

IWF response to the European Commission's Roadmap- EU Strategy for a more effective fight against child sexual abuse

Name of organisation responding: The Internet Watch Foundation

Address: Discovery House, Chivers Way, Vision Park, Histon, Cambridgeshire, United Kingdom, CB24 9ZR

Contact details of person submitting the response: Michael Tunks, Policy and Public Affairs Manager, mike@iwf.org.uk Tel: 07377449342

1. Scope of the response

- 1.1 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.
- 1.2 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.

2. About the Internet Watch Foundation

- 2.1 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.
- 2.2 The IWF exists for public benefit and performs two unique functions in the UK:
 - A) We provide a secure and anonymous place for the public to report suspected online child sexual abuse images and videos and;
 - B) Use the latest technology to search the internet proactively for child sexual abuse images and videos.
- 2.3 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.
- 2.4 The IWF also plays a vital role in providing the internet industry with several quality-assured technical services to prevent the spread of known child sexual abuse images and videos online and to stop the 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, government and law enforcement.
- 2.5 Our work is funded almost entirely by the internet industry: 90% of our funding comes from our 152 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.
- 2.6 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.

2.7 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.

3. Summary

- 3.1 We believe that the EU has an important role to play in tackling child sexual abuse, particularly online. **We are calling on the European Commission to replace the current Directive on combating the sexual abuse and sexual exploitation of children (the directive) with a regulation directly applicable across EU Member States.** This would resolve many of the challenges with the non-transposition of the current directive and provide opportunity for clear standards and expectations of what is required when it comes to dealing with the issue of child sexual abuse on a Europe wide basis.
- 3.2 Supra national structures are required for dealing with these issues and must be maintained and further strengthened as controlling the spread of child sexual abuse is a global issue and one which can only be solved through effective collaboration. The IWF and UK Safer Internet Centre, look forward to continuing to play our part long after the UK's exit from the Union. We are in active discussions with the UK Government to remain part of the Connecting Europe Facility as part of the future negotiations and with the UK Government about securing our future funding.
- 3.3 The European Commission deserves praise for its commitment to funding the work of hotlines and helplines across the European Union and for promoting initiatives such as Safer Internet Day, the Safer Internet Forum, hosted annually in Brussels, and the development of the Better Internet for Kids Strategy. These provide vital networks for collaboration between Member States and an exchange of information and best practice.
- 3.4 The IWF does, however, recognise the current challenges that face the European Union as set out in the European Commission's roadmap consultation. We have watched with horror as the EU and the Netherlands has become global hotspot for the hosting of this abhorrent imagery and believe that now is the time to address the matter head on.
- 3.5 The European Commission must consider how it forces file sharing sites, image hosting boards and cyberlockers where IWF analysts locate most of this content to comply with new EU legislation. These companies are not household names, that would be easily recognisable to the public, but the problem exists in vast quantities and have traditionally been beyond the reach of both law enforcement and hotlines in the country in which they operate.
- 3.6 Despite these challenges, there are examples of best practice. The partnership approach taken by the IWF with law enforcement, Government and industry has helped reduce the hosting of child sexual abuse in the UK from 18% in 1996 to less than 1% where it has remained since 2003. The European Commission must remember that the active participation of industry is crucial in whatever new framework is decided upon and will be critical in the success or failure of any new approach.
- 3.7 The IWF has made several recommendations within this response about future steps the European Commission could take to improve the response within the EU to this abhorrent crime. We believe that we have much experience upon which the EU could draw upon such as proactively seeking this content from the internet, in the development of technical tools and services, on collaborating with industry and in ensuring exceptional standards in our work. We stand ready to assist the Commission as it further develops its strategy.
- 3.8 We recommend that the Commission draws on the recommendations made by the European Parliament's LIBE Committee in November 2017 and implements the following we have highlighted in this response:
 1. Hotlines must be permitted to proactively search the internet for child sexual abuse
 2. Increased investment in technology to detect child sexual abuse imagery
 3. Mandatory reporting from the industry and development of preventive measures
 4. An explicit legal role for hotlines and appropriate funding
 5. Hotlines should be able to be designated as Trusted Flaggers
 6. Step up on education and awareness-raising of the dangers of the internet to children

7. Joined up approach with other legislative proposals, especially the Digital Services Act
 8. Be aware of potential implications of other legislation on current effective mechanisms
 9. More transparency and accountability from the internet industry
- 3.9 We firmly believe the European Commission has a real opportunity to have a huge impact on this problem through the range of measures and consultations recently announced on the Digital Services Act, the roadmap on the EU strategy for a more effective fight against child sexual abuse and the roadmap on the EU Strategy for the Rights of the Child and respectfully request that the European Commission ensures effective co-ordination across the aims of the three new initiatives.
- ## 4. The problem
- 4.1 **The IWF understands and recognises the challenges as set out in the European Commission's Roadmap consultation document and indeed the roadmap references the IWF figures, which confirms that Europe is in the unfortunate position of hosting the most child sexual abuse material anywhere in the world.**
- 4.2 The amount of child sexual abuse images and videos hosted in Europe has been continuing to rise for the past five years and has now reached crisis point. The IWF's annual report last found North America as the global hotspot for child sexual abuse images in 2015, when 57% of the world's global child sexual abuse images and videos were hosted there.
- 4.3 Whilst North America has seen a reduction to 9% in 2019, Europe has seen an explosion. Last year 89% of the webpages the IWF removed were hosted in Europe. Just under 94,000 webpages of the 132,700 we actioned for removal were hosted in the Netherlands.
- 4.4 As Europe's problem with hosting has continued to grow, many of the issues can be attributed to the situation in the Netherlands. There was a first significant shift in the hosting of this content in the Netherlands in 2016, when our annual report highlighted an 18% increase on the previous year. In 2019, we recorded a further 24% increase from 2018, and the Netherlands is now responsible for 71% of all reports we actioned.
- 4.5 **It is also important to point out that the IWF does not typically find this content on social media platforms.** We have consistently found that less than 1% of the reports that we action for removal are found on social media. The problem tends to be more with image hosting boards / sites, cyberlockers and banner sites.
- 4.6 In 2019, image hosting boards and sites were responsible 84% of the content the IWF acted against. These are internet forums which operate mainly through the posting of images and are used for discussion on a variety of topics and issues. They are very similar to bulletin board systems but with a focus on images. Image hosting sites let users upload images which are available through a unique URL and this URL can then be used to make online links, or be embedded in other websites, forums and social networking sites.
- 4.7 Cyberlockers, file hosting services, cloud storage services or online file sharing providers, were responsible for 6% of the reports the IWF actioned for removal in 2019.
- 4.8 There are three significant challenges the IWF believes Europe needs to overcome in order to resolve the issue of why so many Child Sexual Abuse Material (CSAM) images and videos are hosted there.
- 4.9 Firstly, there is the issue that **some hosting companies are either slow to act or ignore requests for removal. Some hosts exploit legal loopholes which enable them not to remove content without a court order and some also have little or no controls or processes in place to limit the amount of CSAM being posted on their site (s)**

4.10 Secondly, **many of these hosting companies know that specific “customers” will be responsible for huge volumes of notices year in year out, yet they persist in maintaining that financial relationship and collecting revenues.** There needs to be a dramatic change in approach from these companies and they must be more proactive in ensuring that they are not complicit in the hosting of this content and act much more responsibly.

4.11 **Thirdly, the rate and speed of technological change must be addressed. Legislation will rarely be able to keep a pace with the rate of technical change.**

4.12 A good example of this, is that a domain hosting child sexual abuse can migrate in a matter of hours. It can move from one hosting provider to another, from one country to another and that makes dealing with this illegal content incredibly complex. Some hosting providers will also not necessarily know who they have sold hosting space to as intermediaries and a range of other obtrusive techniques can be used to prevent the person responsible from being easily identifiable. This also means that the uploader of illegal content could be in the Philippines for example, using a hosting company based in the US who is hosting the content on a server in the Netherlands and is free to access from wherever you are in the world. Once the content is removed, it can then be reuploaded somewhere else, unless that hosting provider is deploying some form of control such as the IWF hash list for example.

4.13 This is, therefore, an extremely complex and difficult sphere to legislate in. We have seen just how challenging this has been with the recent e-privacy file in the previous legislative cycle.

4.14 **Every day we discover new and emerging threats to children posed through the internet. There are numerous examples of where many of new approaches and technical standards have failed to take account of the interests of children in the design stage of new products.**

4.15 Take for example the Internet Engineering Task Force’s (IETF’s) recently adopted DNS over HTTPS¹ standard. Whilst we understand the reasons why the new standard was adopted and the importance of privacy online, not enough attention was paid to the implications for children and the IWF’s URL blocking list, which could be completely circumvented without any warning to internet users if deployed universally, as well as any parental controls which may be being deployed by an ISP.

4.16 New forms of encryption, such as those Facebook is proposing for its messenger app also create challenges in the detection of child sexual abuse content online. We are extremely concerned by this development, and so far, the steps taken by Facebook do not reassure us that these measures will improve child safety online, in fact quite the opposite. The IWF is calling for their new encryption to have equivalency with the current system². It is vitally important to the protection of children that offending content can still be identified by law enforcement.

4.17 **Address the significant rise in self-generated content-** A third of the reports (38,424) the IWF hotline actioned in the past year contained this content and three in four (29,312) contained images of girls in the 11-13 age range. We are extremely concerned that the current Covid-19 pandemic

¹ The IWF has produced a range of blogs and a short video which explain this issue in detail:
<https://www.iwf.org.uk/news/exposing-child-victims-catastrophic-impact-of-dns-over-https>
<https://iwf.org.uk/news/dns-over-https-'what-does-mean-'>
<https://iwf.org.uk/news/dns-over-https-why-we're-saying-doh-could-be-catastrophic>
<https://iwf.org.uk/news/dns-over-https-it-should-not-have-come>
<https://iwf.org.uk/news/new-form-of-encryption-could-threaten-ability-to-block-child-sexual-abuse-material-say-mps-and>

could also have further exacerbated this problem as children are separated from their friends during the current lockdown and spending increasing amounts of time online.

5. What more could be done?

- 5.1 **The IWF believes that now is the time for the introduction of a new CSAM regulation to replace the current directive.** There are many benefits to doing so. Firstly, Member States will have to comply with a new regulation, this would resolve many of the transposition issues with the current directive and introduce greater pace from member states to meet their obligations. Secondly, we believe that primary legislation is needed by both the EU and Dutch Government to resolve the constitutional issues that enable image hosting boards and cyberlockers to host this content in the Netherlands. Finally, it gives the opportunity to set Europe wide standards and definitions of child sexual abuse, which would make it easier for companies to take action upon.
- 5.2 **The European Parliament's LIBE Committee produced an excellent report in November 2017, which made a number of recommendations that the IWF asks the European Commission to consider carefully to improve the response to child sexual abuse.**
- 5.3 **Hotlines Proactively seeking CSAM content-** recommendation 25 within that report the importance of hotlines being permitted to proactively search the internet for child sexual abuse. This has been a vitally important tool in the armoury of the IWF. In the first full year of the IWF proactively seeking content, there was a 147% increase in the amount of child sexual abuse that was able to be removed from the internet.
- 5.4 This is particularly important as the accuracy of public reports is increasingly inaccurate. In May 2019, the IWF processed 8,500 reports. In May 2020, during the Covid-19 pandemic the hotline processed 12,500 reports. Accuracy of public reporting in 2019 was 11%, but this has further dropped and at present is only 9% accurate. So, whilst public reporting can offer vital intelligence, the more reports we receive, the less accurate those reports tend to be.
- 5.5 **Investment in technology to detect child sexual abuse imagery is also vitally important.** The IWF would encourage the European Commission to invest in projects and infrastructure which helps to fight child sexual abuse globally. It is important that the European Commission encourages and facilitates technology companies working with NGO's and hotlines to invest in solutions that are effective and can be deployed worldwide. These points are covered under recommendations 10, 32 and 33 of the LIBE Committee's recommendations.
- 5.6 The IWF has now invested further in web crawling technology and is currently developing several image classifiers which will further enhance the speed at which this imagery can be identified and processed.
- 5.7 It is important to remember, however, that whilst investment in technology is helpful in dealing with the volumes of content available on the internet, there is still an important need for human assessment of imagery. There is currently no technology available that can accurately age a child, and this becomes particularly problematic the older the child is.
- 5.8 **Mandatory reporting from the industry.** Recommendation 24 of the LIBE committee report recommends that Member States in collaboration with hotlines make it a mandatory requirement for ISPs to report and remove child sexual abuse detected on their infrastructure to law enforcement and national hotlines. It also calls on the ISP to preserve the evidence in line with legal processes.
- 5.9 **An explicit legal role for hotlines and for them to be funded appropriately.** Should the European Commission consider the introduction of mandatory reporting; it must consider carefully the resourcing requirements that would be required to service such a function. The recent Dutch hotline report³ for example highlights "that for a number of reasons, they are still experiencing a backlog in 2019." They attributed this due to the number of reports being still high despite having an expanded team and due to the fact that most of their work was unable to be automated. The hotline also claimed that duplicated reports were also an issue.

³ <https://inhope.org/EN/articles/eokm-published-its-2019-annual-report> Page 9

5.10 The issues with non-compliance with court orders and the lack of resources have created a perfect storm of events, which is fundamentally two of the reasons why the Netherlands and the EU is now the hotspot for the hosting of this content.

5.11 **Trusted Flaggers.** The European Commission has previously consulted this issue in previous consultations. This is certainly something that the IWF would welcome. If hotlines could be given legal standing that goes beyond the scope of the current directive and in a more regulatory framework, this would certainly have some impact on the problem. However, we also recognise the importance of hotlines operations complying with the relevant legal processes when imposing limiting fundamental rights on the internet as recommendation 29 from the LIBE report states.

5.12 **Raise education and awareness of the dangers of the internet to children.** Recommendations 12, 17 and 30 all reference their importance and the access to public funds in order to provide these awareness raising initiatives.

5.13 The IWF believes that this is essential. Whilst we recognise that we have a role removing this content once it has been identified and have a number of services that can prevent its circulation, we have always believed that prevention is better than cure and a more effective way to reduce the heavy costs child sexual abuse has on victims and society.

5.14 **Joined up approach with other legislative proposals.** The IWF applauds the new European Commission for the proactive approach it has taken to addressing the issue of child sexual abuse within the European Union. It is long overdue. The European Commission has recently announced a flurry of activity including this consultation, plans for a new Digital Services Act and a further roadmap on Child Rights. The European Parliament Intergroup on Children's Rights has also recently hosted an event where Commissioner Johansson called for a new EU centre for preventing and combating Child Sexual Abuse.

5.15 All this activity is most welcome, but the IWF would request that whilst there is political impetus on this issue that all the relevant activity from the European Commission is co-ordinated and joined up in its approach. The Digital Services Act represents an excellent opportunity to ensure that we get the right approach to regulating this activity within the EU, but this must be complemented by effective measures to fight child sexual abuse and include vital public awareness messaging campaigns and the sharing of best practice. Not only must this legislation ensure it complements the other measures within the EU, it must also be much more effective in ensuring action at Member State level. The fact that the current directive has not yet been fully implemented simply must be addressed this time around.

5.16 The IWF would also ask the European Commission to consider the international context of decisions it reaches. For example if it considers the introduction of mandatory reporting, it should also ensure that this complements the processes already established by the National Centre for Missing and Exploited Children in the United States and not duplicate efforts by starting off to investigative processes, when one will suffice.

5.17 **Unintended consequences need to be carefully considered.** The European Commission should also be careful to guard against any potential unintended consequences that impact on current effective mechanisms for dealing with child sexual abuse online. One previous example is when the Commission recently updated the General Data Protection Regulation. This led to some difficulties for hotlines as it led to Hash's being qualified as personal data in many jurisdictions. The IWF spent a six-month period resolving this issue with the Information Commissioner in the UK and it significantly slowed down the IWF progress in agreeing a hash sharing arrangement with the US National Centre for Missing and Exploited Children (NCMEC).

5.18 Another issue which has yet to be resolved is the implications this legislation has caused for the WHOIS database which is administered by the Internet Corporation for Assigned Names (ICANN). The database was a previously open source register of domain names which provided helpful information on who is hosting certain domains and webpages and contact information for those responsible for the hosting of certain content. This was a very useful tool for hotlines in seeking the swift removal of content, but unfortunately, it is no longer available publicly due to changes in the GDPR. ICANN is currently working to resolve the issue, but progress remains glacially slow.

- 5.19 **Need for greater transparency and accountability.** The IWF supports greater levels of transparency and accountability from the internet industry that helps to further identify the scale of the problem of child sexual abuse online. Recent surveys from the telecoms and proposed online harms regulator in the UK, Ofcom, has concluded that there is clear public appetite for a greater level of demand for rigour and accountability to the public on how companies are dealing with illegal and harmful content on their platforms. Just last week Ofcom's Online Nation report⁴, published data that found 81% of children (aged 12-15) surveyed had a potentially harmful experience online in the last 12 months. For adults it was 61%.
- 5.20 The IWF has also recently discovered that in the first month of the Covid-19 pandemic, 8.8 million attempts were made to access child sexual abuse material in the UK. Whilst this cannot be directly attributed to human attempts, it does give some idea as to the potential scale of the problem. This data, however, was only provided by three of our members and we have no comparable data from before to compare this with. This could certainly be a helpful measure for companies to report on in the future.
- 5.21 The principle of transparency and accountability is a well-established regulatory principle that is applicable to other regimes at present including the telecoms sector. This approach would be entirely consistent if it was to be applied to any future regime.
- 5.22 **We would advise the European Commission not to be prescriptive in its use of technological solutions within primary legislation.** The pace of technological change means, that any technical solutions enshrined in legislation today can be quickly outpaced by the technology of tomorrow and could lead to frequent redrafts of that law. Legislation must remain flexible enough to take account of future technical challenges online. We therefore advise the European Commission to look at secondary legislation such as codes of practice and the potential for greater regulation, transparency and accountability mechanisms as effective ways to tackle the problems currently faced.
- 5.23 **The European Commission must also draw upon skills and expertise of those already working within this space.** Legislators cannot get this right in isolation and they will need to draw on the skills, knowledge and expertise of engineers and those already working within this space (including companies, NGOs and law enforcement). A careful balance must be drawn between the need to drive growth and innovation and safety online. Both factors are of increased importance given the recent Covid-19 pandemic and the impact that necessary, nationally imposed lockdowns have had on jobs and the protection of children online.
- 5.24 **The new strategy to tackle child sexual abuse should also seek to raise the bar, by further addressing challenges with grooming and live streaming.** These are extremely difficult issues to control online. Rapid migration of victims, often in a matter of minutes, through various platforms often to encrypted services makes grooming very difficult for companies to accurately detect and identify. With both issues, there is currently no technical silver bullet solutions that are going to resolve these challenges, but it should form a part of the European Commission's new strategy in a bid to raise awareness and the need for solutions. Our recent research in partnership with Microsoft, highlights the complexity live streaming sites pose and how captures from live streams end up on dedicated child sexual abuse websites.
- 5.25 **Dramatic change required from hosting companies.** Finally, the Digital Services Act means that there is an opportunity to dramatically change the expectations of companies. We must tackle the issues associated with image hosting boards and cyberlockers. They should be compelled to join the IWF and deploy our technology proactively to prevent the upload of known imagery and do all that they can to stop this content from appearing in the first place. Prevention is better than cure.

6. Current effective measures to fight CSAM

⁴ https://www.ofcom.org.uk/_data/assets/pdf_file/0027/196407/online-nation-2020-report.pdf page 31

The IWF model

6.1 Despite the significant challenges that remain in tackling child sexual abuse online and wherever possible preventing it from occurring in the first place, there are some good examples of best practice, which we would respectfully encourage the European Commission to consider further building upon when shaping the new strategy. Many of the challenges set out above, technical solutions and awareness raising campaigns and initiatives run by the IWF have led the world in our approach to tackling this issue.

6.2 In 1996, the year the IWF was founded, 18% of the world's known Child Sexual Abuse was hosted in the UK. **Thanks to the partnership approach the IWF has taken with industry, government and law enforcement, this is now less than 1% and has been ever since 2003 and demonstrates what can be achieved when we come together to tackle CSAM online.** Any reforms proposed by the European Commission, must recognise that effective co-operation from the industry is vital.

6.3 What started out in 1996, as just five companies agreeing to found and join the IWF has now turned into 152 and the IWF has now secured a significant global presence and those within membership commit to doing all they can to prevent CSAM from appearing on their platforms.

6.4 Our success has been based upon our independence from government and law enforcement, which enables us to successfully navigate the 4th amendment issues with the American companies and helps to encourage public reports without the fear of reprisal from law enforcement. The IWF now operates 40 reporting portals globally, including our first portal in Europe, recently established in the Ukraine.

6.5 The IWF brings a range of public benefits in the fight against child sexual abuse online in the European Union:

- We provide the public with a place to anonymously report suspected CSAM not only in the UK, but 40 different countries around the world.
- We have assisted in the identification and removal millions of child sexual abuse images and videos from European hosting space.
- **We are the only European hotline permitted by its Government to proactively seek this content online and not just rely on public reports.**
- A quarter of the data submitted to the INHOPE's ICCAM database came from the IWF in 2018.
- 42% of removals in the UK are actioned within two hours of the host being notified and our hotline chase ups rapidly speed up the removal of this imagery within Europe.
- We have established a hash sharing agreement with the National Centre for Missing and Exploited Children (NCMEC) in the US that now contains 3.5 million hashes.
- We are run effective awareness raising campaigns and are now seeking to address the issue of self-generated content in a new campaign with Home Office and industry.
- We create world leading solutions such as web crawling technology, image classifiers, chatbots and develop new reporting solutions.
- The IWF is a global leader. A 2018 report from INHOPE claimed: "*The IWF maintains exceptional standards in all areas and it practices can be recommended to new or existing hotlines wishing to develop or expand its services.*"

6.6 The way the IWF was established means that our quality and judgement 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 child sexual abuse.

6.7 The IWF model requires that companies act on Notice and Takedown issued by the IWF for content hosted in the UK. Internationally, we work with other relevant hotlines or law enforcement agencies

to action removal. The quality of our judgment is essential to this process, particularly, to law enforcement and the companies and the judiciary.

6.8 The reason the IWF has been so effective to date is because we operate within a clearly defined legislative framework where our harm is clearly illegal.

6.9 Secondly, following the removal of such content, it is vitally important, in order to ensure compliance with human rights law that certain procedures are followed including the right to appeal. The IWF continues to be audited on a bi-annual basis by a senior, former High Court Judge and the appeals process also should include at its final stage, a determination by the Chief Inspector.

6.10 These processes are vitally important to ensuring that the IWF can act before the Courts process and adds further legitimacy and credibility to the work that we do. It further demonstrates that a hotline's ability to act prior to the Court process is entirely legitimate, right and proper.

6.11 The IWF are prepared to explore the feasibility of extending our current remit to consider the possibility of including grooming and live streaming, in consultation with our Members. We can use the 24 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 governments for the benefit of children. We also made this offer to the UK Government in our response to their consultation on Online Harms.

European Commission Funding-

6.12 The European Commission also deserves credit for leading the way in funding the work of the Internet Watch Foundation, the UK Safer Internet Centres and the work of other hotlines and helplines through the INHOPE and INSAFE networks.

6.13 This funding is vitally important and currently equates to 50% of the UK Safer Internet Centre's total funding. It currently equates to approximately 30% of Childnet's annual turnover, 14% of the Internet Watch Foundation's turnover and 6% of SWGfL.

6.14 Over the last ten years, Safer Internet Day, in the UK has been completely transformed. In 2011, the first year the UK Safer Internet Centre ran Safer Internet Day just 70 organisations signed up to support the day and its important safety messages to children and young people.

6.15 In 2020, over 1,700 organisations supported the day and reached three million UK children, 50% of children aged 8-17 in the UK. The campaign day also reached 26% of their parents and 19% of children went onto have a conversation with someone about something that had been worrying them online.

6.16 The impact of this funding has been crucial in driving progress in the fight against child sexual abuse online. The UK Safer Internet Centre has since 2012, trained 21,000 professionals who work with around 6 million children. 98% of these professionals recognised that their training better equipped them to protect children online. The Online Safety outreach programme run by SWGfL as part of the UK Safer Internet Centre, is the largest online safety outreach programme in the country.

6.17 The funding has also enabled Childnet International to directly engage with 6,700 school children, 1,400 parents and 3,000 teachers in 2019. Childnet's Digital Leader's programme has recruited 1,00 schools and trained 4,000 children to educate their peers in the responsible and safe use of technology.

6.18 The UK Safer Internet Centre has also gone above and beyond in its approach to tackling online harms efficiently and effectively outside of the funding it receives from the European Commission. SWGfL also operates a platform for the reporting of harmful content online. This reporting function

assists users with reviewing decisions made by social media platforms and assists users in the accurate reporting of concerns to social media companies.

6.19 The same charity also is responsible for the operation of the Revenge Porn helpline, which has also seen a significant spike in reports throughout the Covid-19 pandemic. These initiatives are vitally important to protecting and educating internet users about the safe and responsible use of technology, but also provide anonymous places to report in the event of things going wrong.

6.20 It is the wish of both the Internet Watch Foundation and the UK Safer Internet Centre to continue playing its part in these important issues long after the UK has left the European Union. Many of the legislative changes being proposed by the European Commission through its Digital Services Act, this consultation and the further consultation on Child's Rights will continue to have an impact on the way companies act in the removal of content internationally.

Ability to act at Supranational level-

6.21 The UK Safer Internet Centre are currently discussing with the UK Government the possibility of the UK remaining within the Connecting Europe Facility funding framework as part of the future negotiations. The UK Safer Internet Centre recognises the importance of acting at a supra-national level to address these issues and believes that it is of utmost importance that this is retained.

6.22 The European Union has an increasingly important role to play in getting the approach to these technically challenging issues right. If the Commission achieves this, the power for a fundamental change in the way child sexual abuse is dealt with is entirely possible. It is not only possible; it is vitally important given the significant challenges faced.

6.23 The IWF and UK Safer Internet Centre stand ready to assist the European Commission in any way we can both now and in the future.

7. Conclusion-

The IWF firmly believes that European Commission has a great opportunity to create a world-class paradigm shift in the fight against the spread of child sexual abuse online. It is vitally important that the Commission builds on current effective practice in tackling the issue and the IWF is keen to contribute its 24 years of experience and convening power with industry to further assist the European Commission in developing its response.

We firmly believe that a good first step in this process would be to announce a revision of the current directive and would support calls for a regulation to resolve the current challenges with transposition in Member States.