Online Safety Bill

House of Lords- Briefing for Report Stage

Key Asks:

1. **To continue to highlight the concerns raised at Committee stage about the Internet Watch Foundation's role in helping Ofcom to deliver the CSE/A provisions in the Online Safety Bill.**

2. **To reject any amendments to Use of Technology Notices for CSE/A content (Section 111) of the Bill.**

3. **To highlight the growing threat from emerging technologies such as the use of Artificial Intelligence to create Child Sexual Abuse Images and ensure law keeps pace with technology.**

Role of the Internet Watch Foundation (IWF)-

- We request that Peers remind the Government of **the importance of implementing the legislation** and making best use of the skills and expertise of the charitable sector, in particular, the IWF, in delivering the legislation.

- It would be helpful for Peers to remind the Government of remarks made by Dame Melanie Dawes, Ofcom CEO, that she "***does not view regulation as a solo effort***"[1] and continue to push Government to set out a timeline for when decisions might be made around co-designation.

- Government amendments at Report Stage, specify that certain Codes of Practice must be delivered by Ofcom within 18 months of Royal Assent (**Amendment 133**) and the insertion of a new Clause after Clause 174, (**Amendment 230**), specify timelines for Ofcom to first publish guidance under certain provisions in this Act, may present a useful opportunity for peers to refer to when decisions about designating other bodies might also need to be taken.

- We also encourage Peers to speak to the expertise of the Internet Watch Foundation in relation to **Amendment 253** (Lord Clement-Jones), which requires Ofcom to co-operate and disclose information with a regulator established by statute or a recognised self-regulatory body for tackling harms arising from illegal content (CSEA), primary priority content harmful to children, priority content harmful to children or priority content that is harmful to adults or in the case of criminal proceedings.

[1] https://committees.parliament.uk/oralevidence/12819/html/ Q.135, DCMS Select Committee Session, 14 March 2023

- We would also request that peers continue to remind the House of the findings of the Independent Inquiry into Child Sexual Abuse (IICSA) which concluded: "***The IWF sits at the heart of the national response to combatting the proliferation of child sexual abuse images online***,"[2] and the report of the joint committee appointed to scrutinise the Bill which recommended: "***We expect Ofcom to work closely with experts like the Internet Watch Foundation, to develop and update the child sexual exploitation code of practice; monitor compliance and during investigations***."[3]

End-to-End Encryption-

We would strongly urge members **reject** amendments to **Clause 111** (Notices to deal with Terrorism content CSEA content (or both).

This includes amendment **255** (Lord Moylan and Baroness Fox) which would create a specific carve out for services that are End-to-End Encrypted not to be subject to these notices.

We also urge Members to reject amendments **256**, **257, and 259** (Lord Stevenson) which introduces additional safeguards and oversight equivalent to Judicial Review for the use of these notices. We already believe that the regulator will have to have a high burden of proof before issuing a notice and we are concerned that additional safeguards will further slowdown the process in the application of these notices and adversely impact the protection of children.

- We would also like to remind members of a research paper published by Ian Levy and Crispin Robinson, two world leading cryptographers from the UK's **National Cyber Security Centre (NCSC)** which suggested there are several techniques companies could be deploying to prevent the spread of child sexual abuse in End-to-End Encrypted environments without compromising privacy.

- The **Information Commissioner's Office** has also issued guidance as part of the UK Government's Safety Tech Challenge Fund which we believe also created strong safeguards, aligned with current legislation on how this technology could be applied.

- The **Internet Watch Foundation** also has a page dedicated to explaining the differences between standard encryption and end-to-end encryption and the impact this will have on child protection.

- The **scale and nature** of the threat of child sexual abuse is **too large to ignore**. We know through the National Crime Agency's Strategic Threat Assessment there are an estimated **500,000-850,000** people who pose a sexual threat to children in the UK.

- The IWF removed **252,000 webpages** in the last year from the open internet; we cannot allow parts of the internet to allow child sexual abuse images to circulate freely, these amendments to Clause 111 make that a possibility and could see the threat from CSAM grow further.

In **rejecting** these amendments, we would request that members remind the House of the scale and nature of the CSE/A threat, highlight the work of the safety tech challenge fund and question why technology companies haven't yet explored options set out in the Levy/Robinson paper to fight child sexual abuse.

---

[2] https://www.iicsa.org.uk/reports-recommendations/publications/investigation/internet point 29, page 33.
[3] https://publications.parliament.uk/pa/jt5802/jtselect/jtonlinesafety/129/129.pdf Point352, Page 103

Artificial Intelligence and Child Sexual Abuse-

- In the past few months, the IWF has been seeing content of child sexual abuse that has been created using Artificial Intelligence. We have received a small number of anonymous reports from members of the public and actioned a small number of webpages (URLs) containing this content.

- Some of this content has been the ***most severe forms*** of child sexual abuse and meets the **Category A** threshold for child sexual abuse and can depict children as young as **0-2.**

- The material is now so realistic that IWF analysts struggle to tell the difference between real images of abuse and those generated using Artificial Intelligence. There has been a stark improvement in the quality of these images in the past three months.

- Though distribution of these images is not currently high, we know that information on how to create these images is being regular discussed amongst offenders in forums and this demonstrates the ***need for the law and regulation to continue to evolve*** in response to these threats.

- The IWF urges Peers to support **Amendments 27, 153-157, 285, 293** to the Bill (Lord Parkinson, Baroness Kidron, Lord Clement-Jones) which brings Generative AI bots into scope of the legislation.

- We also support Amendments to Clause 70 **(Amendment 206-209 and 276)** which makes it clear that Part 5 providers (Pornographic Service providers) that ensures automated tools or algorithms made available by providers or content created by them are expressly covered in the Bill.

Age Verification-

- IWF welcomes amendments **37, 38, 41,102, 210-217, 278, 284, 291, 292** to Clauses 16, 17, 30, 31, 72, 206, 211, 212 of the Bill which strengthens the provision around age verification and estimation. We also support **Amendment 277** which clarifies that self-declaration of age is explicitly ruled out and **encourage peers to vote in favour** of these amendments.
- We also are **in favour** of strong protection of data for users and support **Amendment 125** (Baroness Kidron, Harding, and Lord Stevenson) that specifies data collected for age assurance should not be repurposed for other purposes.
- We also encourage peers to ensure that there is alignment with the ICO's Age-Appropriate Design Code and encourage peers to **vote in favour** of amendments **100** and **101** (Baroness Kidron, Lord Stevenson, Baroness Harding.)
- We are also in favour of **Amendment 270** which requires Ofcom to produce and publish a report about the use of age assurance by regulated entities.

Violence Against Women and Girls-

The IWF has long campaigned for a greater focus on the disproportionate amount of harm women and girls suffer online.

- Girls were present in **96% of the images and videos** we removed from the Internet in 2022.

- We have also seen a huge increase in self-generated child sexual abuse images in the past three years.
- Over three quarters of the content we removed from the internet in 2022 was self-generated by children themselves. We removed **199,363** webpages with girls appearing in **80%** of self-generated child sexual abuse material we removed.
- This issue tends to affect **11-13 girls**, who appear most in the imagery we remove, with **7–10-year-olds** the fastest growing age range in 2022.

We ***welcome*** the introduction of **Amendment 152** (Lord Parkinson et al) which will require Ofcom to produce guidance about the protection of women and girls for providers of Part 3 Services.

Secretary of State's Powers-

We welcome amendments to the Bill from the Minister, Lord Parkinson, to Clause 39 (**Amendments 134-138**) which provides clarification that the Secretary of State can only direct Ofcom on matters of National Security, Public Safety, Public Health or for relations with the Government of a country outside the United Kingdom related to Terrorism or CSEA.

We are also encouraging peers to support the **Amendment 140** (Baroness Stowell et al) which would require Parliament to be informed when a direction has been issued for matters of public security, without including details of that direction. It is important for organisations like the IWF and Parliament to be aware of potential changes to CSE/A Codes so that we can assist in responding to the threat or at least aware that a change has been requested or made.

We encourage peers to **vote in favour** of this amendments.

Duty to Report Child Sexual Abuse Material-

We support the Government amendments (**185** and **186**) to Clause 60, Regulations of Reports to the NCA, which requires companies to retain data they have reported to the NCA in relation to child sexual abuse for a specified period of time.

Review of Pornography-

The IWF also supports the Government's announcement to review the laws around pornography.

We have recently announced that we are working with Mindgeek, a technology company, which operates several brands, including Pornhub, which offer legal, adult themed content to a global audience to explore a potential blueprint for the adult industry in how they can fight the spread of child sexual abuse online, in a two-year pilot project.

This work builds on the successful collaboration between the IWF, Lucy Faithful Foundation and Mindgeek in developing a chatbot which deploys on Pornhub and alerts users to when they are using keywords which may return child sexual abuse material and diverts them to where they can get help and support. The IWF welcomes the opportunity of feeding in the findings of our work to the Government's review.

For more information about this briefing please contact:

Michael Tunks, Head of Policy and Public Affairs, Internet Watch Foundation (IWF)

mike@iwf.org.uk 07377449342