IWF response to the European Commission's roadmap- Delivering for children: an EU strategy on the rights of the child.

Name of the organisation responding: The Internet Watch Foundation (IWF)

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

Contact details of person submitting the response: Tess Leyland, Policy and Public Affairs Assistant, tess@iwf.org.uk, +44 (0) 7496 580 902

1. Introduction

1.1. The Internet Watch Foundation (IWF) welcomes the European Commission's commitment to furthering the rights of the child and believes that now is an appropriate time to revisit and update the EU's 2011 agenda. The IWF is committed to embedding a "child rights-based approach" and is supportive of the aims of the UN Convention on the Rights of the Child (UNCRC) which are as applicable today as they were 30 years ago when they were first established.

1.2. The implementation of the Sustainable Development Goals, in particular Goal 16, which includes a target to end abuse, exploitation, trafficking and all forms of violence against children is equally as important. These aims drive the very mission of the IWF each day.

1.3. In recent years, the EU has undertaken several critically important initiatives that have furthered the rights of the child both within Europe and internationally. The Better Internet for Kids Strategy placed the safety of children at the very heart of digital policy, and the work of the Connecting Europe Facility in funding and supporting the international reach of both INSAFE and INHOPE networks have allowed the exchange of best practice, fostered innovation, collaboration and cooperation at a supra-national level. Furthermore, the recently announced EU strategy for a more effective fight against child sexual abuse laid out an ambitious and far reaching programme of change that seeks to redefine the fight to protect children from sexual abuse and address Europe's crisis as the global hotspot for the hosting of indecent images and videos of children.

1.4. This new child rights strategy must also complement the new EU strategy for a more effective fight against child sexual abuse. Both strategies will be vitally important components in tackling the challenges children in the EU face today and if implemented effectively could be a real opportunity to deliver on children's rights.

1.5. It is important, however, not to underestimate the challenge of applying child rights in a digital context and this will be the focus of our submission to this roadmap consultation. You can of course, read more of the IWF's views on the more effective fight in response to child sexual abuse in our roadmap response to that consultation.[1]

2. About the Internet Watch Foundation (IWF)

2.1. The 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.

---

[1] https://www.iwf.org.uk/sites/default/files/inline-files/IWF%20response%20to%20EC%20roadmap%20on%20a%20new%20strategy%20to%20fight%20CSAM.pdf

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. Recommendations

3.1. **The European Commission's new strategy must uphold the delicate balance between protecting children's rights to privacy, freedom of expression and the right to a secure childhood, free from sexual abuse and exploitation, a particular challenge in the online environment.**

3.2. We recommend the European Commission consider the adoption and support of the recommendations of the Committee of Ministers to Member States of the Council of Europe on the [Guidelines to respect, protect and fulfil the rights of the child in the digital environment](#), adopted on 4 July 2018, which outlined a range of measures Council of Europe Member States could employ to further their commitment to the rights of the child. **Specifically, requiring industry to take all reasonable, proportionate, and effective measures to address potential child sexual abuse on their platforms. In light of Europe being the global hotspot for the hosting of this abhorrent imagery, particular attention should be paid to the Netherlands and image hosting boards and cyberlockers who are located there.**

3.3. Children must be respected, and their views consulted and considered in all matters relating to them. **We urge the European Commission to continue to engage with children and further include their thoughts, feedback and concerns into the 'fundamental rights check-list' outlined in the 2011 agenda on the rights of the child.**

3.4. **Products and services made available to children must be age-appropriate for children of different ages and maturity, including accessible terms and conditions, and clear reporting mechanisms. Legislators must lead by example through ensuring all legislation takes full consideration of the best interests of the child.**

3.5. **The technology industry should also ensure children's rights are heard and considered in the development of new services or technical standards on that take full accounts of <u>ALL</u> of a child's individual rights, balancing their right to privacy, freedom of expression, and protection from abuse and exploitation.**

3.6. **Digital literacy and resilience are key to furthering the rights of children, and we urge the European Commission to invest in digital literacy programmes, educational resources, and awareness raising initiatives for both children and their carers.**

3.7. **That the European Commission considers alongside this response, our response to the EU Roadmap on the new strategy for a more effective fight against child sexual exploitation and abuse and the recommendations contained within that submission.[2]**

4. The challenge

<u>Balancing privacy, freedom of expression with the safety and security of children online:</u>

4.1. Balancing the needs of a child's right to privacy (UNCRC, Art. 16), play (UNCRC, Art. 31) and to freely express themselves (UNCRC, Art.13) with the absolute necessity to ensure their safety, wellbeing and right to a childhood free from abuse and exploitation (UNCRC. Art. 19, 34 & 36 and Sustainable Development Goal 16.2), and security with their right to learn (UNCRC, Art. 28) is extremely challenging.

4.2. The online environment is extremely complex and often there is an inbuilt juxtaposition between these aims and objectives. It is an issue which is beginning to dominate much public policy debate about the future of internet governance and the roles and expectations on companies and Government in this space.

4.3. The internet is undoubtedly a force for good. It brings clear benefits to children in a multitude of ways – it allows them to learn, play, socialise and engage in civic and political conversation. There is no doubt that this generation of children are better connected, better informed and more entertained than many generations that have been before, and clearly access to the internet is fundamentally a good thing for child rights.

4.4. We have seen just how important children's connection to the online environment has been during the Covid-19 pandemic. Many schools have resorted to online learning and teaching in the new socially distanced world we find ourselves in at present. Clearly, those without internet access are at a significant disadvantage when it comes to learning at present, and often they are the most vulnerable children in society.

<u>The impact of Covid-19 on children:</u>

4.5. The current Covid-19 pandemic has also highlighted not only the good, but the challenges and dangers to children online.

4.6. In a press release on 4 April 2020, the UK's National Crime Agency announced that it suspected a minimum of 300,000 individuals in the UK posed a sexual threat to children, either online or

---

[2] https://www.iwf.org.uk/sites/default/files/inline-files/IWF%20response%20to%20EC%20roadmap%20on%20a%20new%20strategy%20to%20fight%20CSAM.pdf

from contact abuse.[3] Both Europol[4] and Interpol have also warned of the increased risk to children during the current pandemic.

4.7. Lockdown measures which have been a necessity for public health reasons have resulted in us all spending more time online. This includes children and those who seek to exploit them.

4.8. The IWF has found that in just one month alone at the start of the UK lockdown, there were 8.8 million attempts[5] to access webpages containing known child sexual abuse material, across just three Internet Service Providers or Mobile Operators serving the UK market. We cannot equate this to individuals or human attempts, but it does highlight a potentially alarming number of attempts and further serves to highlight the significant risks to the safety and welfare of children. Unfortunately, the IWF does not have comparable data with other times of the year or prior to the pandemic to compare this to.

4.9. In addition, our Hotline recorded a 50% increase[6] in reports from the public from 23 March to 9 July 2020 when compared to 2019. Of these reports, 5,367 reported URLs were confirmed to contain images or videos of children suffering sexual abuse, a 65% increase on the number actioned last year, as more users have stumbled across this material and more children have been revictimised.

4.10. We are also waiting to see what the full costs of the pandemic may be to children once school teachers and social workers can once again can intervene in the lives of children who have been locked down and not in schools or public sector settings for the last 6 months. The National Crime Agency suggests that whilst reporting from children themselves has remained stable, there has been a sharp decline in referrals from teachers and social workers during the pandemic.

4.11. The longer the pandemic goes on and the longer children are not at school, the greater the risk that abuse is never reported or unearthed by the authorities. We know that child sexual abuse tends to be an interfamilial crime and that the abuser is often known and trusted by the child that they are abusing. This is something the European Commission should be alert to in both the new strategy to protect children from abuse and in further delivering their rights as children to a right to a childhood free from abuse and exploitation.

Protection of children from sexual abuse and exploitation online:

4.12. In recent years, the amount of known child sexual abuse imagery hosted within Europe has steadily increased. 2019 marked a crisis point, as 89% of the 132,676 webpages identified by the IWF to contain the sexual abuse of children were hosted within Europe, with the Netherlands responsible for 71% alone.

4.13. It is also important to recognise that the problem of the hosting of images and videos is not on social media platforms, who generally do quite a good job of keeping their platforms free from abuse, and when it is discovered they report to the National Centre for Missing and Exploited Children (NCMEC) in line with US law. As a result, the IWF detects that less than 1% of the world's known child sexual abuse content is located on social media.[7]

---

[3] https://nationalcrimeagency.gov.uk/news/onlinesafetyathome
[4] https://www.europol.europa.eu/newsroom/news/exploiting-isolation-sexual-predators-increasingly-targeting-children-during-covid-pandemic
[5] https://www.iwf.org.uk/news/millions-of-attempts-to-access-child-sexual-abuse-online-during-lockdown
[6] https://www.iwf.org.uk/news/'definite-jump'-as-hotline-sees-50-increase-public-reports-of-online-child-sexual-abuse-during
[7] https://www.iwf.org.uk/report/iwf-2019-annual-report-zero-tolerance Page 51

4.14. In 2019, image hosting boards (84%) and cyberlockers (6%)[8] were the most likely to be found hosting this content. In the interests of protecting the rights of children to a childhood free from child sexual abuse, this is something the EU must be taking firm, effective action on. Many of the "bad actors" are not household names and significant pressure must be brought to bear on them to ensure that they comply with new obligations proposed in the Digital Services Act, Child Rights Strategy and a new strategy to for a more effective fight against child sexual abuse.

4.15. The EU must also address the reasons why so many Member States are not confirming with the current directive to counter child sexual exploitation. This is something we called for in our response to a new strategy to fight child sexual abuse.

Challenges with the development of new technical standards and legislation related to the online space:

4.16. The pace of technological change is rapid and often outpaces the legislative frameworks and policy initiatives of Governments globally and international bodies such as the UN and supra-national structures like the EU. Each year, new technical tools and standards are established that sometimes inadvertently impact the safety of children online.

End-to-end encryption:

4.17. End-to-end encryption continues to present a major challenge in this space. Current plans by Facebook to implement end-to-end encryption on its messenger service could undermine current preventative tools in place to address this child sexual abuse. Facebook claims to be prioritising the privacy of its users, which of course is a fundamental Human Right as confirmed by the UN Declaration on Human Rights, but we are very concerned about what this may mean for the protection of children as encryption will make it much harder to identify infringing content.

4.18. In 2018, Facebook made 16.8 million reports to the NCMEC – more than 90% of the 18.4 million total reports received that year. These reports included both suspected child sexual abuse imagery and attempts by offenders to groom children, including coercing them into sharing indecent images, or organising physical meetings.[9]

4.19. As one of our Members, the IWF works closely with Facebook and we have been calling on them to ensure that if they do encrypt messenger, there must be equivalency with the current way that they detect child sexual abuse. We want assurances that child protection will not be hampered and that victims will be protected in some way.[10]

4.20. This is a good example of where there needs to be a balance between privacy and protection, and it is an incredibly complex application to the digital world.

DNS over HTTPs:

4.21. This challenge presents itself again in the proposed roll out of the DNS over HTTPs standard, recently adopted by the Internet Engineering Taskforce (IETF). The standard did not consider the interests of children during the policy development process and, as a result, it too had the potential to undermine existing measures, quite unwittingly, to protect children. The measures had the potential to over-ride blocking lists for both child sexual abuse material and terrorist content, override parental controls and would not have informed parents, children or users of the changes before it was too late.

---

[8] https://www.iwf.org.uk/report/iwf-2019-annual-report-zero-tolerance Page 51

[9] https://www.justice.gov/opa/press-release/file/1207081/download Page 2

[10] https://committees.parliament.uk/oralevidence/451/default/ Page 33

4.22. The IWF produced a series of blogs and a short film on the issue which are available in the footnote below.[11]

E-Privacy:

4.23. It is not just industry members or technical bodies that are guilty of inadvertently failing to account for the rights of children. The European Commission's e-privacy file currently requires significant further work on a proposal initially brought forward in 2017. Challenges surrounding the drafting of the e-privacy legislation did not appreciate the need for monitoring to identify known child sexual abuse material and prevent its further dissemination. The IWF along with many other children's charities raised concerns about the proposal[12] in October 2018, calling for greater alignment with the principles established in the General Data Protection Regulation (GDPR). The issue also led to some difficult headlines as outlined in the Daily Telegraph, accusing the European Commission of protecting the privacy of potential offenders over that of child victims as the legislation did not initially include exemptions allowing investigators or companies to implement these voluntary, preventative measures.[13]

4.24. The file remains unresolved and recent proposals on the file have sought to enshrine hashing within the legislation which we believe would be a mistake in terms of future proofing the legislation. It would prevent a whole range of tools that could be of use in the future, including the use of text-based analysis to tackle emerging threats such as grooming. It further stands to highlight the complexities of balancing privacy with the protection of children.

5. What has worked well?

GDPR, Age Appropriate Design Code and the Best Interests of the Child:

5.1. The European Union's reforms to the GDPR in 2018, whilst initially creating some initial challenges for organisations like the IWF in the sharing of hashes with international partners, has on the whole been successful in changing the debate about how an individual's personal information (data) is used online.

5.2. The changes brought about in GDPR were certainly world-leading and the principle at the heart of the change was undoubtedly about giving individuals more control over their personal data. Some of the mechanisms contained within the regulation including the right to be forgotten, the right to erasure and the right to be informed have been important changes and been central in changing approaches online providers take to an individual's data.

5.3. One of the recommendations of the Guidelines to respect, protect and fulfil the rights of the child in the digital environment[14] further builds upon the GDPR and suggests that all actions in the Digital Environment should be taken in the best interest of the child as the primary consideration. It further states that this should consider all the rights of children and balance a child's right to protection as well as a child's right to participation.

---

[11] https://www.iwf.org.uk/news/exposing-child-victims-catastrophic-impact-of-dns-over-https
https://iwf.org.uk/news/dns-over-https-%E2%80%98what-does-mean-%E2%80%99
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

[12] https://www.iwf.org.uk/news/iwf-joins-coalition-of-charities-raising-concerns-over-european-commissions-e-privacy

[13] https://www.telegraph.co.uk/news/2018/10/14/european-commission-putting-paedophiles-privacy-ahead-fighting/

[14] https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

5.4. This has formed a central part of the UK's innovative approach to the Age Appropriate Design Code[15] which contains 15 principles aimed at improving the way children's data is handled online. It is the first Code of its kind, published on 21 January 2020, and whilst the Code is not yet in force, (subject to Parliamentary approval), as the foreword from the Information Commissioner sets out, is "reflective of the global direction of travel in the EU, the OECD and the USA." The Information Commissioner, Elizabeth Denham, also said: "there are laws in place to protect children in the real world and there must be laws to protect them in the digital world too."

5.5. Further measures contained within the Code include guidelines to produce data impact assessments that guide businesses through various steps in the process including when to consult with children and their parents and how to manage and minimise potentially harmful risks.

5.6. Other measures include transparency requirements that offer guidance to companies on tailoring the approach that they take to explaining their rights to children in an age appropriate manner by clearly defined age ranges.

5.7. The Code also talks about "nudge" techniques which are very well-established design features which lead or encourage users to follow a designer's preferred paths in the user's decision-making process. The Age Appropriate Design Code encouraged companies to think about "nudges" that encourage health and wellbeing, not to use "nudge" techniques that encourage poor privacy decisions, and to encourage pro-privacy nudges where appropriate.

The Better Internet for Kids Programme:

5.8. The Better Internet for Kids strategy includes several excellent initiatives which seeks to improve child rights online.

5.9. Pillar one of the strategy, providing high quality content to children, is beginning to show signs of coming to fruition. The Audio-Visual Media Services Directive will be an important part of the new regulatory framework when it comes into full force later this year. We particularly welcome the provision in the Directive to ensure that video sharing platforms do all that they can to prevent the spread of child sexual abuse on their platforms. The IWF stands ready to assist those seeking to comply with the Directive in the provision of technical services which help them to do so.

5.10. Pillar two of the strategy includes a number of initiatives that seek to improve the participation and involvement of children. The INSAFE network regularly runs sessions at the United Nation's Internet Governance Forum (IGF) and there is even a session dedicated solely to children through the youth IGF. The IWF participates actively in the Dynamic Coalition for Online Safety and there are clear attempts at both EU, UN and international levels to involve children and promote their rights.

5.11. The funding that the Commission has given to Safer Internet Centre's has also been crucially important to involving children, protecting children from harm and, without this funding, many Member States simply would not have been able to protect their children or involve them as widely as they have been. The funding given to the UK Safer Internet Centre has been crucial. Last year, Safer Internet Day in the UK reached 3 million children and young people aged 8 - 17, 50% of the overall child population in the UK. It also reached 26% of their parents and 19% of children said they were encouraged to have a conversation about their online safety with someone if something was worrying them online.

5.12. The EU funding provided by the Connecting Europe Facility has enabled the UK Safer Internet Centre to take safer internet day from a minor event in 2011, where just 70 companies supported

---

[15] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

the day, to over 1,700 organisations in 2020.

5.13. Our education packs were downloaded 1.1 million times and as well as directly engaging with 6,700 children, 1,400 parents and 3,000 teachers in 2019 alone, the UK Safer Internet Centre has trained over 21,000 professionals working with approximately 6 million children since 2012.

5.14. The IWF's experience mainly pertains, however, to pillar four of the Better Internet for Kids strategy which aims to improve the response to child sexual abuse online. There is no doubt that the INHOPE network is an important part of co-ordinating the response to the spread of child sexual abuse online, particularly with the ICCAM mechanism that enables us to transfer cases to relevant member state hotlines.

5.15. It is unfortunate, despite the funding that has been provided through the Connecting Europe Facility that Europe is now the hotspot for hosting this content. The IWF is an example of what can be achieved when industry, law enforcement, and government come together to tackle the issue, taking hosting of this abhorrent content in the UK from 18% in 1996, the year we were founded, to less than 1% ever since 2003. We have made several recommendations of how this response could be improved, but there is no doubt that the Connecting Europe Facility has been crucial to ensuring Member States have some form of hotline to process public reports of child sexual abuse. It is vital that every citizen has somewhere that they can report to, that is accessible and enables them to do the right thing.

6. What more could be done?

Centring on the rights of the child:

6.1. Any updated strategy on the rights of the child must place children at its centre. In accordance with Art.12 of the UNCRC, **children's views must be respected, considered, and addressed in all matters relating to them.** We recognise the European Commission's commitment, as laid out in the roadmap, to consult with children in the crafting of this strategy and urge the European Commission to continue this conversation with wider initiatives.

6.2. We believe that the commitment in the 2011 strategy for the 'fundamental rights check' on relevant draft legislation is a positive step but could be furthered through ensuring consultation with children on how potential legislation could affect their rights. The UK Safer Internet Centre, part funded through the Connecting Europe Facility, ensures that children are at the very heart of policy making through regularly publishing research on how children navigate the internet, and engaging and training 4,000 Digital Leaders. The Digital Leaders programme enables and empowers children to present their views on digital policy and further expands their right to be heard by legislators, ensuring that legislation is not designed exclusively for adults but addresses the concerns and needs of this wide user base.

6.3. We urge the EU to extend the 'fundamental rights check-list' outlined in the 2011 agenda on the rights of the child to all primary and secondary legislation, as well as general comments, directives and guidelines published to Member States, to ensure that children's rights are at the very heart of the Union.

6.4. One in three children use the internet. Platforms and information society services today are often designed for adults, and then retrospectively modified for children – most often limiting their online experience, rather than allowing them to thrive. **The potential impact on children and their rights, and how children will use and benefit from these services must be considered at the outset of their design** and development and the results incorporated into the final product which centres the best interest of the child.

6.5. Children's needs and wants vary greatly at different stages in their development. **Digital platform designers, legislators, and educators must recognise this and provide age-appropriate**

solutions for these children at different ages and maturity levels. This can include, but is not limited to, the use of appropriate terminology and accessible terms and conditions, in a range of formats, technical services, and clear and appropriate ways for children to report incidents of their rights being violated.

6.6. Initiatives such as the UK's Age Appropriate Design Code seek to provide incentives for industry through setting out standards for businesses to safeguard children's data, and centres the best interests of the child at it's very core.[16] This principle-based approach will allow the code to remain relevant in the face of technological advancement. The IWF recommends that the European Commission draws from this approach and introduce preventive legislation or guidance for companies providing services to EU users, including children, to ensure services are properly audited to promote the best interests of the child and the wealth of opportunities online, whilst protecting them from harm.

6.7. As outlined in previously, recent years have shown industry, technical bodies and legislators have often failed to fully consider the impacts on the rights of the child when rolling out services, developing new technical standards, or crafting legislation. Furthering and protecting the rights of children and ensuring that positive opportunities and rights are not undermined in the face of threats is a delicate balance. **We would encourage the European Commission to consult widely with those who have significant experience, technical knowledge, expertise and credibility in these areas in the development of policy. We also believe that there could be space for the European Commission to also influence standard setting bodies such as the IETF in the DNS over HTTPs examples to ensure that they are doing all they can to develop a child's rights-based approach.**

Education, Digital Skills and Resilience:

6.8. **Digital literacy, resilience and skills are key to furthering the rights of children**. Children must be empowered to understand their rights, how to exercise them, and how to report incidents of said rights being violated and must have the tools to navigate the online environment. **Parents and carers too must be digitally literate to best support their child and nurture this resilience**. We therefore encourage the future strategy to include measures for appropriately funding, designing, and disseminating digital literacy programmes, educational resources and awareness raising initiatives at both a European and Member State level. Such will allow the European Commission to address the challenges that each Member State faces, and to appropriately navigate the range of cultures and attitudes within the Union. The Connecting Europe Facility undertakes much of this important work through the Safer Internet Programme which enables Member States to engage in this critical topic, and through the INSAFE and INHOPE networks which has enabled Europe's excellent record in fostering collaboration and cooperation between nations. The Connecting Europe Facility must continue to be appropriately funded and resourced to continue its important work.

6.9. **The IWF urges the European Commission to revisit the Better Internet for Kids Strategy of 2012** to address gaps that have arisen within the document and ensure that Europe's children are best prepared to navigate the online world.

6.10. Whilst there are differences between the physical and online worlds, the two are often interconnected. The IWF applauds the European Commission's commitment to providing online safety teaching in schools, through the investment made in the work of Safer Internet Centre's in particular, but believes that this must be done supplemented through other curricular measures – **including providing appropriate relationship and sex education to address the rise in self-generated content of child abuse, through discussing healthy relationships, sexting and**

---

[16] https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-0.pdf

how to deal with inappropriate requests.

6.11. Children must be empowered to understand what constitutes a healthy relationship, and if this information is not readily provided, they will simply find it elsewhere – from sources that may provide them with an unhealthy or limited understanding. Furthermore, the current Better Internet for Kids strategy limits it's reach through focussing on providing such information primarily through schools, a limit that current global events has highlighted as schools across the continent have been forced to close. Providing such information online, or through youth groups, or training social workers, could further the reach of this critical information and improve the digital literacy and resilience of the younger generation.

6.12. Furthermore, though the IWF understand the importance of parental controls in empowering parents and protecting children from harmful content, we believe that the current Better Internet for Kids strategy fails to account for children's rights to be informed of decisions affecting them and their right to privacy. Art. 12 of the UNCRC enshrines the child's right to express their views in matters relating to them, and Art. 5. highlights the rights of the parents to provide guidance to their child, whilst recognising the child's capacity to make their own choices as they grow. We would therefore encourage the European Commission to amend the strategy to ensure that children are aware of any parental controls in operation, be it restricted access or monitoring, and can understand what this means at the appropriate stage in their development with the guidance and support of interested and actively engaged parents.

6.13. **The IWF calls on the European Commission to build on the important work that is already being undertaken**. Initiatives such as Safer Internet Day have an unparalleled reach, providing countless children with the skills and confidence to use the internet critically, effectively, and positively. Funded by the Connecting Europe Facility's, Safer Internet Programme through DG Connect, we call on the European Commission to continue to continue investing in this programme. In 2020, UK Safer Internet Day reached 49% of all UK children aged 8 – 17, and 26% of their parents. Of these, 77% of children felt more confident about what to do if they were worried about something online, and 19% spoke to someone about something that had been worrying them, whilst 76% of parents reached spoke to their children about using the internet safely.[17]

A global response:

6.14. The internet transcends the traditional boundaries of nation states. To protect and further the rights of children in the digital age, **the European Commission must work with centres of expertise across the globe.** Legislators must draw on the skills, knowledge, and expertise of experts including, but not limited to, supra-national organisations, NGO's, law enforcement, Hotlines, and industry.

6.15. The IWF believes that every internet user should be empowered to fight the spread of criminal material online and works with countries across the world to provide Reporting Portals for their citizens. As of today, IWF reporting portals are live in 40 countries, across 4 continents, empowering 2 billion people to report suspected images of children being sexually abused to our expert analysts. Internet users must be encouraged to report suspected content through awareness raising campaigns in individual countries, and we urge the European Commission to invest to ensure more people are aware of the role of Hotlines, how to report, and what constitutes criminal material.

6.16. The importance of increasing the visibility of reporting portals was noted in the Better Internet for Kids strategy, and this work must continue.[18] However, the European Commission must recognise that the increased visibility of Hotlines will result in more reports. The Dutch Hotline's

[17]https://d1afx9quaogywf.cloudfront.net/sites/default/files/Safer%20Internet%20Day%202020/Safer%20Internet%20Day%202020%20-%20Impact%20report_0.pdf

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0196&from=EN Page 14

recent annual report highlights the challenges they face with resources, stating that they were still dealing with a backlog of reports due to a high number of public reports, the limits of automation, and duplicate reports.[19]

6.17. Hotlines provide a critical role, relieving the burden on law enforcement and allowing more children to be safeguarded. The importance of this role is only growing as we all spend more time online. To effectively fight this global crime, Hotlines must be empowered to make best use of their expertise. **We are calling on the European Commission to standardise the powers of Hotlines, including their ability to assess reports, issue notice and takedowns, and proactively search for content.** The ability to proactively search is particularly important - in the first full year of proactive searching, the IWF removed 147% more criminal content than the previous year as our analysts were able to put their time, skills and knowledge to best use. Public reporting is notoriously inaccurate: in May 2020, our Hotline processed 12,500 reports from the public with only 9% found to contain criminal content.

6.18. There are several guidelines currently deployed by leading supra-national organisations, including: WePROTECT's Model National Response; The Broadband Commission for Sustainable Development's report on Child Online Safety; and the International Telecommunication Union's recently revised Child Online Protection Guidelines.[20] We urge the EU to ensure that it's new strategy on the rights of the child compliments existing strategies deployed internationally and encourages the promoted initiatives such as the IWF's Reporting Portal Solution. We applaud the EU's Commitment to promote the reform of child protection through closely monitoring progress on the rights of the child throughout the accession process in candidate countries for the Union, and request that the European Commission broadens this monitoring to include the initiatives and solutions outlined in the above international guidelines.

6.19. **The IWF would encourage the European Commission to positively invest in projects, infrastructure and technical solutions which further empower and safeguard the rights of the child.** Investing in areas such as machine learning could have a significant impact on protecting children's right to privacy, and from safeguarding them from abuse, whilst allowing them to make best use of the wealth of opportunities available online. However, any such research projects or proposals must consider the potential impact on the rights of the child.

Clear, effective legislative frameworks:

6.20. We recognise that urgent and comprehensive action is needed to address the crisis of European hosting of child sexual abuse imagery. However, we urge the European Commission to take a considered approach and work with key stakeholders to ensure that any legislative solution prioritises the best interests of the child, and that potential unintended consequences are considered. **In drafting legislation or strategy, the European Commission must work in tandem with child rights organisations, industry, law enforcement and children themselves to ensure that solutions are technically possible, effective, and work as intended – to build a world that safeguards and furthers the rights of the child.**

6.21. The IWF welcomes the European Commission's ambitious programme of legislative reform and believe that this moment represents a unique opportunity to effect real, long-lasting, positive change in the fight against child sexual abuse online and further children's rights across the world. **To realise this, there must be effective coordination between the Digital Services Act, the EU strategy for a more effective fight against child sexual abuse, and the EU strategy on the rights of the child**. To remain relevant in the face of the unprecedented pace of development, any legislation or strategy must take a flexible, principle-based approach. The impact of any initiative must be closely monitored and regularly reviewed to ensure that it

---

[19] https://inhope.org/EN/articles/eokm-published-its-2019-annual-report
[20] https://www.weprotect.org/the-model-national-response
https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_report.pdf
https://www.itu-cop-guidelines.com/

represents the most effective solution to fighting online child sexual abuse.

6.22. We urge the European Commission **not to be prescriptive in its use of technological solutions in legislation**, as the sheer pace of change in this area could result in legislation quickly becoming outdated and cumbersome. An effective strategy must be technically neutral and flexible to allow for emerging technical solutions, threats, and products.

6.23. The European Commission should look **to standardise legal frameworks across Member States** to ensure that the legislative regimes best protect the rights of the child. Frameworks should encompass the full range of unlawful acts committed in the digital environment and provide children with effective forms of redress if said rights are violated. The standardisation of definitions, terminology, and categorisations across Member States will further support the sharing of data, best practice and initiatives to best protect the rights of children online, and will support the development of a reliable, comparable data set to inform evidence-based policy making at a national and supra-national level.

6.24. The European Commission must seek to **build upon expertise and examples of best practice already operating within Europe**, utilising the remarkable work that has been accomplished across the continent. Hotlines provide a critically important role through relieving the burden on law enforcement and empowering the public to report any suspected illegal imagery. In the wake of the Covid-19 pandemic, the need for Hotlines will only intensify. We urge the European Commission to provide an explicit legal role for Hotlines to cement their future role in the fight against this content, to fund them appropriately, and standardise the powers of Hotlines so they make best use of their intelligence and expertise.