Written submission to the Special Rapporteur on the sale and sexual exploitation of children.

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: Tess Leyland, Policy and Public Affairs Assistant, tess@iwf.org.uk, 01223 20 30 30.

About the Internet Watch Foundation

The Internet Watch Foundation (henceforth the IWF) is a not-for-profit, partnership organisation that works with the internet industry, law enforcement and government to remove child sexual abuse images and videos from the internet. We are an international hotline for such imagery, and issue Notice and Takedowns for content hosted in the UK, and block images with the cooperation of industry for those hosted outside the UK.

The IWF is charity, and as such 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 Chief's 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. These include image hashing utilising Microsoft's PhotoDNA; a URL blocking list of live webpages, updated twice a day; 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.

We are technical experts, and over the past 23 years we have evolved, improved and expanded to meet the growing threats of the online world – developing cutting edge technology and supporting government, law enforcement and industry to protect children. The IWF committed to working collaboratively and internationally to eliminate child sexual abuse from the internet, sharing our knowledge and expertise to build a better future. Our CEO, Susie Hargreaves OBE, is a board member of the UK Council for Internet Safety (UKCIS), an International Advisory Board member of WePROTECT Global Alliance, and a member of the of the UN ITU's Child Online Protection Steering Group and the Broadband Commission Working Group, and our Deputy CEO and CTO, Fred Langford, is the current President of INHOPE. Furthermore, the IWF establishes reporting portals in the most under-developed countries in the world, with the 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 27 portals including in India, Tanzania, Zambia, and Uganda.

1. ***Context, awareness and attitudes underpinning the sale and sexual exploitation of children.***

What are the current challenges, trends and emerging threats defining the scope and extent of the sale and sexual exploitation of children?

As the UK hotline for indecent images of children, the IWF sees a vast amount of content daily. In 2018 our analysts assessed 229,328 reports and confirmed that 105,047 webpages contained images or videos of child sexual abuse. Each confirmed report could contain hundreds, if not thousands, of indecent images of children. As such, we are uniquely positioned to identify overall trends and emerging threats in the creation of, viewing, and sale of content showing the sexual exploitation and abuse of children.

Self-generated content:

The most striking trend we have noticed over the past few years is the rise in self-generated content of victims. Increasingly, children are being groomed, tricked and coerced into performing sexually over a webcam. Individuals on the other side of the webcam are then recording this, unknown to the children, and creating still images, which together with the recordings, are then shared online. Often, we see this happening in a home – a bedroom or bathroom. In several cases, a parent or carer has knocked at the bedroom door to call their child to dinner, unaware that behind the closed door their child is being groomed.

From 1 January to 30 June 2019 the IWF actioned 22,484 reports of self-generated child sexual abuse material, exactly 1/3 of all confirmed reports. Of this:

- 96% of reports featured girls, 2% boys, and 2% of girls and boys together.
- Of the content featuring girls, 85% were aged 11-13. 1 in 10 reports featured girls aged 7-10.
- Of the content featuring boys, 68% were aged 11-13. 2 in 10 reports featured boys aged 7-10.
- 16% of the material was category A; 25% category B; and 58% category C.[1]

Encryption:

Encryption is a well-documented challenge in limiting the availability and sale of child sexual abuse content. VPNs can bypass blocking measures and peer to peer messaging allows illegal content to pass through undetected. As concerns surrounding user privacy and the use of data grow, industry is responding to these concerns by introducing greater safeguards, and encryption is becoming more prevalent. Whilst user privacy and security are of utmost importance this cannot be prioritised at the expense of victims of child sexual abuse.

Over the past decade, known child sexual abuse content has been blocked at an Internet Service Provider (ISP) level through the DNS requests. However, this status quo is soon to change, with the wider implementation of the Internet Engineering Task Force's (IETF's) DNS over HTTPS (DoH) protocol. This protocol effectively allows end to end encryption on the DNS request, obscuring the user is searching for from their ISP, and giving the browser they are using sole control of this information. There are several other issues with the potential implementation of this encryption, outlined at an ICANN panel earlier this year.

[1] We assess images in relation to UK law according to the levels in the Sentencing Council's Sexual Offences Definitive Guidelines. As of April 2014, there have been three levels: category A: showing sexual activity between adults and children including rape or sexual torture; category B: images involving non-penetrative sexual activity; category C: indecent images of children not falling into category A or B.

As it currently stands, the major browser providers (Mozilla, Google and Apple) do not enforce the same safeguards surrounding blocking material: such as parental controls, anti-terrorist content, and the IWF's URL block list of known child sexual abuse imagery. Through introducing this service and implementing it at default without fully explaining to the user the unintended consequences of this technology, DoH could endanger countless users to exposure to the worst images of child sexual abuse imagery, and the victims of said abuse to continual revictimisation. Current limitations on the extent of child sexual abuse material available will vanish overnight.

DeepFakes:

An area that is increasingly moving into the centre frame is that of the prevalence of 'DeepFakes'. This issue will soon raise serious questions surrounding what constitutes the sale and sexual exploitation of children online. If, for example, an image contains the body of a child, but the head of an adult – or vice versa, or if the image is a compilation of different images of children. This raises questions for us as to whether it is classified as a criminal image of a child.

What progress has been made in shifting the language and the narrative around these issues by the wider community of experts and practitioners?

Child pornography vs child sexual abuse:

The IWF believes that there is no such thing as 'child pornography', a term that is often used internationally at a legislative level, and domestically within the media. The term pornography implies a level of consent that a child cannot give, and refers to a commercialised, legitimate industry.

In contrast, using the term 'child sexual abuse' does not stigmatise or harm the child, nor does it legitimise the act. It identifies it for what it is – sexual abuse. The Luxembourg guidelines, adopted in 2016, outline the terminology considerations of the use of 'child sexual abuse', 'child sexual exploitation', and 'child pornography', encouraging the use of the terms in tandem. However, we believe that these guidelines should go further and eradicate the use of the term 'child pornography'.

The IWF is planning to embark on a media campaign to change the discussion surrounding these issues and challenge the use of the term by UK publications and broadcasters.

Where is the issue?

The IWF data is very clear; child sexual abuse imagery is most often found on image-hosting sites – 82% of content identified by IWF analysts in 2018 was on these webpages. However, there is a popular belief that most content is found on widely used social networks. There is also a widely held misunderstanding that all content is on the Dark Web, whilst most content is on the open web. These misconceptions pose a challenge when we engage with stakeholders, and we find that there is a lack of understanding regarding the complex eco-system of the internet.

Recent polling undertaken on behalf of the IWF found that, when asked what the biggest challenge in controlling illegal content was, 38% of UK MPs cited resistance from the internet industry. As a partnership organisation comprising of 147 Members, including the industry leaders of Google, Amazon, and Facebook, the IWF has worked closely with engaged industry throughout our history. We have found that when it comes to child sexual abuse, there is consensus among our membership. However, what we also see clearly is that there are vast numbers of internet companies who provide the right environments for those who wish to hide, share and trade upon the sexual abuse of children. This segment of the internet industry is not engaged in online safety initiatives, or not engaged enough in the right initiatives.

The focus by parliamentarians on industry, whilst well meaning, is reactive and does not tackle the problem at source. More focus is needed on preventative measures to challenge behaviour, to prevent the content being uploaded, or created, in the first place, and to educate users.

Furthermore, there are misconceptions surrounding where content is hosted. Few realise that, due to current legislation and their strong hosting infrastructure, a significant amount of content is hosted within the Netherlands. In 2018, 47% of all images and videos identified by the IWF to contain the sexual abuse of children were hosted within the Netherlands. So far in 2019, this figure has increased significantly.

What are some of the good practises of raising public awareness and sensitisation of issues of sale and sexual exploitation of children at the local, national regional and global level?

The IWF has been working with the UK Home Office and the Marie Collins Foundation to develop a campaign to help young men (18-24) navigate the internet responsibly. This target audience was identified as campaign research, conducted by Ipsos Mori, showed that young men in this age range were the most likely to encounter sexual images of children online. The three main objectives were:

- Building knowledge of how to report sexual images of under 18s to the IWF;
- Increasing understanding of the law regarding Indecent Images of Children;
- Increasing understanding of the harm caused to victims.

The campaign is currently entering its fourth phase. The third phase of the campaign, which won the Best ISPA PR Campaign award in July, centred around a video of sock character telling his owner where to report child sexual abuse images if he were to stumble across them. This idea was chosen as the humour of the sock character and the innuendo implied by its use was seen to resonate with the target audience, and ensured the campaign was memorable.

The video was promoted on social media platforms and through the gaming platform Twitch. Alongside this, the campaign engaged with the public to raise awareness of this important topic – by sharing a picture of their socks with the hashtag #sosockingsimple. The campaign was supported by charities, law enforcement and influencers, and as of May 2019 over 7 million people had seen the sock film, over 3.2 million had engaged with the campaign, and the IWF campaign page had received over 209,000 visits. Through taking an unconventional method to address the taboo of child sexual abuse, the campaign facilitated conversations that may not have otherwise occurred

2. Risk factors, root causes and demand for the sexual exploitation of children.

What are the root causes and origins of demand for the sale and sexual exploitation of children?

What tools are available to States and non-State actors to effectively address the underlying causes of sale and sexual exploitation of children, beyond training and awareness raising?

Though linked to awareness raising, the IWF feels it is important to stress that several viewers may not realise that they are viewing the sexual abuse of a child. They may have stumbled across the content whilst browsing a legitimate, commercial pornography website. Furthermore, if the child concerned is an adolescent then it can be exceptionally difficult for the viewer to tell what they are viewing, especially if the child is 16 or 17 years old.

What are the remaining challenges and obstacles in overcoming this scourge?

A national prevent campaign:

Though the amount of content hosted in the UK is miniscule, only 0.04% of all content detected by the IWF in 2018, the demand is far higher. The National Crime Agency predict that there are up to 80,000 people in the UK representing some form of sexual threat to children online.[2] While UK-hosted supply is low, demand is high.

The IWF is calling for the UK Government to fund a sustained national prevent strategy to address this demand, delivering a no tolerance message, particularly targeting young men aged 16–25. Tackling this group with the aim of prevention would free up law-enforcement to focus on high-risk offenders and save countless children from revictimisation.

Adequate resources:

The resources for the IWF are finite and, considering the scale of the problem, modest. There is great potential to do far more in this field. The IWF currently has 14 content analysts. As the majority of content is found via our proactive programme, more analysts would mean that more content could be found and removed.

3. *Children's vulnerability to sale and sexual exploitation, including in the context of cross-border challenges, technology and innovation.*

What is the available evidence across children's vulnerability to sexual exploitation, including about existing and emerging drivers of risk?

IWF research:

The IWF regularly publishes data on the abuse that we see through both our annual reports and longer, less frequent, research papers.

In May 2018, the IWF released the study 'Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse'. The study was funded by Microsoft, and analysed data collected during the three-month period of August – October 2017. Key points from the study in relation to vulnerabilities, and drivers of risk, are:

- 96% of children were on their own, typically within a home sitting.
- 98% of the children depicted were assessed to be 13 or younger.
- 96% featured girls.

What groups of children are especially vulnerable to exploitation in general and/or specific forms thereof?

Girls aged 11-13:

As shown in the data outlined under question 1, the IWF has noted a significant increase in recent years in the amount of self-generated content viewed by our analysts. Overwhelming, this trend is affecting young girls, aged 11 – 13.

Whilst this data does show that young girls are more vulnerable to such exploitation, it is worth noting that this may be due to the increased risk.

Grooming on online gaming:

Children can be groomed through a variety of different media – it is not limited to online forums and private chatrooms. Increasingly discussion is moving to the area of online gaming.

The UK's Children's Commissioner recently published an article on online harms, in which it outlines its findings from a series of workshops with school children. Their findings stress the issues with online gaming platforms arise due to the lack of anonymity, opaque reporting systems and the social

[2] UK Home Office, 3 September 2018, https://www.gov.uk/government/news/tackling-child-sexual-exploitation-online

nature of the platforms.[3] Furthermore, in a recent report published by the select committee for the Department of Digital, Culture, Media & Sport, the gaming industry's response to the challenge of protecting users form the risk of grooming was reported as 'mixed'.[4]

4. The over-arching legal normative framework, commitment and institutional capacity.

What progress has been made in global, regional and national legislative frameworks to address children's vulnerability to sale and sexual exploitation, and to address impunity?

Five Countries Security Summit:

In August, the Five Countries Security Summit committed to an immediate upscaling of the response to ensure that children across the globe are protected against online child sexual exploitation and abuse, with the aim that there should be no safe space for offenders to operate in. Building on a statement agreed in 2018, it was agreed that the countries would collaborate with industry to design a set of voluntary principles. These principles will ensure online platforms and services have the systems needed to stop the viewing and sharing of CSAM and the grooming of children.

The summit went on to remind all sectors of the digital industry to consider their impact on the safety of children when developing their systems or services. It stressed that encryption must not be allowed to conceal or facilitate the exploitation of children.

Incoming Online Harms legislation:

The Online Harms White Paper, published in April, outlines the UK Government's plan for a comprehensive legal framework. The paper includes plans for an independent regulator with the power to issue substantive fines, a duty of care on platform providers and a comprehensive media literacy strategy for both parents and children. The consultation for the paper closed on the 1 July, and we are currently awaiting the government response. The IWF submitted a response to the consultation, which can be found here.

With the sands of the UK political system shifting daily, we cannot yet confirm when this legislation will enter the House for debate, as that will be outlined by the Queen's speech currently scheduled for after the rapporteur has requested written submissions by.

The Age Appropriate Design Code:

Earlier this year, the Information Commissioners Office published proposals for its 'age-appropriate design code', to further child protection online. The proposed code centred the best interests of the child, as laid out in the UNCRC, and set out several expectations for industry: including data collection to be minimal by default, location services to be off by default, and explanations for children to be age-appropriate.

Reforming relationship and sex education:

Alongside the Online Harms White Paper, the UK government has recently reformed relationship and sex education in the UK, which will come into effect this academic year. Before this review, the guidance for schools had not been updated for 19 years and was therefore ill-suited to prepare children for the myriad of risks they could face online. The new legislation outlines that the guidance

[3] Reeves, E., 'Children's experiences of online harm and what they want to do about it', 27 August 2019, https://www.childrenscommissioner.gov.uk/2019/08/27/childrens-experiences-of-online-harm-and-what-they-want-to-do-about-it/

[4] Department of Digital, Culture, Media & Sport Committee, 'Immersive and Addictive Technologies, 9 September 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1846/1846.pdf, pp. 20 - 21

must now be revisited by ministers every 3 years to ensure that advise is relevant and children are well prepared for the digital world.

A changing EU framework:

The EU is preparing to review directives that have shaped national legislation throughout the continent. Initiatives such as the Digital Services Act and the AI Regulatory Framework will reopen fundamental questions, such as intermediary liability, that need to be carefully considered. It is critical that existing practises that effectively identify and remove illegal content continue, and current efforts must not be disrupted due to legislative changes.

Since proactive searching was introduced into the IWF's mandate in 2014, the amount of content that is identified and removed by our analysts has significantly risen. In the first year of this new power, IWF analysts identified twice as many child sexual abuse webpages than in the previous year. For the whole of 2013, the IWF identified 13,330 URLs featuring child sexual abuse – in 2014, 27,850 URLs were assessed and actioned for removal. In 2018, 105,047 URLS were actioned for removal, of these 88,775 URLs were proactively found. Of all reports the IWF received from the public in 2018, only 28% accurately reported child sexual abuse material. The IWF would therefore encourage other hotlines to be granted the power to proactively search for this illegal content.

To what extent do these frameworks adequately address or take due account of the challenges posed by transnational internet and financial flows, and their implications for accountability and challenging impunity?

5. ***New and innovative strategies to effectively prevent and protect children from sale and sexual exploitation.***

How adequate is our global multi-stakeholder response to this complex phenomenon?

How adequate are current systems and strategies to protect children effectively?

The IWF is internationally recognised as a model of best practise. We work alongside government, law enforcement, and industry, but remain independent of all and are governed by an independent Board. This unique role enables us to effectively identify and remove content at source, prevent users from stumbling across criminal images, and help safeguard the children pictured in the images and videos. These partnerships also place effective checks and balances on our work - our quality and judgement are held to the highest possible standards.

Under the IWF model of working, the majority of funding comes from internet companies who become 'IWF Members'. They pay a fee which is charged according to their size and sector. This model means that any internet company, of any size, can access the highly sought-after services provided by IWF to keep platforms safe. All Members have access to all services, regardless of the fee they pay. It also means that internet companies themselves are paying the cost of helping to remove the criminal imagery which is circulated online; there is no taxpayer burden.

What are the current global and domestic human rights and protection challenges in the context of evolving global developments?

Are these sufficiently accessible complaints mechanisms available to victims and their representatives?

6. *Data and monitoring.*

How effective are current tools and monitoring systems, including collection, analysis and publication of routing data, in supporting the prevention of and response to the sale and exploitation of children?

Current monitoring systems suffer from a lack of common standards or definitions across borders, making it difficult to measure the extent of the problem and collaborate efforts. The lack of a set definition over what constitutes CSEA, or the categories used in identifying CSAM, makes it difficult to build a detailed picture of the state of child online safety worldwide. Furthermore, it is common for different states and stakeholders to collect data for age groups 0-14 and 15-24, which renders children invisible in the data. When data is gathered that way, it means we do not know what we are seeing, and we do not yet know the full scope of the problem. It's likely that until there is global internet saturation, we will not have reached the full extent of the scale. Alongside the standardisation of legislation and the categorising of images, more work must be done to encourage the responsible reporting of suspected CSAM by the public so that we can build up an idea of the scale of the problem, and appropriate resources can be invested to address it.

There is also an urgent need to reach agreement on sharing data sets including hash lists internationally.

There is, however, growing collaboration in this field. Nationally, in 2018 the IWF was the first non-law enforcement agency to get access to the Child Abuse Image Database, allowing us to hash CSA images in house, and share thousands of hashes through our partners in the internet industry worldwide.

7. *Institutional accountability.*

How far are responsibility and accountability of each and all pertinent actors being enforced and upheld (inc. corporations in the tech, travel and tourism and other sectors)

The UK Government's Online Harms White Paper sets out ambitious plans to further enforce the responsibility and accountability of stakeholders in the online space. These include an independent regulator to focus on the internet industry, introducing codes of practice to deal with illegal activities, and a duty of care on service providers and platforms to protect users from an array of harms. The consultation period ended on 1 July 2019, and the UK Government is planning to respond by the end of the year.

Several European states have recently introduced laws to address online harms. Under the 'German Network Enforcement Act', which came into force 1 January 2018, online platforms face fines of up to €50 million if they do not remove 'obviously illegal' hate speech and other postings within 24 hours of receiving a notification.

Similar legislation is upcoming in France which will require platforms to take down 'obviously' hateful content, and will establish a regulator through extending the remit of Conseil Supérieur de l'Audiovisual, reinforcing the duty of cooperation between major platforms and law enforcement/the judiciary, and effectively fighting the duplication and dissemination of content deemed hateful. Alongside this, on 3 July 2019, French MPs approved a 3% tax on the French revenues of tech giants, including Google, Amazon and Facebook.

Alongside these national initiatives, transnational legislation is also being reviewed. As mentioned earlier, the EU is looking to reform legislation surrounding liability, currently outlined by the E-Commerce directive.

8. The way forward.

How can impact of the mandate be further enhanced in the future?

Where are the major gaps in advocacy and awareness?

As such a significant amount of the content that we see in our hotline is self-generated by children, there is an urgent need for a greater understanding of this content. This is a highly nuanced issue, and we need to protect all children from being caught up in this. The UK is experiencing a national crisis with regards to the creation and distribution of this imagery.

Part of this problem lies in sex and relationship education to children, which must be refreshed regularly. It is crucial to ensure that the right information is getting to children at the right age – not too late. Furthermore, the effect of girls needing self-validation, to be liked and wanted, is something that appears to lead them to being vulnerable online – but this work is still in its infancy. Therefore, alongside sex and relationship education, work must be done to improve the self-perception of children, especially girls.

Finally, a greater focus is needed on the different methods through which individuals can disseminate CSAM. In recent years there has been a great focus on peer to peer encryption services, such as WhatsApp, but this conversation needs to broaden to include other services and feature such as Apple’s AirDrop.