Online Harms White Paper Response

Organisation responding: The Internet Watch Foundation (IWF)

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

Contact details of person responding: Michael Tunks, Policy and Public Affairs Manager,
mike@iwf.org.uk 01223 20 30 30

Scope of the response

The IWF's remit is distinct and limited to tackling illegal content, specifically online child sexual abuse material hosted anywhere in the world and non-photographic images of child sexual abuse hosted in the UK. For this reason, our response to the Online Harms White Paper is limited to this specific area. We also want to be clear that our response is based on what we believe to be in the interests of those who have been abused and had their suffering compounded by having their imagery shared online. We have also consulted our independent Board and 148 Members in producing this submission and will be continuing to discuss the future role of the IWF in the new regulatory framework with them all as well as the Government over the coming months.

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.

Our work is funded almost entirely by the internet industry: 90% of our funding comes from our 148 global Members which include 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 as well as some of the smaller operators within the internet ecosystem who pay as little as £1,040 per annum yet still access everything we have to offer.

The remaining 10% of our funding comes directly from the European Commission's Connecting Europe Facility for our role within the UK Safer Internet Centre, providing a Hotline resource for the UK.

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

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 judge, every two years and the report published in full.

Introduction

We welcome the Government's Online Harms White Paper and the opportunity to contribute to the new proposed regulatory framework. We particularly welcome action taken by both the Home Office and Department for Digital, Culture, Media and Sport to ensure that there is engagement with stakeholders, and for affording us the opportunity to contribute to those discussions.

Scale of the CSEA challenge online and its impact on victims:

At the Independent Inquiry into Child Sexual Abuse (IICSA), evidence from law enforcement stated that there were at least 100,000 people in the UK accessing indecent images at any one time.

Despite our impressive record in reducing the amount of content hosted in the UK from 18% in 1996 to 0.04% in 2018, people in the UK are still accessing images hosted elsewhere in the world. Last year the IWF removed 105,000 URLs showing the sexual abuse of children - a 32% increase on the previous year (2017). Only 41 of those URLs were hosted in the UK. As each URL can contain from one to thousands of images, this equates to the removal of millions of images and videos.

Most of the images and videos actioned were duplicates of previously detected child sexual abuse material (CSAM). Our analysts know only too well the impact that a child's image circulating online can have. In some cases, our analysts watch a victim grow up online as they are robbed of their childhood and subjected to vile abuse over many, many years. Our 2018 annual report followed just one child, Olivia, over a period of three months and even though we know she was rescued five years ago, we saw images of her aged from three years to eight years old on average five times per day, and in three out of five of these images she was being raped or sexually tortured.

It is vital for Olivia, and others like her, that this imagery is stopped from circulating online. Every time an image is viewed online it repeats the suffering for victims. It is vital to victims and survivors of abuse that they know there is someone out there working on their behalf to ensure that their abuse images are removed as swiftly as possible, and that everything is being done to have them permanently removed from the internet. The swift and effective removal of content is also within the public interest. If imagery is removed and not readily available on the clear web, it then becomes possible to prevent offences (of viewing indecent images of children) from happening in the first place.

The position and future role of the IWF

We want to make clear that our position is fundamentally about doing what is best for victims and survivors of child sexual abuse and that these interests come first, above any self-interest or preservation.

Despite our work in reducing the amount of known child sexual abuse material in the UK, we are conscious that further challenges still exist, and we are committed to playing our part in making the UK the safest place in the world to go online and discussing with our Members, Government, law enforcement and the new Regulator what more we could do in the future to assist.

Any future regulatory framework must build upon current working practice in order to improve the service that is given to victims and survivors of CSEA.

Need for technical expertise:

We are keen to share our 23 years of experience and technical expertise by assisting the Government and the new Regulator in developing the proposed CSEA Code of Practice. We believe that this should be principles-based, developed in partnership with the IWF and internet companies and subject to public scrutiny through the use of Parliamentary Select Committees. It has also been raised with us that whilst the interim Codes (CSEA and Terrorist content) – proposed for sign off by the Home Secretary – create an opportunity for companies to get ahead of regulation and trial new approaches before the introduction of the Regulator, this could also conflict with the independence of a Regulator.

Over the past 23 years the IWF has evolved, improved and expanded to meet the growing threats of the online world and our record shows that we clearly know how technology changes, evolves and works. We provide a vitally-needed, safe, secure and private forum for companies to talk about the issues they have with child sexual abuse material on their platforms. The new regulatory framework must encourage companies to continue sharing their experiences and solutions and we believe that they are best placed to do this through the IWF. Our membership fees are based on a sliding fee structure, dependent on the size and sector of each company. This means that the very largest tech companies pay the most, the smaller ones pay the least and that all companies, regardless of size, benefit from all of the skills, products and services that we provide.

Build on current regulatory arrangements:

We would urge that the Government carefully considers the scope of the harms proposed within the White Paper. With no less than 29 online harms that the Regulator is proposed to be responsible for regulating, it will require significant resources, potentially significant public funding and investment and will almost certainly require the Regulator to work with those who have an understanding in these areas, at least initially if nothing else. We would therefore encourage the Government to look to existing effective regulatory solutions such as the IWF, and respectfully ask that the proposed new regulatory framework complements and does not damage existing approaches, as well as continuing to encourage and preferably enhance the sharing of information on this issue amongst the companies.

We believe that there is a vital role for the IWF in a new regulatory framework. IWF is able to act as a conduit between the companies and the Regulator in terms of the provision of services. It can also act as a conduit between the Regulator and government, being able to provide much needed technical advice on the art of what is possible. IWF also brings a proven and effective delivery mechanism with its own purpose-built existing technical infrastructure.

In short, we believe that the IWF already provides an effective solution which is respected across the globe. On the basis that we are fundamentally part of the future solution, it is important to consider how the business model of the new Regulator would impact on us, being that we are 90% funded by industry and 10% funded by the EU. Our concern is that government may seek to levy money from the industry to pay for the Regulator, and that without careful consideration as to how this is done, it may impact on existing initiatives, such as the funding we receive directly from industry. In turn, this could have a catastrophic impact on the amount of child sexual abuse images we are able to remove from the internet.

The IWF brings clear public benefits;

- We provide the public with a place to anonymously report suspected CSAM not just in the UK but also in 27 other countries, with an expected 50 countries by the end of 2020.
- We have removed millions of criminal images and videos.
- We remove 45% of content we identify as hosted in the UK in under two hours, with our fastest removal time being under four minutes.

- We are the only non-law enforcement agency to have a connection to the child abuse image database (CAID) and we assist law enforcement with speeding up their response by grading and sharing image hashes with industry.
- We have assessed 500,000 images for law enforcement and provided vital evidential information which has led to the rescue of children from abuse and the prosecution of offenders.
- We create and develop the right technology which directly benefits victims and disrupts offenders. We do this by bringing together industry tech experts to work with our technical team and analysts. We then share this technology with our Members to multiply its benefits.
- Our technical services are deployed across the world, ensuring people are protected from accidently stumbling upon CSAM and disrupting the distribution and behaviour of the perpetrators.

Global nature of the internet:

We understand that the internet operates on a truly global basis and if the new regulatory framework is to be successful, the UK Government must consider how it operates within an international context. Challenges such as how to get companies that are based abroad and outside the jurisdiction of UK law to comply with the UK Regulator need to be carefully considered. The UK Government also needs to pay attention to existing laws and legislation such as the European Union E-commerce Directive and the Child Sexual Abuse Directive, which are likely to be retained after the UK leaves the European Union, and ensure that any future regulatory framework complies with these laws or at the least does not come into direct conflict with their application.

The IWF has a great deal of experience in international co-operation. Our membership base is truly global, and our services are deployed internationally by companies. We utilise our international connections through the INHOPE network and our contacts within law enforcement globally to remove content that is hosted outside of the UK.

Because the White Paper proposes regulation only within the UK, this could potentially lead to a fragmented model of internet regulation where each country creates its own laws, which companies must comply with. This could impact on current models for international collaboration. The UK Government should consider discussing this potential impact with international partners, initially through the Five-Eyes arrangement and with the European Union in particular.

The IWF is also working internationally in countries that cannot afford to have their own hotlines by establishing reporting portals in the most under-developed countries in the world, with support of a grant from the Global Fund to End Violence Against Children. We aim to have 50 reporting portals established by 2020 and we are currently operating portals in India, Tanzania, Zambia, Uganda, as well as all 13 British Overseas Territories.

The way the IWF was established means that our quality and judgment is held to the highest possible standards and accountability by the industry, law enforcement and government, who act as an effective check and balance. No other charitable organisation possesses the technical expertise of the IWF, the links and trust with industry and the ability to convene safe confidential spaces between these stakeholders to debate challenging ethical and technical issues related to protecting children from online sexual abuse.

Conclusion:

The IWF brings skills, knowledge and experience which will be essential to an effective new regulatory landscape and is keen to play its part in helping to shape this, mindful that the most important thing is to achieve the mission of eliminating online child sexual abuse material. Specifically, there are several things we believe we could do to assist the Government:

1. **Helping to shape the CSEA Code of Practice, by brokering discussions between the Government and those organisations, such as ourselves and our Members, that have the technical knowledge skills and expertise in dealing with CSEA.**

2. **We are open to discussing with our Members the possibility of taking on additional responsibilities related to CSEA such as grooming and live streaming to assist the Government, law enforcement and the new Regulator.**

3. **We are committed to sharing our skills and expertise with others to play our part in developing the new regulatory environment.**

As a final comment, the reason the IWF has been able to be so effective to date is because we operate within a clearly defined legislative framework and where our harm is clearly illegal. It is our belief that the UK has some of the strongest child protection laws anywhere in the world and we welcome the fact that the Government is exploring how to strengthen them further.

Online Harms White Paper positives:

We welcome the ambition and intent of the White Paper. We are particularly pleased to see that it has a strong focus on tackling the issue of online child sexual abuse and exploitation and that this includes a focus on new and emerging challenges in this space.

Live streaming and grooming:

We are prepared to explore the feasibility of extending our current remit to take into account grooming and live streaming, in consultation with our Members. We can use our 23 years of world-leading experience in dealing with child sexual abuse images and videos online and the unique, independent and trusted position we have created in that time in order to conceive a solution to tackling grooming and live streaming with industry, law enforcement and Government for the benefit of children in the UK and across the world. Live streaming and grooming currently sit outside the remit of the IWF but are clearly posing significant challenges to the safety of children online, as our research in partnership with Microsoft on captures of live streaming has demonstrated. We are concerned about both, and we are also acutely aware that there is not yet a viable technical solution for these two issues. We are ready to assist government, industry, law enforcement and the new Regulator as and when solutions do become available.

Regulator and Code(s) of Practice:

We welcome the Government's intention to introduce a Regulator and Code(s) of Practice, which will assist companies in defining what is expected of them and recommendations made about their effectiveness at dealing with illegal and harmful content that arise on their platforms. Any proposed legislation that helps achieve our mission of an internet free from child sexual abuse and exploitation is to be welcomed. We believe that the proposed Code(s) of Practice should be developed in partnership with the companies and others, such as ourselves, who have technical expertise in areas of specific harms. We also believe that there should be sufficient public scrutiny of the Code(s) of Practice with the possibility of Parliamentary Select Committees playing a role in scrutinising these codes to ensure that the privacy rights of individuals and free speech considerations are taken into account and balanced fairly and proportionately alongside the rights of children.

Transparency and accountability:

We support calls for greater transparency and accountability, and with the support of our Members, we are currently reviewing our own arrangements and considering some of the recommendations from the White Paper and the draft Code of Practice for CSEA. It is clear from recent public opinion surveys carried out by Ofcom that there is a greater demand for rigour and accountability from the public in how technology companies are dealing with challenges of illegal and harmful content on their platforms. The public want a greater level of awareness and understanding of

what companies are doing to protect them and the dangers of the harmful side of the internet[1]. Transparency and Accountability is a well-established regulatory principle that applies to other regimes at present. One example of this would be Ofcom publishing information on how telecommunications companies handle complaints and network issues. This would be a consistent approach were it to be applied to the newly-proposed regulatory framework.

Education of vulnerable and curious/offender groups:

We are also pleased to see that the Government has focussed not only on the new online regulatory framework, but the White Paper also includes a section on empowering internet users to keep them and their children safe online. As the White Paper highlights, initiatives such as an online media literacy strategy are important in getting people to critically engage with, understand and question what they are viewing online.

We believe that there needs to be a better approach to sex and relationships education in schools and in particular, a more open dialogue with girls aged 11-13. Sadly, self-generated imagery now makes up one third of all the child sexual abuse content which we remove from the internet. Of that third, 82% of that imagery features the 11-13 age range and 99% of that is girls.

To support CC Bailey's request for a joined-up approach, the IWF is calling for a national "Prevent" campaign aimed at young men in the 18-24 age range. We know these young men make up the largest group viewing Indecent Images of Children (IIOC) on the clear web and we want to stem their viewing habits before they graduate to more extreme content. Much more can and should be done to prevent people from ever viewing indecent images in the first place. The Government's CSEA Code of Practice detailing possible action from companies, schools, law enforcement and professionals working with children should be a vital first step to achieving this.

Principles-based approach:

We are pleased to see that the Government has taken, in the main, a "principles-based" approach to regulation and not attempted to be overly prescriptive regarding the way to deal with internet harms. Overall, the UK Government should be commended for being one of the first governments in the world to publish proposals for a regulatory framework of internet regulation and commended in their overall approach to this White Paper. There are many good aspects to the paper as well as many details still to be worked through.

Flexibility of legislative and regulatory response:

We are also supportive of the Government's attempts to address the spectrum of harms, and that different harms may require different legislative and regulatory responses. This flexibility will be vital in ensuring that the new regulatory framework is able to co-exist alongside, or in partnership with, and complement existing regulatory solutions like the role of the ICO on data protection regulation for example.

Challenges with the Online Harms White Paper

Technical challenges and the speed of change on the internet

Despite the Online Harms White Paper's positive points, we believe that the Government still has some way to go in providing further detail and clarity to industry, other Regulators and others operating in this fast-paced environment. It is an ever-evolving, technically challenging and complex space and it is important that the introduction of a rigid regulatory framework does not have unintended consequences.

[1] https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/internet-use-and-attitudes/internet-users-experience-of-harm-online

We are clear that given the speed of change on the internet, the new Regulator must be given space to determine what the right regulatory responses may be and ensure that they are proportionate and flexible enough to respond to future technical challenges online. This cannot be achieved in isolation and the new Regulator will need to draw upon the expertise and experience of the engineers and others already working in this space (in companies, NGOs and law enforcement) in order to maximise the benefits of this new regulatory framework. The Government should also carefully consider its use of primary legislation and its application to the online world. Whilst we recognise the importance of technology that is designed democratically and with effective public scrutiny, this should not slow down the pace at which the industry is able to develop and grow. Doing so could significantly damage the competitiveness of the UK tech sector; a balance between these two issues must be found. Given that technology significantly outpaces legislation, and primary legislation is much more challenging to amend or reverse in the event of technological change, the Government and Regulator should seek to make as much use as possible of secondary legislation and codes of practice.

The Regulator will need to establish strong, positive and effective working relationships with the industry. Therefore, the Regulator **must** be truly independent from Government and free from political interference in the way that it operates, if it is to be making judgments on issues such as free speech. There is also a need to ensure that whoever is entrusted to carry out this work is significantly resourced and well equipped to manage expectations about the role the Regulator is expected to fulfil.

The Regulator will require a deep technical understanding of the global internet landscape and of the complexity of different sizes and types of organisations and how they operate within the internet ecosystem. The IWF has significant experience of working with all types of companies across the internet ecosystem and has developed tailor-made services to meet the needs of the different platforms. We understand how the internet works and are a body trusted by industry, law enforcement and Government in the work that we undertake. Our services are all quality assured. For industry to take services, which they do on a voluntary basis, they need to have total confidence in the quality of those services and trust the assessment of the IWF. Likewise, for content in the UK, Government and law enforcement trust us to carry out Notice and Takedown procedures.

The Regulator will need to provide clear guidance on how a company will be deemed to be discharging its duty of care. The Regulator must be in a position to understand whether a company really is doing all that it can to prevent the spread of illegal and harmful content on its platforms or whether the tools and services provided are not applicable to their services/platform in order to draw meaningful conclusions that can be communicated to Parliament and the public. This technical understanding will be crucial to understanding not only the current debates about technology and content regulation, but also future debates. The IWF, through its regular dialogue with companies and in its ongoing transparency and accountability reviews, will be able to assist the Regulator and companies in ensuring compliance with the new code.

The internet is a fast-moving and changing landscape and the Regulator needs to ensure that there is flexibility built into everything it does to ensure it remains relevant. This is perfectly illustrated by the current issues around the increasing use of encryption and the DNS over HTTPs (DoH) debate. In the 12 weeks that this paper has been out for public consultation, there has been an increasing number of media articles and questions in the Houses of Parliament that highlight the challenges that the implementation of this technology will have for measures such as age verification and the blocking of illegal content, none of which is referenced within the Online Harms White Paper. These are just some examples of how quickly online technical challenges can emerge and how quickly regulatory responses will need to react to these issues.

Funding the Regulator

It is essential to carefully consider how the new Regulator will be funded. This exercise should look at the whole ecosystem of dealing with online harms, and how existing, effective, systems are funded. Our concern is that if Government seeks to levy money from the industry to pay for the Regulator, that

without careful consideration as to how this is done, it may impact on existing initiatives, such as the funding we receive directly from industry. In turn, this could have a catastrophic impact on the amount of child sexual abuse images we are able to remove from the internet. We would like to see a system that ensures all initiatives are properly resourced with no negative impact on any one.

The International Dimension:

There is a need for an international approach to illegal and harmful content. The internet is, by its very nature, a global tool, but this has to be seen as the starting point for a conversation that moves us towards a more global, collaborative solution for how we deal with online harms.

The amount of child sexual abuse images and videos hosted in the UK is less than 0.04% - a mere 41 URLs – whereas in 1996, the year the IWF was founded, 18% of the world's known child sexual abuse images and videos were hosted in the UK. Whilst we now have a world-leading and effective regime for dealing with these hosting issues in the UK, this does not stop our residents from accessing this material hosted elsewhere in the world. For example, in 2018 of the 105,000 webpages removed, 48,900 (47%) of these were hosted in the Netherlands.

82% of the content removed was found on image hosting companies, who are typically not members of the IWF and not operating in the UK and therefore out of scope for the new Regulator. The IWF adds imagery found on these platforms to its URL blocking list to ensure that innocent internet users do not stumble across content we have assessed to be illegal, as an interim measure whilst we pursue removal at source (the most effective way of removing content) through other hotlines and law enforcement. What this means, in reality, is that the problem of tackling CSEA must be one of international approach and partnership with not only industry but also law enforcement and governments across the globe.

Several companies have told us of the difficulty in creating technical solutions which meet the proposed UK Government regulatory requirements because their operation is based globally. Their preference would be for an internationally agreed approach to regulation. As well as the technical challenges this raises, there are legislative ones too. Just one example of this would be legal definitions and standardisation of what constitutes an 'illegal' image and its severity which can vary from one country to another.

As a priority, the UK Government should discuss with countries such as Canada, New Zealand, United States and Australia at its upcoming Five Eyes Summit, the creation of an agreed international standard for categorising illegal CSEA. As there is currently no agreed international standard categorisation of illegal CSEA, it limits the ability to share data and technical solutions across the world. Whilst the UK continues to be a member of the European Union and, indeed when it leaves, the UK should also be seeking to influence a new standard for Europe that complements anything that may be agreed with the Five Eyes partnership, which will be particularly important as the EU is now responsible for the most hosting of CSAM content globally. The IWF recently attended a European Commission workshop on this issue and would be happy to share its learnings with the UK Government and to continue using its technical and international expertise to assist the European Commission.

As a first step, the up-coming Five Eyes Summit, to be hosted in the UK, could be used to work out the collective approach to improve all our responses to online harms. The Five Eyes Summit can look to encourage buy-in from elsewhere and encourage the sharing of information between countries for maximum global impact in dealing with CSEA. If the UK is serious about its ambition to make the UK the safest place in the world to go online, it must work with other countries to achieve this objective.

Scope:

The Online Harms White Paper refers to no fewer than 29 different online harms that the Regulator will have to consider. It will be essential to define clearly what each of these harms are and what the expectations of the Regulator are with regards to them.

This issue has been raised to us during discussions with our Members who want greater clarity on the definition of who and what is in scope of the White Paper and therefore answerable to the new Regulator. The size of the challenge should not be underestimated. The burden on small and medium sized businesses should not be underestimated and the Government should look to create a system which is as easy as possible for small and medium sized businesses to navigate. The IWF's current membership structure is a good example of how smaller companies can easily comply with the law, and we discuss this in our introductory remarks to this response.

Much of the previous Green Paper debate had focussed on the role of content regulation on social media and on the challenges of dealing with legal but harmful content. There are two main concerns with the current scope of the paper:

Firstly, there is a concern that this is a regulatory environment that has been designed primarily for social media and then extended to fit and encompass other parts of the internet. There are significant challenges to this approach. For example, requiring ISPs to monitor all the content going over their networks will require changes to the law and be extremely costly. This could also be technically impossible if DNS over HTTPS was to be implemented.

Secondly, the Government is consulting on the inclusion of private communications providers. It can be difficult to define and draw the line on what is public communications vs private communications and perhaps more thought needs to be given to the scope of the companies and the sorts of regulatory regime and requirements that they will be subject to. The Government must pay careful attention to current laws and legal frameworks in this area including Article 15 of the E-Commerce Directive and many other well-established international treaties and UN commitments the UK Government is a signatory to. This includes the UN Declaration on Human Rights and, Article 12, of that declaration of an individual's right to interference with their privacy, family, home or correspondence. One way that the Government could begin this discussion would be to focus on the issue of User Generated Content (UGC) which is a manageable and understandable definition for everyone to start from.

Legislative challenges:

Careful consideration must be given, and appropriate attention paid, to the existing legal frameworks in the design of the new regulatory landscape to ensure that current efforts are not disrupted, or overly burdensome or unachievable, and that unrealistic requirements are not placed on business which could ultimately harm the vibrancy of the digital economy in the UK. Linked to the above issues outlined under 'scope', there are legal implications to the introduction of a new regulatory framework. As the White Paper correctly identifies, the current liability regime in the UK is derived from the European Union's E-Commerce Directive. We believe that this is a vital piece of legislation in ensuring companies remove illegal content from their platforms once they have been notified. The White Paper continues to state that whilst it is important to ensure that companies have the right liability for illegal content, it is not the most effective mechanism for driving behavioural change of companies. Whilst we agree with this and stress the importance of a need for dialogue with the companies, one of the biggest issues is that if ISPs are going to be asked to actively monitor their networks in the future for content this would be in direct conflict with Article 15 of the directive. This proposed legislation, however, does create some opportunities to encourage greater collaboration and clarity between existing solutions, which we would encourage the Government to think further about. Any proposed changes to legislation could have the potential to impact on the role, function and ability of the IWF to remove content.

We are also aware that following the recent European Parliamentary elections, that there is the possibility of the E-Commerce Directive being reviewed by the European Commission. **Whilst the UK is still a member of the European Union, we would encourage an urgent dialogue with the European Commission on how any changes to the E-Commerce Directive may impact on this new regulatory environment being proposed in the UK.**

The Government should give more thought as to the detail of the proposed "duty of care" and its application to the online world. Whilst there are good examples of how this operates in the offline world, with the health and safety executive for example, how this operates in the online environment, is not quite so straight forward. Many of the Government's proposals within the White Paper would still be quite subjective judgments. Some of the steps taken by companies may be, in effect, self-regulatory and it will be important for the Regulator to have the power to be able to differentiate between the harms and how companies meet the compliance standards expected of them.

From an IWF perspective we welcome the inclusion of file sharing sites, image hosting boards and cyberlockers as this is where our analysts find more than 87% of the content that we get removed from the internet. However, the challenge with this, as raised above, is that many of these companies tend to be hosted outside of the UK and therefore outside of the jurisdiction of UK law. Thought needs to be given as to how you force some of these smaller companies, where the problem exists in vast quantities, to comply with the Regulator and UK law when they have often traditionally been beyond the reach of law enforcement or the hotline of the country within which they are operating.

Question 1:

This Government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the Government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

The IWF believes that transparency and accountability is vital to building up a true picture of the scale of the challenge that tech companies are facing in tackling illegal and harmful content on their platforms. This is far from a straight-forward issue and initial attempts by DCMS in the Internet Safety Strategy to define a reporting template for companies highlighted just what a challenging task this is.

The IWF believes that the new Regulator should be responsible for setting principles about what companies are expected to do and how they are expected to do it. Two key principles we think the Regulator should be tasked with are:

1. Clearly setting out the responsibilities of the companies.
2. Assessing what processes they are deploying and communicating what impact they will have with the public and Parliament.

There is a lack of a standardised approach internationally to reporting on online harms. Until now it has been largely left to the companies to produce their own transparency reports and there needs to be more of an agreed standard that companies can be compared to and to ascertain the size of the problem on their platforms. From an IWF perspective, if the UK Government was able to work with other governments around the world to define an international standard for CSAM it would make it much easier for the companies to report on this issue. We would be happy to offer our expertise on these issues.

The Regulator also needs to carefully consider the obligations that transparency reporting would place on certain companies, particularly small and medium sized enterprises. As the White Paper establishes, companies have varying capabilities based on their size and resources and this must be reflected in future reporting arrangements to ensure smaller and medium sized companies are not disadvantaged. The Government needs to carefully consider the impact that reporting requirements have on the vibrancy of the digital economy if the UK is not to drive digital start-up businesses abroad. We therefore welcome the Government's commitment to a duty to encourage innovation and to provide additional support to small businesses.

It is also vital that the Government utilises current mechanisms for engaging with companies about the challenges that are posed by internet harms. The IWF regularly convenes industry, law enforcement and companies together and more needs to be done to improve the dialogue further with smaller companies. The Government or new Regulator must create a culture where companies feel

like they can talk to them and open up about issues on their platforms without the fear that they are going to be prosecuted, fined and publicly named and shamed before being given the help, support and access to vital information and services that they require. From our experience we have found that working constructively with companies to solve their issues is the most effective way of creating the required changes and impact.

As a result of some of the recommendations in the Online Harms White Paper, the IWF is currently consulting with its Members and an independent consultancy on further developing its transparency and accountability policy.

Question 2:

Should designated bodies be able to bring 'super-complaints' to the Regulator in specific and clearly evidenced circumstances?

Super-complaints would clearly be a helpful step in understanding the scale of an issue. It has been successfully used in other sectors such as the Competition and Markets Authority (CMA), in policing (HMCIC) and in health care with the proposed outcome of identifying systemic issues which cannot otherwise be dealt with through existing complaints mechanisms.

Whilst super-complaints are helpful there would need to be clear advice and guidance provided to those seeking to make super-complaints and it may be helpful to limit these complaints to those with specific expertise working in these areas, such as charities and law enforcement agencies.

Question 2a: If your answer to question 2 is 'yes', in what circumstances should this happen?

Answered above

Question 3:

What, if any, other measures should the Government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

As we mention in the introduction of our submission, we believe that it is vital that members of the public have somewhere where they can securely and anonymously report illegal child sexual abuse imagery to that is independent of Government, Law Enforcement and the new Regulator. The IWF can, through its discussions with Government, Law Enforcement and the Regulator, raise concerns, or direct issues or complaints to the relevant authorities.

Question 4:

What role should Parliament play in scrutinising the work of the Regulator, including the development of codes of practice?

We believe that it is vital that the Government considers who the intended audience is for this regulatory reform.

In terms of Parliamentary involvement, we believe that an annual report to Parliament on the progress of the Regulator would be an important step in generating public confidence in the work of the Regulator. However, beyond that, we believe that technical knowledge and expertise will be vital to the role of the new Regulator. Parliament is probably therefore not best placed with the technical expertise required to assist in the development of codes of practice and this should be left to the Regulator, industry and other technical experts; however, we do see the potential for a public scrutiny role for Parliament, perhaps through the use of Select Committees, to test Codes of Practice with public sentiment around harms, scrutinise senior appointments made by the Regulator, the work of the Regulator and in scrutinising the budget of the Regulator.

Parliament also clearly has a role in the protection of free speech and ensuring that the rights of individuals to a private life are also balanced against the safety needs of children.

While Parliament will understandably want to be involved in responding to public calls of online harms that need to be addressed, Government needs to think very carefully about the burden that this could place on the Regulator and we would encourage Government, Parliament and the Regulator to focus on a smaller group of harms before expanding the remit further.

Regarding the Code of Practice for CSEA, which as mentioned we will respond to in detail separately, we understand the rationale is, given the illegality of the content, for it to be signed off by the Home Secretary, however we believe there needs to be further thought particularly in relation to the independence and authority of the Regulator. We also believe that the establishment and ongoing review of the Code of Practice could have a profound impact on the work of the IWF. We would therefore like to see a duty placed on either the Home Secretary or the Regulator to consult relevant experts such as ourselves in the development of these codes of practice.

Question 5:

Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

Answered above

Question 6:

In developing a definition for private communications, what criteria should be considered?

An emerging challenge for the new regulatory framework will be to consider how the Regulator will deal with the technological trend for greater levels of encryption and user privacy. DNS over HTTPs for example, if implemented, would have a catastrophic impact on the ability to block illegal child sexual abuse content through ISPs. It will lead to complications with the enforcement of the Government's age verification policy on adult pornographic websites and would also have implications for the blocking of terrorist content and copyright, as well as parental controls currently offered when a customer sets up their broadband connection with any of the major ISPs operating in the UK.

Companies will only be able to deploy technical services to disrupt the distribution of illegal images if they can see what activity is being conducted on their platforms, which is why the Regulator and Government will need to carefully consider the impact of end-to-end encryption, DNS over HTTPs and other privacy issues and ensure that this is not at the expense of child safety requirements.

Question 7:

Which channels or forums that can be considered private should be in scope of the Regulatory framework?

As above.

Question 7a:

What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

As above.

Question 8:

What further steps could be taken to ensure the Regulator will act in a targeted and proportionate manner?

It is essential that the Regulator operates a principles-based approach with proportionate action. Given the lack of detail in this respect in the Online Harms White Paper, the detail of this will need to be worked through over coming months.

Question 9:

What, if any, advice or support could the Regulator provide to businesses, particularly start-ups and SMEs, comply with the regulatory framework?

Start-up companies need a place that they can engage with the Regulator or other companies within the scope of the regulatory framework to access high quality advice and support about building in safety by design. We believe that the IWF could play a role in advising these start-up companies in the deployment of our services and in discussion with some of the larger platforms about the challenges that they face. This must be a forum where start-up companies are encouraged to disclose issues with their platforms or the design of their companies in order to get assistance about designing out issues before they come to market. This must be based on a flexible, principles-based approach that is not overly prescriptive and takes account of the resources available to the companies and that does not set unreasonable expectations of a company which will, by its very nature of being a start-up, have only small amounts of engineering resources or other relevant expertise.

Early engagement with organisations like the IWF could also be of benefit to start-ups. Access to our services can be as little as £1,040 for our smaller Members and they will therefore benefit from those services and relationships that we have with our larger Members, such as accessing Microsoft's PhotoDNA. We would encourage the Government to consider what other technical tools and expertise could be shared across the companies to aide smaller start-ups with other challenges that they may have on their systems.

Clearly, there is a role in identifying what the emerging technical challenges will be. There needs to be a strong understanding of the technical challenges in the internet ecosystem, so the Regulator will be vital to identifying these trends and working with the industry to designing technical solutions to future challenges. The scale of this task should not be underestimated.

Question 10:

Should an online harms Regulator be: (i) a new public body, or (ii) an existing public body?

A key point that we have made throughout our submission is the need for the Regulator to have a strong relationship with the industry it is regulating and be able to understand the technical and legal complexities of the online environment. The Regulator will also need to have a strong working knowledge and understanding of regulatory frameworks and their application to industry. One of the important aspects Government will need to consider is the time it will take to pass legislation that introduces a new Regulator. It would be our view that the Government should be seeking to utilise the current skills and expertise of regulators and experts already operating in this space to drive meaningful change, even in the period whilst the legislation is being passed. We would favour a regulator that already has a relationship with the industry and whose powers could be expanded to cover online harms. We believe that Ofcom is probably best placed to do this, given that they already exist as a public body, are accountable to Parliament and already regulate broadcast media, the BBC and telecommunications amongst other industries. This means that most of the skills and expertise are already in place and may just require expanding further to deal with internet harms. They may however need to expand their skills and expertise further in areas such as human rights and criminal law expertise.

Even though Ofcom knows the area of regulation well there needs to be an acknowledgement that regulating the internet brings different challenges than broadcast media, which it already regulates. The internet has no spectrum limitations, 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. The scope also includes illegal content, which by its nature requires a totally different approach.

Finally, the new Regulator, will need to understand how it works in partnership with other regulators. We have already mentioned elsewhere within this submission that understanding the complex

network of other regulators and their roles and functions within the landscape is going to be crucial. An organisation which already understands the landscape, again would be preferable.

Question 10a:

If your answer to question 10 is (ii), which body or bodies should it be?

Answered above.

Question 11:

A new or existing Regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

The IWF has significant concerns about how the new regulator will be funded and the impact that this may have on existing solutions. The IWF is 90% funded by the internet industry and, outside of the major American players, there is relatively little money to fund both statutory and voluntary initiatives. Our concern is that unless there is security of funding for our work, and other initiatives (such as education and engagement through our partners in the UK Safer Internet Centre) is maintained, there could be a lot of good work which is unintentionally wiped out once industry begins to pay for a regulator.

A lack of funding security would have a significant impact on the ability to remove indecent images of children. It could also increase the workload on an already significantly stretched and under-resourced law enforcement service and could potentially hinder the excellent international collaboration that the IWF has with the European Union, INHOPE network, portal programme as well as our ability to deploy UK assessed services globally and internationally.

We have suggested in our introduction that we would be open to diversifying our funding so that we are not so reliant upon industry funding, but their contribution to us is much more than just funding. Our ability to leverage other in-kind benefits from the industry are also vitally important to the fight against CSAM online. We have benefited from engineers-in-residence, technical tools such as Microsoft's Photo DNA as well as hosting space for our crawler developments. This is generated by companies wanting to do the right thing and by contributing not just financially, but resources to a charitable organisation.

We would welcome further discussion on the IWF's role in a future regulatory framework with the Government and new Regulator to ensure that victims and survivors of child sexual abuse can still have their imagery removed from wherever it is found in the world.

Question 12:

Should the Regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the Regulator?

The Regulator needs to have a range of powers that probably includes most of those suggested within the Government's White Paper. However, experience from other nations shows that even when a Regulator has these powers, they are rarely used. In Australia, the e-safety commissioner has powers to fine companies that are not compliant, but these powers have, to the best of our knowledge never been used, however, this does not mean that the powers in and of themselves do not help in focussing the attention of companies.

At the recent Independent Inquiry into Child Sexual Abuse, the naming and shaming of companies who weren't in compliance was also discussed. Evidence from the IWF, the NCA and Chief Constable Bailey was given specifically on this issue and there was a mixed response as to how effective this had been. All three organisations remarked on the importance of a dialogue between the companies, law enforcement and regulators in order to achieve changes. All three remarked that there were occasions when naming and shaming had been effective and times when it hadn't been quite so

effective. They agreed that this should be seen as a last resort, when it was clear that action wasn't being taken or the companies were not particularly forthcoming or responsive. The Regulator should have the power to issue improvement warning notices to the industry and be responsible for reporting publicly on the effectiveness of companies at dealing with issues of harmful and illegal content on their platforms.

Finally, we believe that further work is required on senior management liability. There are many considerations that must be factored in, when making this decision. Firstly, it depends upon who is in scope. For example, is it right that a Senior Executive of an ISP is held to account for supplying the internet access to an offender who is using a VPN, the dark web or a browser configured with DNS over HTTPs to carry out unlawful or harmful activity when the ISP is not aware of what information is being passed over its networks in these scenarios? The Government needs to provide more detail of how such a regime could work and do more to make its case before we are able to make a firm judgment on whether it is appropriate.

Secondly, there is the issue we have mentioned previously, in which many of the companies that are known to cause issues in the hosting of child sexual abuse material on their services are hosted outside of the jurisdiction of UK law. How could the Government force executives of companies based overseas to act in compliance with UK law? This is further complicated by cloud hosting providers who for example are responsible for a site administered in Malaysia, is hosting in Uzbekistan, and receiving services from a potentially corrupt provider.

Finally, some of the sanctions such as ISP blocking may be rendered useless if DNS over HTTPs is implemented and whilst blocking is a barrier, it is not a fool-proof solution and can be easily circumvented by the use of VPNs and other technical means by the most highly motivated of people. This could have the unintended consequence of pushing people into areas of the internet that you might not want them to be, just to access a popular version of the site that the Regulator has blocked access to. ISP level blocking also needs to be part of a carefully considered legal process due to concerns around freedom of expression and Government would need to clearly set out under what conditions it would happen. Currently our industry Members block on a voluntary basis, under a strict licence, and it works effectively, but if there are sweeping changes with companies being requested to block lots of other harms this needs to be carefully considered. We also strongly believe that there should be separate lists for different harms and the lists should not be conflated which would make sharing internationally even more complicated.

Question 13:

Should the Regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

Answered above.

Question 14:

In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the Regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

We believe that any decision reached by the Regulator should be open to judicial review ultimately. The IWF currently operates in this way and we've so far not had any complaints made or upheld against us. The quality of the Regulator's work will be crucial to ensuring that it is not open to a significant number of appeals. The difficulty for the Regulator will be in ensuring that the appeals process is not overused in areas where content is less well defined in the legal but harmful area where judgments are going to be more controversial and more subjective in nature. There will clearly be a need to manage public expectations.

Question 14a:

If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?

See above.

Question 14b:

If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

No fixed view.

Question 15:

What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

The IWF believes that the numbers of child sexual abuse images and videos being circulated can be reduced on the clear web by internet companies joining the IWF and taking our technical services. The Government needs to assist both industry and the IWF in encouraging the take-up of those services. For companies to access IWF services they need to go through the due diligence process to assure us that they have the security, technical and business infrastructure to receive and deploy said services without the risk of leaking criminal content. Clearly this is a challenge, particularly for new start-ups.

That said, the Government should be encouraging entrepreneurs and those with bright ideas for internet companies to start-up in the UK by providing guidance on who they can talk to for advice and get access to tools and services which have been designed by the larger internet companies that can be used by the smaller providers for maximum public benefit. One of the ways the IWF attempts to bring companies together is by hosting an annual hackathon, which brings together technical experts from industry to assist us with some of the challenges we face, help design solutions and encourage a dialogue between the companies.

Question 16:

What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

The Government has set out its approach to three internet harms; 1. Harms with a clear legal definition 2. Harms with a less clear definition 3. Underage exposure to legal content. We agree with these three definitions of harm and clearly the focus of guidance and safety by design should be focussed on those that cause the highest harms and how easy it is for citizens to access these harms, i.e. the reach of the platform causing the harm.

This does not mean, however, that all advice and guidance on high harm, high reach platforms need to be regulatory. As we have mentioned elsewhere in our submission any guidance produced must consider the roles of all of the relevant stakeholders (ICO, BBFC, IWF etc.) in the field of internet regulation and encourage compliance with all of the relevant regulatory and "non-regulatory" requirements.

The Government could also consider how a Regulator or other bodies such as the UK Council for Internet Safety could produce a number of factsheets based on the experience of tech companies, such as What Works guides which advises and gives practical, evidence-based examples of how to deal with difficult and complex content issues on their platform.

Question 17:

Should the Government be doing more to help people manage their own and their children's online safety and, if so, what?

The IWF has mentioned already the need for campaigns to tackle the issue of child sexual abuse online. We need better sex and relationships education, with a particular focus on educating young girls in the 11-13 age range around the dangers of self-generated sexual content and sharing that content online. Secondly, young men need educating about the law, being encouraged to report child sexual abuse material where they find it, and in preventing their viewing habits from escalating from legal pornography, to harder forms of pornography - which may in itself be illegal – and then eventually crossing into child sexual abuse imagery. We need a national prevent campaign and to put additional funding and resources into those who request and need help when they express concern about their activity and escalation online, before they cross the line of accessing illegal content online.

This submission has focussed on the IWF's remit with regard to tackling online CSEA. However, the IWF is also a partner in the UK Safer Internet Centre (UKSIC) with partners Childnet International and SWGfL. The partners deliver an intensive programme of online safety in schools and with professionals working with children and they also provide a helpline for professionals. Collectively the partnership delivers the annual UK Safer Internet Day (UKSID) each February. This full programme of work is currently funded by the EU with funding agreed until the end of 2020. On leaving the EU, there will be a substantial funding gap for the three organisations IRO £1m per annum without which, crucial online safety delivery could cease.

Question 18:

What, if any, role should the Regulator have in relation to education and awareness activity?

As we stated at the start of our submission, we believe that education and awareness raising activity is vitally important in tackling online harms. We have mentioned that there is a need for a greater focus on sex and relationships education in the 11-13 age range of girls and in the 18-24 age range of young men, for the area of harm we deal with.

It is our view that this should be the responsibility of Government primarily to lead and co-ordinate effective campaigns which will require input from Department for Education, Home Office, DCMS, Cabinet Office and Department for Health. There is clearly a need for Government to join-up some of the work on sex and relationships education with balancing the rights and responsibilities online, in the same way that PSHE does in the physical world.

The UK Safer Internet Centre does a great deal of work in raising awareness in schools and amongst professionals and this work should be further expanded. The Government must ensure that initiatives like Safer Internet Day continue after the UK leaves the European Union and we would recommend that initiatives such as RICU's work in the Home Office is further expanded and built upon.

We believe that the Regulator will have enough to focus on in understanding the regulatory landscape and technical challenges of the internet sector and that should be their focus. There are plenty of charitable organisations that have a good understanding of engagement in schools and with professionals such as those that make-up the UK Safer Internet Centre. Their expertise should be funded by central government and companies to continue to promote online safety.