believes it is important that the online safety regime is established with a clear, transparent and sustainable funding regime. This will ensure that any regulatory interventions in relation to CSAM will be sustainable, consistent and practical, to enable Ofcom to achieve long lasting and effective change.***

4.10. ***Throughout much of our work, we see large amounts of CSAM content hosted on smaller providers such as image hosting boards and cyberlockers, hosted largely in the Netherlands. Often these smaller, lesser-known, services are a huge part of the problem. Whilst we understand Government wants to ensure that regulation is not overly burdensome for smaller companies, we believe that in the case of CSAM there should be a zero-tolerance approach to the hosting of this content, regardless of size.***

4.11. ***We have concerns over the definition of CSE/A content related to clause 43 of the Bill. The current draft of the Bill gives the power to Scottish Ministers to amend this clause. Whilst this in and of itself is not an issue, the IWF performs Notice and Takedown for the whole of the UK and it is important to ensure that dealing with CSE/A content does not become more complex or complicated due to one administration acting unilaterally, meaning it could make it more difficult to remove this type of content.***

4.12. ***We believe that the intersections between some of the clauses proposed in the legislation will require significant expertise from those working on content moderation decisions on a daily basis. For example, Clause 43 illegal content and clause 45- content that is harmful to children- can have very fine margins and it is important that we get these decisions right so that evidence can be used in the Court process to convict or acquit people correctly of suspected crimes once they are caught in possession of images.***

4.13. ***We would urge the committee to consider how best to include age verification of adult websites.***

5. The future role of IWF in Regulation-

5.1. For the past 25 years, the IWF has formed a vital part of the online safety landscape in the UK. In 1996, the year we were founded, 18% of the world's known child sexual abuse material (CSAM) was hosted in the UK. Today it is less than 0.1% and has been less than 1% ever since 2003.

5.2. Each year we remove millions of child sexual abuse images and videos from the internet. In 2020, we assessed **299,619 reports of suspected CSAM and confirmed 153,383 as containing CSAM.**

5.3. Our success has been built on the fact that we have been able to leverage funding from the internet industry on a voluntary basis in exchange for the services that we offer them to assist them in keeping their platforms free from CSAM.

5.4. Since the Government proposed new Online Safety legislation, we have been focused on the potential this legislation has to improve outcomes for children in the UK, and the role that the IWF could play to improve this response.

5.5. We believe the IWF is well placed to do this because we believe we bring unparalleled experience both domestically and internationally to this area and we would welcome the opportunity to bring this experience to bear in supporting Ofcom in delivering the vital child protection elements of the new regulatory structure.

5.6. Together with our members, we have been incredibly successful at removing millions of child sexual abuse images over the past 25 years, but there is clearly more to be done. In meeting the challenges, we believe the IWF's hugely successful – international – model of collaboration with the internet industry should be safeguarded and not jeopardised, and that the IWF should play a pivotal role in the UK regulatory framework.

5.7. The IWF has amongst its members some of the largest US tech companies. The majority of our top tier US members are likely to be within the scope of this legislation. We want to ensure that all the services offered by the IWF continue to be used by our members, in addition to the new regime. For them to continue taking services from the IWF and to ensure that the good work of the IWF is not lost or left behind, it is important that we maintain a clear separation between any regulatory functions we may take on as part of the Online Safety Bill, and our charitable functions. This is in part due to legal challenges in the US around 4th amendment issues and to ensure that the excellent collaborative working relationships we have with industry can be maintained, enhanced and nurtured further without confusion between our regulatory role and our membership role.

5.8. It is also worth pointing out that the IWF's wider membership is largely unaffected by the draft Online Safety Bill as it is currently drafted. For example, we have amongst our members two ISPs in the Philippines, the largest mobile network operator in South Africa and the largest mobile network operator in Kenya, who have joined the IWF because they value the quality of our services and want to protect their users from child sexual abuse material. The current draft of the Bill is not likely to affect these members as they do not have the necessary link to the UK, or do not fall within the current scope of providing user-to-user or search services and will not be providers of 'regulated services'.

5.9. That is why we have been working with specialist regulatory lawyers, in consultation with our Board and membership, to ensure that we have the best of both worlds. We have been working to establish a new model that, if implemented, would see:

- The IWF establish a new regulatory arm to assist Ofcom, whilst,
- The charitable arm continues with its current work, providing uninterrupted services and data internationally, and the notice and takedown regime in the UK.

Our vision is that the new regulatory arm of the IWF would have functions delegated to it by Ofcom. This arm would be funded through Ofcom, by a regulatory levy on the industry.

5.10. Annex 1 accompanying this submission sets out how the structure between the IWF's regulatory functions and membership functions would be carried out. The regulatory arm we are proposing would have a separate and independent board governing its activities that would be appointed by Ofcom. The charitable board would continue to govern the IWF's current charitable activities in the same way it does now.

5.11. The IWF's Chief Executive, would be responsible for the day-to-day line management of a newly appointed Director of Regulation on the IWF's regulatory arm, but the Director of Regulation would be accountable to the newly appointed Ofcom board.

5.12. The diagram in Annex 1 also includes a standalone interface between the IWF's regulatory arm and the IWF's charitable arm. This interface would ensure that information could flow

both ways between the IWF's regulatory function and that of its membership function and would ensure clear systems and process for requesting information would have to be in place to avoid any conflicts of interest. This would be the responsibility of the Chief Executive to manage.

5.13. The IWF has taken extensive legal advice on the proposed establishment of the IWF's regulatory arm, and we have a legal paper that we would be happy to share with the committee with comparator regulatory regimes that have worked very effectively, including the Advertising Standards Agency, National Trading Standards, and the British Standards Institute as just three comparator examples of what we are proposing.

5.14. We have identified five areas where we can assist Ofcom:

1. **Code of Practice for Child Sexual Exploitation / Abuse (CSE/A)-** The IWF has already been heavily involved in assisting the Government in developing the voluntary interim Code of Practice on CSE/A[4]. We have provided feedback on two draft iterations of the interim Code and acted as a valuable interlocutor between the industry and Government on what is technically possible. We have also provided further case studies to support the code's guidance and suggested measures, demonstrating how valuable our expertise is in informing the steps companies should be taking to protect children from harm. We envisage an ongoing role for the IWF in drafting and consulting on further iterations of the Code in the future. At present, there is no reassurance from Ofcom that it will build upon previously published codes, but any further iterations of the Code must be created in consultation and dialogue with both the IWF and industry and ensure that any previous good work is taken into consideration.

2. **Investigations-** This would be a new role for the IWF. The IWF is proposing a new separate regulatory arm (see Annex 1) which would ensure a clear air gap between this new regulatory function of conducting investigations into companies, and the membership side of our organisation. The benefit of this model would be that Ofcom would be able to draw on the skills and expertise of the IWF's analysts – who work with CSAM day in day out and know lots about the problem, platforms and where this content is typically found and located – but the IWF's Regulatory Arm would remain independent of its membership function. This would enable us to continue to work with the wider industry. To work effectively, and to maintain and preserve valuable trusted industry relationships and compliance with our services including notice and takedown, we regard this new regulatory role into investigations being limited to providing information to the regulator only and for a clear and specific purpose. ***The IWF should not be involved in any enforcement decisions as this function is best carried out by Ofcom.***

3. **Monitoring compliance-** The IWF's proposed regulatory arm could also play a role in monitoring compliance with the CSE/A Code of Practice. The IWF regulatory arm would have the benefit of being legally protected to view and proactively search for CSE/A content and could report back to the regulator on its findings. The skills and experience built up by the IWF over the past 25 years means we have a good understanding of how the problem manifests online and we would be well placed to assist Ofcom with ensuring early compliance with the code. Again, as with investigations, it would be important for the IWF's regulatory functions to be able to keep a clear separation from that of its membership model to avoid conflicts of interest.

4. **Mandatory Reporting-** It is important to recognise that any US company that is within scope of the mandatory reporting requirement should not be required to report to the UK body as this would duplicate the system of mandatory reporting which is already in place to the National Center for Missing and Exploited Children (NCMEC) in the US. It is also the view of the IWF that those companies, should not have to pay a levy to establish a similar regime here in the UK, if they are not required to report to it.

[4] Interim code of practice on child sexual exploitation and abuse (publishing.service.gov.uk)

In reality, this means a small number of UK companies and in scope companies who do not currently report elsewhere will be required to report to the mandatory reporting body. This body will need to be appropriately resourced, however, as it is possible for technology companies to generate large numbers of reports if they encounter a particular issue on their service.

As the appropriate authority for Notice and Takedown in the UK, the IWF is well placed to play a part in a Mandatory Reporting function under the new regime. This is due to the excellent working relationships we already have in place with both law enforcement and the internet / tech industry.

We can assist our members with their reporting duties through our charitable arm, but also further this by taking on the mandatory reporting function under our new regulatory arm. This would, however, mean some changes for the IWF.

Paragraphs 205-215 of the impact assessment accompanying the Bill outlines the requirement to report CSE/A. Paragraph 206 contains figure 5: The Mandatory Reporting Process. Under Step 5 in that process, it specifies that the designated body will process reports by referring to law enforcement for investigation, including where children may be in immediate danger. We would likely have to move to a 24hr/ 7days per week/365days per year reporting service.

This would require appropriate funding and resources, with consideration given to securing funding on a long-term basis, beyond the Government's cyclical spending review processes. It would also be helpful if the Government could provide more information as to the compliance costs and costs of establishing the Mandatory Reporting regime which are currently missing or incomplete in the impact assessment.

5. **Transparency reporting-** Transparency reporting is an extremely tricky area, which requires careful handling, good relationships with industry and can carry significant financial and reputational penalties for companies if it is not handled appropriately.

It is important that appropriate context is set in the establishment of any transparency reporting. Big numbers of referrals from companies to NCMEC for suspected CSAM found on their services, does not automatically mean that their services are problematic, it might mean they are good at detecting it and dealing with it appropriately.

The IWF has been actively involved in recent ministerial discussions about the transparency reporting requirements[5] in the Online Safety Bill along with companies, Ofcom and other civil society organisations, that have made recommendations on how transparency reporting might work in the future. We already provide some information on where we find and locate content in the IWF's annual report, and we believe this is an area where we could further assist Ofcom.

5.15. Please see Annex 1 to our submission to this committee, which sets out a visual flow diagram of how the separation in functions between the IWF regulatory arm and charitable functions would work in practice.

6. Co-designation and interface with other bodies-

6.1. As mentioned in our introductory remarks, it is disappointing that the draft Online Safety Bill does not include any detail on how the Government or Ofcom intends to co-designate bodies, or how it will develop working relationships with other bodies (domestically or internationally) to implement the regime.

---

5 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944320/The_Government_Report_on_Transparency_Reporting_in_relation_to_Online_Harms.pdf

6.2. Following discussions with DCMS, we understand that the reason behind the lack of further detail about co-designation in the Bill is because Government believes that the Secretary of State already has the relevant powers for co-designation under section 69 of the Deregulation and Contracting Out Act (1994).

6.3. Whilst we accept this may be the case, we feel it would have been beneficial to see more information published alongside the Bill about how co-designation might be achieved or even a timeline on when such decisions will be taken. This detail could be included in the Explanatory Notes to the Bill.

6.4. The absence of this sort of information is problematic for a number of reasons. Firstly, it makes it extremely difficult for Parliament to effectively scrutinise the potential effectiveness of the legislation and the regime if it is not clear how Government or Ofcom intends to work with the "range of organisations" it specified in its response to the Online Harms White Paper (or even establish who they have in mind and how they have arrived at these conclusions).

6.5. Secondly, organisations that will be working closely with the regulator are going to need time to prepare, upskill and potentially recruit new staff to fulfil any new role(s) that they may take on to assist the regulator. The lack of a timetable or details on how co-designation, collaboration and how and when certain provisions in the legislation may be enacted could be detrimental to achieving the goals of the legislation or may delay implementation.

6.6. Thirdly, in the child protection space, this is complicated further by the Government confirming in its press release accompanying the draft Bill and covered in the Bill's impact assessment in paragraphs 205-215 that it will be introducing a designated body via secondary legislation which will handle the mandatory reports from technology companies based in the UK or that are within scope of the legislation, but not currently required to report elsewhere (internationally). As mentioned above, the IWF is currently recognised as the appropriate authority for the issuing of Notice and Takedown requests in the UK through the Memorandum of Understanding we have in place with the National Police Chiefs' Council (NPCC) and Crown Prosecution Service (CPS). We therefore feel that further detail about the designated body and the operation of the new Mandatory Reporting requirements is vital to understanding the impact of the Bill on the IWF's work.

6.7. Finally, this lack of clarity impacts on the overall work of the IWF. For the past 25 years, the IWF has been a world leader in the field. We have the operational infrastructure and best practice work processes which have made the UK one of the most hostile territories in the world to host online child sexual abuse material.

6.8. By not simply acknowledging that the IWF will be part of the solution, and what our new role will be, this has created a lack of clarity which impacts the IWF's day-to-day resourcing, relationships (including with our members), fundraising ability, and puts additional pressure and concern on our team of content analysts who already deal with some of the worst content imaginable online.

6.9. At present, there is little information about what is required of this designated body, the reports it will be responsible for processing, how many reports it may receive and how it should interact with Ofcom, law enforcement and the IWF.

7. Role of Ofcom-

7.1. Throughout the White Paper consultation process, we have supported the appointment of Ofcom as the Regulator for Online Safety.

7.2. However, we do have some areas of concern:

- How will Ofcom work with others currently working in this space domestically and internationally?

- The breadth of harms that Ofcom is being asked to regulate as part of this Online Safety Bill.
- Its technical understanding of the internet and illegal harms (and CSEA in particular).
- How will Ofcom seek to deal with complex international problems?

Co-operation with content regulators-

7.3. We recognise that Ofcom's role will be to look at the systems and processes companies have in place for dealing with harm and less about specific "content and harm". We believe that for the regime to be effective, Ofcom will have to work with a number of individual "content regulators" whose expert support, insights and knowledge will be invaluable to it in obtaining information about the extent of certain harms and where they might occur.

7.4. For example, the IWF is the UK-based, world-leading body for dealing with CSAM imagery online and is ideally placed to support the regulator in relation to this type of content. Other expert input may be required in relation to other types of content (such as terrorist content).

7.5. It appears that little consideration has been given to how these expert charities and bodies are going to be financially supported to respond to requests for information from Ofcom or supported financially to carry out the potentially burdensome duties on behalf of Ofcom within this Bill. Whilst Ofcom has taken some steps to cooperate with some of the largest domestic regulators in this space, such as the Information Commissioner (ICO), Competition and Markets Authority (CMA), through the establishment of the Digital Regulation Forum (DRCF), it has been much quieter on how it plans to co-operate with other organisations working in this space.

7.6. ***Further information from the Government and Ofcom on how it plans to partner with an already under pressure charitable sector and fund some of these outsourced activities would be helpful.***

Breath of harms in scope-

7.7. As set out in our introduction, the Government has consistently explained that it wants the highest possible protections to be in place for children. The IWF agrees that the focus of this Bill must be ensuring that we make the online environment safe for children. We believe that the Government and Ofcom should set out more detail about the priority areas for focus within the draft Online Safety Bill. It would be our suggestion that the Bill starts with areas where there is already good collaboration and laws to guide action such as CSAM and Counter Terrorism, before moving to areas that are much more complex and less well defined.

7.8. Given the amount of time it has taken the Government to bring forward this Bill, we are seeing calls for greater action on harms such as fraud, the racist abuse of footballers, the abuse of public figures, the sale of weapons online, to name but a few examples to potentially be included as harms in scope of the regulation.

7.9. ***The more harms the Bill seeks to cover, the greater the level of support we believe Ofcom as a regulator will need.***

Technical understanding of the Internet-

7.10. We recognise the significant benefits Ofcom brings as a regulator to Online Safety. Its strong track record in broadcast and telecommunications and accountability mechanisms to Parliament are all positives. However, as we stated in our response to the Online Harms White Paper, ***we felt that Ofcom would clearly have gaps in its expertise around understanding human rights and criminal law***.

7.11. Whilst Ofcom clearly understands regulation, regulating the internet is very different to broadcast or telecommunications.

7.12. The Internet has no spectrum limitations and has low costs to entry and vast amounts of content that is shared, curated and created. In addition to this, there are serious human rights concerns if state agencies seek to decide what content is allowed online (and offline) on a global network where information is abundant rather than scarce.

7.13. The scope of the Online Safety Bill also includes illegal harms, which requires a totally different response compared to harmful content. Again, this is an area which is not currently within Ofcom's area of expertise. This a complex area requiring specific expertise.

Use of Powers and Proportionality-

7.14. The Bill currently gives Ofcom significant powers which have the potential to significantly impact on the privacy of individuals. This applies particularly in relation to CSE/A as we know from the Government's full response to the Online Harms White Paper:

"The regulatory framework will apply to public communication channels where users could expect a greater degree of privacy- for example online instant messaging services and closed social media groups".[6]

7.15. The full response further states:

"Ofcom will set out how companies can fulfil their duty of care in codes of practice, including what measures are likely to be appropriate in the context of private communications."

7.16. The legislation will also enable Ofcom (the regulator), "to have the power to require companies to use automated technology that is highly accurate to identify illegal child sexual exploitation and abuse content or activity on their services, including, where proportionate, on private channels."

7.17. Whilst we welcome these steps, and we have long said it is possible to have both privacy and protect children, the impact assessment accompanying the draft Bill contains only five very short paragraphs on the impacts on the privacy of users. We feel that both the privacy of adults and children also need to be carefully balanced with the need to protect children. This is an area that could be further strengthened within the Bill to ensure that an appropriate balance is struck between privacy and safety.

7.18. Other pieces of legislation such as the Regulatory Investigatory Powers Act (RIPA) contain several safeguards within the text of the legislation, such as: the information is gathered for a specific purpose or individual investigation; the acknowledgement that an investigation may impact on a person's right to privacy or is conducted in an immediate response to an event or act. There are also several tests which must be met before the Home Secretary can enforce surveillance. We would call on the Committee to look very carefully at other examples of legislation such as RIPA to ensure that there are appropriate checks and balances contained in the Online Safety legislation.

Use of Technology Notices-

7.19. Chapter 4 of the legislation provides the statutory basis for Ofcom's power to require a service provider to use accredited technology to identify and remove CSEA content on both public and private channels.

7.20. Whilst we welcome the powers the regulator will have to direct companies to deploy services that clearly limit the spread of child sexual abuse material, we believe this section of the Bill requires closer scrutiny and poses some interesting questions:

---

[6] Online Harms White Paper: Full government response to the consultation - GOV.UK (www.gov.uk) point 29

1) How will Ofcom come to a view as to the prevalence of illegal material across a service? Will it rely on law enforcement and intelligence agency reports, and if so, how will the regulator preserve an independent role?

2) Clause 64 (b) refers to the use of "accredited technology" by companies on any part of their service (including both public and private). How will this be achieved if a service is encrypted, as currently there is no way of detecting this content in an encrypted channel? Some services in scope are end-to-end encrypted – is it the intention of the Bill to mandate decryption in some circumstances? What protections for privacy will be in place?

3) Clause 66 (3) states that the use of a technology notice may impose this requirement only in relation to the operation of a regulated service that (a) is in the United Kingdom or (b) as it affects United Kingdom users of the service. This could be practically difficult for large global companies to implement as most tools and services are currently deployed at a global level. Whilst we support the ambition to protect UK users from CSE/A what steps are being taken to ensure that this is technically possible, particularly with smaller companies who may not have the engineering capacity to carry out such a task?

4) Clause 66 (4) states that technology is accredited if it is accredited by Ofcom (or another person appointed by Ofcom) as meeting the minimum standards of accuracy. Clause 66 (5) defines the minimum standards of accuracy as being approved by the Secretary of State following advice from Ofcom. This leads to several questions, such as what do the public think is an acceptable level of accuracy? The recent debate in the EU around the temporary derogation from the e-privacy directive, has highlighted just how contentious the use of these technologies can be and it is important that there is a level of accountability and the right to appeal and redress in any inaccuracies with technology. Also, as we have mentioned elsewhere in this submission, neither Ofcom, nor the Secretary of State are technical experts in CSEA or as internet standards setting bodies. How will they make use of outside expertise when enforcing these notices, or even laying the groundwork for a potential breach that may then lead to them issuing a use of technology notice, if they cannot identify the extent of a problem with a platform?

7.21. ***We would urge the pre-legislative scrutiny committee to give greater thought to the Use of Technology Notices. These are technically complex challenges and pose significant questions about privacy, technical capacity and capability and will require an extremely strong level of technical knowledge and understanding of how platforms work and operate. It is vital that Ofcom has access to organisations who have:***

a) knowledge and understanding of the nature of harms it is potentially proposing a use of technology notice for, and,

b) an extremely high level of understanding about the platform it is proposing to serve a use of technology notice to, and

c) an understanding of whether what it is asking for is technically achievable.

Co-operation with law enforcement-

7.22. In the case of illegal content, the regulator will require a close working relationship with law enforcement. One area that is missing from the Bill is some form of legal protection for the regulator if it is going to regularly encounter illegal content in the course of its work and some form of process for referring illegal content to law enforcement.

7.23. Of course, if the IWF is co-designated as the relevant body for CSE/A then, this protection will already be in place through the Memorandum of Understanding between the NPCC and CPS.

7.24. The introduction of Mandatory Reporting (as raised earlier in this submission) will also require the designated body to have strong relationships not only with law enforcement in the UK but

also with other international law enforcement agencies and organisations dealing with CSAM. We think there are very few organisations with the technical, legal and welfare arrangements in place that can deliver this function in the UK.

7.25. ***Indeed, our view is that mandatory reporting can only be provided by either law enforcement, the IWF or a combination of these two organisations.***

Role of the Secretary of State-

7.26. The Draft Online Safety Bill gives a great deal of power to the Secretary of State in relation to illegal content (and in particular CSAM). Whilst we understand the rationale behind this, we think it is important that the Secretary of State obtains relevant and timely advice from CSAM experts before taking decisions in relation to CSAM, and that this should be provided for in the legislation.

7.27. In relation to CSE/A, the Secretary of State may direct that Ofcom modify a Code of Practice to ensure that this meets Government policy or for national security and public safety reasons (clause 33).We are concerned (and have previously raised this in our submission to the Online Harms White Paper) that this power could call into question the independence of the regulator if, as the legislation currently suggests, it must comply with the decision made by the Secretary of State. The biggest concern we have with this is that "government policy" is an overly broad phrase and could be used to exert control over Ofcom. The possibility of too much central government constraint on Ofcom could undermine Ofcom's independence as a regulator and its ability to draft, implement and enforce Codes of Practice in a politically neutral way.

7.28. ***It is our view that any significant changes to Codes of Practice should not be pursued without significant industry and Parliamentary consultation.***

7.29. The Secretary of State will also have the power in Clause 41 (which relates to the meaning of illegal content) to specify relevant offences (see subclause 4). This subclause specifies both CSE/A and terrorist offences but also includes in paragraph (d) other offences not within paragraphs (a), (b) or (c) where the victim is an individual. We think this is overly broad and could include offences contained in the Communications Act 2003 such as inciting violence, hatred, stalking harassment, cyberbullying and blackmail. Including these offences could further dilute and spread the legislation and the companies within scope of the regulation too thin. The intention of the Bill is to be risk-based and proportionate, tackling those harms greatest to children. The lack of clarity around future areas of illegal content, risks undermining the regime and risks services over censoring content or, worse, directing much needed moderation resources from areas of high harm such as CSE/A. This may also raise legitimate concerns about human rights.

7.30. ***We prefer a strong and clear focus on preventing and detecting CSE/A and terrorist-related offences and we suggest that paragraph (d) is narrowed or removed altogether.***

7.31. Some commentators have also commented that subclause 7 of Clause 41 is extraterritorial in scope. It states, "no account shall be taken of whether or not anything done in relation to the content takes place in any part of the United Kingdom", thus giving these offences if specified under subsection 4 (d) extra-territorial scope.

7.32. We urge the Government to limit Clause 41 to focus purely on illegal harms where clear legal definitions exist around terrorist and CSE/A content, where extraterritorial collaboration is therefore much more straight forward. This also ensures that the Bill very clearly focuses on putting child protection and national security at its very heart, as the Government has said it would do.

7.33. In practice, in the CSE/A space, most of this cross-border collaboration is already happening. Each year the IWF co-operates internationally with other agencies to remove vast amounts of CSAM that is hosted outside of the UK.

Funding-

7.34. ***The IWF believes it is important that the online safety regime is established with a clear, transparent and sustainable funding regime. This will ensure that any regulatory interventions in relation to CSAM will be sustainable, consistent and practical, to enable Ofcom to achieve long lasting and effective change.***

7.35. As we have mentioned elsewhere in our submission, we believe that it is important that any current voluntary-funded initiatives from the internet industry continue and that any regulatory levy is not unnecessarily burdensome on industry. We have stated that a large reason the IWF has been a success is that on a voluntary basis we have been able to leverage funding from the industry to tackle child sexual abuse online. Without this industry funding, we would not be able to take reports from members of the public, proactively search the internet and work with technology companies to generate the latest technical tools and services that are so vital to tackling the problem and keeping platforms free from CSAM in the UK.

7.36. We recognise that as a result of regulation, it is likely that more companies will want to become members of the IWF. This is because most of the technical tools and services we offer to the industry will go some way to ensuring compliance with the new regulatory regime, but it is possible that small and medium sized businesses simply won't be able to afford a regulatory levy to pay for the regulator *and* pay for membership of the IWF. The Secretary of State and Ofcom should therefore think carefully about who should pay the levy and the impact this will have on voluntary initiatives.

7.37. The IWF is, however, also proposing a new regulatory arm to assist Ofcom with the functions proposed in point 5.14 of this submission and clearly these new responsibilities will require some form of funding from the regulator. It should be stressed that these are ***new*** functions that are not currently performed by IWF, and it should be noted that under this model there would need to be clear separation between the activities of the IWF's regulatory functions and the IWF's charitable functions.

7.38. ***This is vitally important in order to maintain effective working relationships and trust with the industry.***

8. Is the Duty of Care approach in the draft bill effective?

8.1. We welcome the introduction of a duty of care for providers of user-to-user services and search services. We see the clear focus Government has given to the importance of safeguarding children through Clause 9 on ensuring a specific safety duty for illegal content (including CSAM).

8.2. We are particularly pleased to see that there is focus on harm to individuals in relation to the safety duty for illegal content, and that companies will be responsible for ensuring they have proportionate systems and processes in place to:

- Minimise the spread of illegal content on their platforms;
- Minimise the length of time illegal content is live for;
- Minimise the dissemination of this content;
- Ensure this content is removed quickly when it is discovered.

8.3. We believe that this approach is incredibly positive. Many of the obligations under this safety duty for illegal content are already provided for via membership of the IWF. We believe that through the technical services we offer to industry, this is both technically possible and relatively straightforward to implement, with most of our membership already taking these steps to protect children and control the spread of illegal CSAM on their platforms. As explained in this submission, we propose broadening the IWF's role with the creation of a regulatory arm, performing specific functions on behalf of the regulator.

8.4. We also believe that this regulatory duty will give opportunity to further enhance the response. We refer to subclauses 4, 5 and 6 of clause 9 which mean that companies must have clear terms and conditions, apply them consistently, and conduct an illegal content risk assessment. We believe that this is something the IWF could further assist our members with in meeting their compliance obligations in the future.

8.5. Whilst we welcome subclause 6 of clause 9, we are concerned that paragraph (b) includes the size and capacity of the provider of a service in determining proportionality of a service's systems and processes.

8.6. ***Throughout much of our work, we see large amounts of CSAM content hosted on smaller providers such as image hosting boards and cyberlockers, hosted largely in the Netherlands. Often these smaller, lesser-known, services are a huge part of the problem. Whilst we understand Government wants to ensure that regulation is not overly burdensome for smaller companies, we believe that in the case of CSAM there should be a zero-tolerance approach to the hosting of this content, regardless of size.***

8.7. The Government has also enhanced the Duty of Care by providing specific safety duties in relation to services likely to be accessed by children in Clause 10. The IWF would hope that this duty is closely aligned from a regulatory perspective with the recent passage of the Age-Appropriate Design Code which ensures that companies mitigate the risks to children by age gating content on their platforms. This regulatory alignment, however, is not clear from the face of the Bill and we would urge the pre-legislative scrutiny committee to seek clarity from the Government, Ofcom and the ICO on the regulatory alignment of this clause with the Age-Appropriate Design Code.

8.8. One challenge that remains within this legislation, however, is how we age verify or age assure users, something we will of course return to later in our submission.

8.9. Whilst we welcome the implementation of clauses 9 and 10 and the separation of the various duties on companies, what is missing at present is clear guidance from the regulator about how a company is supposed to discharge its duty of care to its users. It is therefore essential that Ofcom has a strong technical understanding of what is possible when developing its guidance in relation to the illegal content duty. **Ofcom will need to work closely with acknowledged CSAM experts, including the IWF.**

Definitions-

8.10. The definitions contained in the Bill is one of the areas of the Bill which requires scrutiny during the pre-legislative phase. Clause 43 of the Bill sets out the legal definitions for CSE/A and further information is contained within schedule 3 of the draft Bill.

8.11. One of the concerns the IWF has with this legislation, is the definition of 'CSEA offence' in clause 43 and schedule 3 of the Bill. Our concerns are:

a) There is potential for amendments to this definition either by the Secretary of State or by the Scottish Ministers. We want to emphasise the need for consistency in how CSEA offences are defined in the Bill. This is important because it impacts how the duties around illegal content will operate in practice. We want to ensure implementation of this part of the Bill is as straightforward as possible. Whilst we understand that the devolved administrations have slightly different laws governing CSE/A, it is important that the Bill applies consistently across the UK. The IWF acts as the hotline for the whole of the UK and whilst we have good working relationships with the devolved administrations, we are concerned that should one administration make changes to their part of schedule 3 (for example by adding or removing offences), this could make dealing with CSE/A content more complex and complicated. Schedule 3 currently includes several offences which would not fall within the IWF's definition of CSAM or CSE/A, when conducting its role of removing child sexual abuse images and videos from the internet.

b) Clause 45 of the Bill is also problematic in its definition of content that is harmful to children. Subclause 5 of this clause states: "*content is within this subsection if the provider of the service has reason to believe that there may be a material risk of the fact that the content's dissemination having a significant adverse physical or psychological impact on a child's ordinary sensibilities.*" Whilst we understand and support the Government's ambitions to ensure that companies act on content that falls below the criminal threshold for action that is distressing for children, we do believe that this definition needs to be further refined and clarified. It would be our preference that this is addressed on the face of the Bill rather than leaving it to Ofcom to produce guidance on what this might mean in practice. A tighter definition of what meets this threshold for 'harmful' to children, will make moderating this content much easier for the IWF's analysts and content moderators (and for industry to apply).

c) One of the biggest challenges for the IWF is how we deal with self-generated images of children, self-referred to us that do not currently meet the Category C sentencing council guidelines (2014) for removal. Clearly this type of content and its dissemination could have "a significant adverse physical or psychological impact on the child" and therefore be dealt with under Clause 45 of the legislation, although equally, such images could also constitute a CSE/A offence under Clause 43, for example if an adult had encouraged the taking of such content. Often it is extremely difficult for the IWF analysts to reach a judgment about the conduct of an image (i.e., how it was produced) and are having to make a judgment on the content of an image (what they see and how it meets a clear legal threshold.) This separation could make content moderation much harder in future and much more difficult to define the spaces in between illegal and harmful content. ***This matters, because every image we grade as illegal is added to the UK Child Abuse Image Database (CAID) and could be used in a court of law as evidence to convict a person of being in possession or distribution of indecent images of children.***

9. What's missing from the Bill?

Age verification for adult websites-

9.1. It is disappointing that the draft Online Safety Bill, section 131 (2), repeals Part 3 of the Digital Economy Act (2017). Whilst we recognise that the Government has taken steps to ensure a platform verifies or assures the age of its users and age gates content appropriately through Clause 10, for example, and other associated measures, we are concerned that adult pornographic websites are not covered at all within the scope of the Online Safety Bill.

9.2. We believe it is not right that an Online Safety Bill is introduced, which deliberately repeals a piece of legislation that would have made children safer online from content that is developmentally inappropriate for them and that this must be addressed through the pre-legislative scrutiny process.

9.3. Research published by Revealing Reality following consultation with children and young people on behalf of the BBFC, states that 62% of children in the 11-13 age range who have reported seeing pornography have done so unintentionally. The report also states children are as young as 7 when they first come into contact with this content online.

9.4. The research went on to suggest that there were three different routes into the viewing of pornography: (1) through search engines, (2) through social media and (3) through dedicated pornographic websites. The Government appears, through the Online Safety Bill, to have taken steps to address the issue both on providers of user-to-user services and search services but appears to have left the door wide open for pornographic websites which do not host user-to-user interactions.

9.5. The former Secretary of State, Oliver Dowden, said at a recent appearance before the DCMS Select Committee that if a way could be found to cover the sites in scope of the Digital Economy Act in some sort of commensurate way, then he would be open to suggestions and amendments.

9.6. We understand that this is a complex area to regulate. Age Verification technologies, we recognise, are in their infancy and we recognise too the privacy concerns of individuals. The statistics and the impact of online pornography, however, on the lives of children and young people, and their ability to form healthy relationships as a result, is something which should be addressed through the online safety bill.

9.7. ***We would urge the pre-legislative scrutiny committee to carefully consider and hear further evidence from relevant stakeholders on how this might be best achieved.***

10. Conclusions-

10.1. In conclusion, the draft Online Safety Bill is an extremely long, complex and complicated piece of legislation, which has taken some time for us to reflect on, review and provide a response to. The design choices in the legislation, such as several different duties of care (for children, adults, illegal content etc), have made this legislation more complex and are currently lacking clear definitions, which will make content moderation much more difficult. The Bill could instead have set out one overarching duty of care. This complexity is further increased by the introduction of competing duties to consider freedom of expression and journalistic content. Similarly, Ofcom is conflicted by being required to consider the economic impact of its decisions. We understand that internet regulation is complex and must consider a wider range of factors, but the legislation could have been designed in a more simple and straightforward manner.

10.2. We believe that it is important to acknowledge the huge benefits the internet has to offer. There is no doubt that this generation of children are better connected, informed, have greater access to information, and are more entertained because of the internet than those that have been before them. This can be easily forgotten in the work we see at the IWF on a daily basis. We only see the darkest side of the internet and of the harm that is done to children.

10.3. We must remember to talk about the huge benefits that the internet has brought to children, whilst trying to improve their online safety. We believe, as the Government has said, that children should sit at the heart of this Bill and that the highest possible protections are put in place to ensure their safety. Anything short of this would be a missed opportunity.

11. Annex 1- The IWF's proposed model of regulation for CSE/A-