



Draft Online Safety (Basic Online Safety Expectations) Determination 2021 consultation

Organisation responding: The Internet Watch Foundation (IWF)

Address: Internet Watch Foundation, Discovery House, Chivers Way, Vision Park, Histon, Cambridge, United Kingdom, CB24 9ZR

Contact details of the person responding: Abigail Fedorovsky, Policy and Public Affairs Assistant, abigail@iwf.org.uk

1. About the Internet Watch Foundation (IWF)

- 1.1 The Internet Watch Foundation (IWF) is an international hotline based in the UK which provides a secure and anonymous place for 2.5 billion people globally to report suspected child sexual abuse material (CSAM) in their local language. If these reports are confirmed as CSAM, our analysts work to have that imagery removed from the internet - wherever it may be hosted in the world.
- 1.2 The IWF's vision is an internet free from child sexual abuse and we are a charity that works in partnership with the technology industry, law enforcement (including Europol and Interpol), and other Government's globally to achieve that aim.
- 1.3 The technical tools and services we provide help to keep technology companies platforms and services free from CSAM. The IWF has over 170 Members from the internet industry who deploy our services to combat the spread of CSAM on their platforms.
- 1.4 **In 2020 we assessed and removed 153,383 reports of CSAM from the internet. Each report can contain from one to thousands of individual images or videos, so this is millions removed in one year.**
- 1.5 Along with 45 other hotlines around the world, the IWF is part of the International Association of Internet Hotlines (INHOPE.)
- 1.6 **In 2020, more than half (57%) of all the unique child sexual abuse URLs exchanged through INHOPE's database in 2020 were identified by the IWF.**
- 1.7 We are also one third of the UK Safer Internet Centre, a partnership of three organisations working to make the internet a safer place for children through providing our hotline, helplines and an awareness centre that provides educational resources to children, their parents, and schools.

2. Summary

- 2.1 The IWF welcomes the opportunity to respond to this consultation. As the UK's hotline for assessing and removing child sexual abuse material, we believe we can contribute unique insights into how the Australian legislation could work when it comes to tackling illegal content online.

2.2 We welcome the Online Safety Act's scope in setting out online safety expectations on a whole range of platforms and services. We would also like to appreciate the emphasis on cooperation, both with the eSafety Commissioner and on platforms needing to communicate and collaborate with each other. We are pleased that providers will have to prevent children accessing class 2 material, as we have seen the detrimental impact that viewing age-inappropriate adult content can have on children in forming their views about relationships and the digital world.

2.3 We would like to offer a few recommendations from our own work, including:

1. **Providers should be expected to sign up for hash and blocking lists from hotlines and law enforcement agencies.**
2. **The eSafety Commissioner should be able to proactively search the internet for child sexual abuse material to determine if platforms are effectively dealing with the problem.**
3. **The eSafety Commissioner should continue to collaborate with hotlines around the world to determine if there is illegal content on platforms.**
4. **The eSafety Commissioner should be aware of new and emerging trends and threats, should work with platforms to tackle these, and should regularly inform platforms of new threats to deal with.**

3. Expectation 6: provider will take reasonable steps to ensure safe use.

3.1 Many hotlines and law enforcement agencies around the world have created hash lists and blocking lists, for instance the IWF's hash list currently has one million unique images on it. We are working with the UK Government to add another two million by 2023.

3.2 We know that the majority of CSAM on the internet is duplicates of the same image or video, for instance US law enforcement confirmed to one victim that they knew of over 70,000 instances where her image had been shared. Mandating that platforms use hash lists allows them to scan and remove duplicates, but also prevents many of these duplicates being reuploaded at all.

3.3 We also know that blocking lists can be highly effective. In just one month in 2020, three of the IWF's members counted 8.8 million attempted hits to our blocking list by UK users alone.

3.4 Given that the internet is not restricted to national borders, as much as possible, it is essential that there is effective global collaboration in sharing some of these datasets across borders.

4. Expectation 8: provider will take reasonable steps regarding encrypted services.

4.1 We welcome Expectation 8 that places requirements on platforms that use encryption to "take reasonable steps to develop and implement processes to detect and address material or activity on the service that is or may be unlawful or harmful." We saw the impact in the EU when Facebook decided to stop scanning their platforms for CSAM because of the temporary derogation from the e-privacy directive not being secured in time. This led to a 48% reduction in CSAM referrals from EU accounts to the National Center for Missing and Exploited Children since December 2020 and further demonstrates the permanent loss of these referrals were the platform to encrypt.

- 4.2 It is the IWF's position that companies should not be encrypting their services until appropriate child safety measures can be implemented on their platforms. This includes being able to prevent, detect and refer any illegal child sexual abuse imagery on their services.
- 4.3 It is essential that this content continues to be identified, so we would recommend that this Expectation ensures equivalency for encrypted platforms. We would suggest that the Australian Government incentivise companies to develop or adopt innovative solutions to continue scanning for illegal content in encrypted services.

5. Expectation 20: provider will provide requested information to the Commissioner.

- 5.1 It is essential that the eSafety Commissioner is able to access full information about the scale of CSAM on platforms, and how effective they are at dealing with this. We would recommend that the Commissioner is able to proactively search the internet for CSAM, enabling them to truly understand whether the platforms are doing enough.
- 5.2 We have seen through our work that proactive searching tends to be much more accurate than public reports. For instance, around 80% of the CSAM we action is found proactively by our team of analysts.
- 5.3 **In the first full year that the IWF was allowed to proactively search for content, there was a 147% increase in the amount of CSAM we were able to remove.**
- 5.4 There are existing systems in place for hotlines to share information with each other and flag any content hosted nationally, for instance through INHOPE. We would recommend that these processes continue, and international collaboration is strengthened as much as possible. This will also enable the eSafety Commissioner a better understanding of which platforms have a problem with CSAM.
- 5.5 Finally, we believe that this landscape is constantly evolving, so the eSafety Commissioner must be able to continue to identify new threats and trends and have regular communication with platforms about how they are addressing these.
- 5.6 For instance, over the last few years we have seen a dramatic increase in the amount of "self-generated"/"first-person produced" indecent imagery, often where young girls are groomed or coerced into sexual activity in front of a webcam or camera-enabled device which is then captured by an offender. This often takes place in a child's bedroom or domestic setting. From 2019-2020 we saw a 77% increase and now so far in 2021 we have seen a 117% increase from the year before.
- 5.7 Most of the victims of this type of abuse are 11–13-year-old girls. It is essential that the eSafety Commissioner is able to update expectations on platforms if there is a particular new and worrying trend such as this, given how quickly new technology appears and dominates the landscape. It is vital that there are both technological and educational initiatives to address trends such as this.

6. Conclusion

- 6.1 We welcome Australia's new Online Safety Act as an important step forward in terms of online safety for children, both in Australia and in the world. We look forward to working closely with the eSafety Commissioner as this, and our own Online Safety Act, develop over the coming years.