

Briefing from the Internet Watch Foundation: Impact of smartphones and social media on children

Westminster Hall Debate: 14 May from 9:30 am

Key Asks:

- 1. To ensure that there is **no delay** in implementing the Online Safety Act
- 2. Any measures around **stronger protections on devices** are welcome but must be seen in the context of **"layering"** online protection measures, not instead of measures already approved in Parliament.
- 3. To ask that measures around device level protections consider what could be done to tackle the issue of **End-to-End Encrypted** applications and ensure stronger online child protection in these environments.
- 4. That MPs campaign for **the five-point plan** published by the All-Party Parliamentary Group on Online Safety on Social Media.

Challenges presented by children's unfettered access to smartphones and social media:

- Ofcom's most recent research suggests that almost **25%** of children aged five to seven have a smartphone of their own.
- **32%** of children aged 5-7-year-olds uses social media independently of their parents.
- **42%** of parents of 5–7-year-olds use social media with their children.

The IWF has had another record year in the number of reports processed and removed from the internet of child sexual abuse. In 2023, we assessed **392,665 reports** of suspected child sexual abuse and **confirmed 275,652** web pages contained images or videos of children suffering sexual abuse.

92% of the imagery the IWF discovered shows "self-generated" child sexual abuse. Where a child had developed this imagery themselves, often in bathrooms or other domestic settings.

For the first time, **the IWF has analysed 2,401 individual child sexual abuse images that had been self-generated, in the 3-6 age range.** Of these images, **91% were of girls** and mainly in domestic settings such as bedrooms and bathrooms.

The abuse, which analysts have seen ranging from sexual posing to sadism, degradation, and even sexual acts with animals is directed by perpetrators and often recorded without the child's knowledge.

Implementing the Online Safety Act:

It is important that there **are no delays** to the <u>Ofcom's Roadmap for implementation</u> of the Online Safety Act.

Ofcom has already published and consulted on:

- Illegal harms
- Age Assurance for Pornographic providers (Part 5 providers)
- Categorisation (advice to Secretary of State published)

And has recently announced its Protection of Children Consultation, on 8 May, which will be due to close on 17 July.

It is the view of the Internet Watch Foundation that Ofcom should be focussed on delivering the improvements promised in the Online Safety Act and that whilst any further measures on smartphone use and social media are welcome, **it should not be seen by industry as an opportunity to delay implementing the measures Ofcom are proposing in their guidance.**

We have welcomed proposals by Ofcom to mandate the use of Hash Matching, Webpage blocking of known child sexual abuse material and the 10 safety by design grooming mitigations, but in our response, we have recommended Ofcom go further by:

- Updating its illegal content codes to **include the detection of new child sexual** abuse material using automated content classifiers as is current industry best practice. Both <u>Google</u> and <u>Meta</u> have issued blogs explaining how the utilise AI and Machine Learning to prioritise and detect new child sexual abuse material.
- To ensure that **age verification measures** are added to the currently proposed grooming mitigations to ensure that they can not be easily circumvented by a child opening an adults account.
- That there is a greater focus on **safety by design** measures to ensure that Age-Appropriate Design is hard wired as part of the development process of services. There is best practice internationally that can be pointed to through the <u>Australian e-safety</u> <u>commissioner's</u> principles, easy assessment tools for services, resources for ethical investment and guidance for the tertiary sector on how to design platforms safely.
- Ensure that **small but high harm platforms** are properly caught by the new regulations, in line with late concession won by Baroness Morgan in the House of Lords.

We have also **consistently called on Ofcom to work with organisations like us in delivering the Online Safety Act's objectives**.

Datasets that we provide such as an image hash list and URL blocking list are services that potentially up to 100,000 companies may need to have access to ensure compliance with the new Codes of Practice but as Ofcom's recent consultation acknowledges, we need to be supported to meet the new demand that regulation has created for our services.

Greater Device level protections for children:

The IWF is extremely concerned about the impact technology has on the lives of children and young people and supports any measures that better protect them online.

Whilst we believe the first objective should be implementing the existing legislation, we also believe that on device protections and advice and age verification at the point of sale are a sensible way of building on existing legislation as part of a **"layered" approach** to online safety.

The All-Party Parliamentary Group on Online Safety on Social Media recently recommended a <u>five-point plan for improved online safety</u> following a symposium held with children and young people and online safety tech providers in February.

The Group recommended:

- 1. A Greater awareness of the Online Safety Act in schools.
- 2. Children having a voice in the process to help design the rules of the road for technology companies.
- 3. Telecoms providers and device manufacturers verifying the ages of their users and issuing clear, simple online safety advice about parental controls.
- 4. The Department for Education reviews its Keeping Children Safe in Education Guidance
- 5. Children should have age-appropriate experiences. Ofcom should consider age gating content and utilizing age verification, estimation, and assurance technology so that children can have a tailored experience online in much the same way broadcast and film is regulated today.

Evidence of best practice:

- In 2019, the French Government, discovered only **44%** of parents had configured their children's devices and only **38%** had used parental controls.
- At the time, children's smart phone usage was beginning on average around the age of
 9.
- By the **age of 12**, children were already being exposed to **pornographic content**, with children also being exposed to **violent and hateful content**.
- In July 2023, <u>France issued two decrees</u> to clarify the <u>application of a law passed on 2</u> <u>March 2022</u> aimed at reinforcing parental control on internet access equipment, which required from manufacturers of terminal equipment to provide users with access to an easily accessible and understandable parental control device.
- Manufacturers **must draw up technical documentation and a declaration of conformity for each type of terminal equipment**. They must also provide users with a certain amount of information, in particular the features and functionalities offered by the parental control device installed on their equipment as well as **an associated explanatory leaflet**.
- This includes as a minimum enabling the blocking or download of content made available by software application shops or access to preinstalled content which is prohibited for minors. Activation of the device must be offered when the device is first put into service.

End-to-End Encryption

The IWF, NSPCC, law enforcement and other child protection charities <u>have consistently warned</u> that the introduction of end-to-end encryption by platforms is a huge blow to child protection efforts.

Ofcom's illegal harms consultation also acknowledge that End-to-End Encryption is a functionality that poses risks to the dissemination of child sexual abuse material and exploitation of children through grooming.

- On 6 December 2023, <u>Meta announced</u> that they had started rolling out end-to-end encryption globally for all personal chats and calls on Messenger.
- Meta is wilfully turning a blind eye to child sexual abuse as they will no longer be able to use highly effective, automated tools such as image hashing, currently considered industry best practice, to detect abuse and safeguard children.

The National Center for Missing and Exploited Children (NCMEC's) latest statistics on instances of suspected child sexual exploitation in the US revealed that:

- Last year 36 million tips were sent to NCMEC from electronic service providers.
- **17.8 million** of those tips came from **Facebook services** and **11.4 million** were made from **Instagram.**

These crucial reports could be lost following Meta's rollout of end-to-end encryption on its services.

We have seen just how damaging it can be when companies stop voluntarily scanning for child sexual abuse imagery.

• In the first six months of 2021, due to changes in EU privacy laws, Meta took the decision to stop scanning for CSA on its Messenger service. This led to a <u>58% reduction in reports</u> to NCMEC from EU accounts. Imagine the impact of this on a global scale.

Techniques that could be deployed to tackle child sexual abuse in E2EE environments:

- Apple announced in August 2021 proposals to detect child sexual abuse in a privacypreserving way. It stated its proposals had the support of both child safety and privacy campaigners adding that hashes used to detect child sexual abuse content when photos and videos were backed up by users to its cloud technology, would **only come from two trusted child protection organisations**, would be **manually reviewed** before being referred to law enforcement.
- <u>Ian Levy and Crispin Robinson</u>, two world leading cryptographers, have also set out suggestions for how child protection could also be improved in end-to-end encrypted environments. This paper included suggestions such as client-side scanning techniques, which could be performed at device level and would be compatible with End-to-End Encrypted environments.

- Ofcom must continue to build out its online safety regime it makes the most of the powers it has been afforded in Section 122 of the Online Safety Act, which sets out how "Use of Technology Notices" may be used.
- This includes compelling companies to use their "best endeavours" to prevent child sexual abuse material from circulating in these environments and what a minimum standard of accuracy may look like. We believe Ofcom should be asking Apple about the developments in its technology and encouraging companies to explore the recommendations set out by Ian Levy and Crispin Robinson.