

## Online Safety Bill - 2<sup>nd</sup> Reading House of Lords

Wednesday 1 February 2023

### Key Asks:

1. To highlight the growing threat of child sexual abuse online, highlighting the latest statistics published by the Internet Watch Foundation (IWF). Speaking in support of why the Bill is much needed.
2. To highlight the gaps in the legislation in implementing the Bill, by explaining the need for Ofcom to work with NGOs like the IWF to deliver the Bill's objectives.
3. To highlight the urgency for Ofcom to clarify the role for the IWF to avoid undermining the IWF's work which could have a catastrophic impact on the UK's efforts to remove child sexual abuse imagery, with an impact directly on abused children and their revictimisation.
4. To defend the current draft of the Bill in relation to End-to-End Encryption and the use of technology notices in relation to End-to-End Encrypted environments. It should be possible to prevent known child sexual abuse images entering or leaving these environments without breaking encryption or impinging on privacy.

### Latest statistics in the fight against the spread of child sexual abuse online, evidence of the hugely positive impact of the IWF's work for the UK and globally:

- [New figures](#) released by the IWF on Friday 27 January highlight the growth, scale and complexity of the spread of child sexual abuse online.
- Since 2019, the last year prior to the pandemic, the IWF has recorded a **1,058%** increase in the number of webpages depicting the sexual abuse of children in the **7-10 age range** who have been groomed, coerced or exploited online.
- In the past year alone, this has grown by **129%** as IWF has removed **63,050** webpages of sexually abused **7-10-year-olds** from the internet who were groomed/coerced online. **8,827** of these reports are Category A, (penetration, torture, sexual activity with animals) - the most severe forms of abuse.
- In 2022, the IWF investigated a total of **375,230** reports of suspected child sexual abuse and confirmed **255,588** reports as containing child sexual abuse containing one, to thousands of images and videos each.
- In 2021, **96%** of the imagery the IWF removed was of girls.
- The IWF is the only non-law enforcement organisation to have access to the national Child Abuse Image Database (CAID). As the recognised experts in the country, IWF have, for the Home Office and law enforcement, assessed and quality assured 2 million Category A and B images for CAID by December 2021.

## Gaps in the implementation of the Online Safety Bill:

- The IWF is concerned that, with the passage of the Bill being months away, there are significant gaps which potentially need closing around how the Bill is going to work and operate in practice.
- Currently the IWF's activities rely on informal collaboration: It has a memorandum of understanding between the National Police Chief's Council (NPCC) and the Crown Prosecution Service (CPS) and there is cross party recognition that this collaboration has been a national success story. Both the Joint Committee appointed to scrutinise the draft Bill reached this conclusion, as did the [Independent Inquiry into Child Sexual Abuse \(IICSA\)](#) which concluded the IWF "sat at the heart of the national response to combatting the proliferation of child sexual abuse images online".
- However, despite positive discussions with Ofcom, Government and Law Enforcement, there is no clarity on the role the IWF will play in the future regulatory framework, including through mechanisms such as co-designation as had been mentioned in the Online Harms White Paper in 2020 and supported through the [Joint Committee](#) Scrutinising the Online Safety Bill. This risks undermining the IWF's globally-recognised efforts and could be catastrophic for the children benefiting from its work.
- The Government failed to provide a response regarding the role of the IWF in the [response to the Joint Committee's recommendations](#). Former Government Minister, Chris Philip MP, had also previously stated: "It expects the good work relationships to continue."
- **Question to Government: "With the Online Safety Bill around 6 months from receiving Royal Assent and the illegal content provisions being the first to be developed in Ofcom's roadmap, when can IWF expect clarification on the role it will play, and how do Ofcom and Government intend to support the organisation in scaling up?"**

## End-to-End Encryption:

- The IWF's view on the proposed amendments already published by the Government for companies "to use their best endeavours" to detect child sexual abuse material in End-to-End Encrypted environments is technically more workable than the previous draft of the Bill (which would have required companies to use accredited technology in End-to-End Encrypted environments).
- It is now possible to detect known child sexual abuse material at the point that it's attempted to be uploaded to an End-to-End Encrypted environment, before it's transmitted, distributed, shared.
- We believe that much more detail is required on what a company's "best endeavours" might look like. A lot of this detail through the proposed amendment is left to secondary legislation and Ofcom to decide what "good" looks like. This is why we believe it is crucial that Ofcom has the ability to co-designate and work with others, like the IWF, who have expertise in this space.
- Secondly, being able to see the content (i.e., the image or the video) is crucial to getting it removed from the internet and preventing it recirculating. The content is also of vital importance to the work of the IWF and law enforcement. It is of particular importance to the NCA who require content in order to obtain a warrant to pursue offenders through court orders.
- Members of the Global Encryption Coalition have recently [sent a letter](#) to the Prime Minister from Members of the Global Encryption Coalition (amongst others) which suggests that the Bill undermines End-to-End Encryption.

- The IWF believe that the Bill does not threaten encryption. At IWF we recognise that strong encryption is fundamentally a good thing that helps keep banking transactions and medical information secure and confidential.
- We are not against encryption, we are not proposing backdoors or seeking to compromise its security in anyway. However, we believe companies should not be seeking to introduce End-to-End Encryption where they have large numbers of child users that are connected or can be contacted by large numbers of adult users without any protections or mitigations in place to identify this imagery.
- We believe the Bill sets the right challenge of companies to ensure they have safety embedded and to balance the right to privacy with the rights of children to grow up in a childhood free from sexual exploitation and abuse.