Online Safety Bill

Second Reading, House of Commons- Tuesday 19 April 2022

Key Asks-

1. **Government provides greater clarity on how Ofcom will work with third parties, including honouring its White Paper Response commitment to co-designation.**
2. **Government speeds up the implementation of the legislation relating to CSE/A by utilising the interim Code of Practice and 5-Eyes Voluntary Principles.**
3. **Parliamentarians defend, promote and champion the effectiveness and accuracy of technologies for dealing with CSE/A content online and actively advocate for their inclusion in guidance from Ofcom.**
4. **The Government considers bringing Virtual Private Networks (VPNs) into scope, ensuring they disable public access to CSE/A content.**
5. **The Government and Ofcom consider the impact of a regulatory levy on third sector voluntary initiatives such as IWF membership that companies currently support.**

About the IWF-

The Internet Watch Foundation (IWF) is a non-profit organisation that seeks to eliminate child sexual abuse material (CSAM) online, wherever it is hosted in the world. We receive reports from members of the public, proactively search the internet for CSAM, and seek to prevent the distribution of this material online through the technical services we offer industry.

Relationship between Ofcom and Third Parties-

The Joint Committee appointed to scrutinise the Government's draft Online Safety Bill concluded that the IWF:

"Made a persuasive case that they should be co-designated by Ofcom to regulate CSE/A content, an argument supported by Crown Prosecution Service (CPS) and Talk-Talk."[1]

Despite the improvements made to the Online Safety Bill, there remains little detail from the Government or Ofcom on the timetable for implementation of the legislation or how the Government intends to honour the commitment made in its full response to the Online Harms White Paper to:

"Ensure the regulator (Ofcom) is able to work effectively with a range of organisations. This will be delivered through a range of means including co-designation." [2]

The IWF has an excellent track record in delivering success in minimising the spread of illegal content, the dissemination of the content and ensuring its swift removal by working with companies. These are all requirements under Clause 9 of the Online Safety Bill.

- In one month (April 2020), the IWF and three of its industry partners blocked **8.8 million attempts** to access known CSAM from UK users.
- In the year the IWF was founded **18%** of the world's known CSAM was hosted in the UK, today it is less than **1%** and has been ever since 2003.
- The IWF's record time from notification for removal of CSAM is **2 minutes**, with **60%** of the notices we issue being complied with in **under 2 hours.**

[1] https://committees.parliament.uk/publications/8206/documents/84092/default/ Page 103

[2] https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response Points 3.27-3.33

The Independent Inquiry into Child Sexual Abuse's thematic report into the internet concluded:

"The IWF sits at the heart of the national response to combating the proliferation of indecent images of children. It deserves to be publicly acknowledged as being a vital part of how and why, comparatively little CSAM is hosted in the UK."[3]

We are calling on the Government for much greater clarity on how the regime will work in practice and how it will build on its already world-leading approach to dealing with CSE/A content.

There is already an interim Code of Practice for Child Sexual Exploitation and Abuse (CSE/A)[4] which the IWF and our industry members assisted the Home Office in designing. Compliance with this legislation could be fast tracked if Government and Ofcom adopted the Code and instructed the companies and the regulator to work with the IWF as a co-designated body to deal with CSE/A.

Notices to deal with Child Sexual Exploitation and Abuse (CSE/A)- Accredited Technology

Under Part 7, Chapter 5, of the Online Safety Bill, Ofcom will have the power to direct companies to use "accredited technology" to identify CSEA content, whether communicated publicly or privately by means of the service, and to remove the content quickly.

At IWF we assist companies to do this by providing them with "hashes" (see below) of previously identified CSAM to prevent the upload of this material to their platform. This helps to stop the images of victims being recirculated again and again. Tech companies can then notify law enforcement of the details about who has uploaded this content and an investigation can be conducted and offenders sharing this content held to account.

These technologies are extremely accurate, and, thanks to the quality of our datasets, they ensure companies are only detecting imagery that is illegal.

The types of technologies Ofcom could consider accrediting include:

Image Hashing:

A Hash is a unique string of letters and numbers which can be applied to an image. This string of letters and numbers can be "matched" every time a user attempts to upload a known illegal image to a platform.

PhotoDNA:

PhotoDNA was created in 2009 in a collaboration between Microsoft and Professor Hany Farid at University of Berkley. PhotoDNA is a vitally important tool in the detection of CSEA online. It enables law enforcement, charities and NGOs and the internet industry to find copies of an image even when it has been digitally altered.

It is one of the most important technical developments in online child protection and is extremely accurate. The failure rate of PhotoDNA is **1 in 50 to 100 billion.** This gives a high degree of certainty to companies that what they are removing is illegal and a firm basis for law enforcement to pursue offenders.

Webpage blocking:

Most of the imagery the IWF removes from the internet is hosted outside the UK. Whilst we are waiting for removal, we can disable public access to an image or webpage by adding it to our webpage blocking list. This can be utilised by search providers to deindex known webpages containing CSAM.

[3] https://www.iicsa.org.uk/key-documents/17805/view/internet-investigation-report-march-2020.pdf Point 29, Page 33

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944034/1704__HO__INTERIM_CODE_OF_PRACTICE_CSEA_v.2.1_14-12-2020.pdf

End to End Encryption (E2EE)-

Despite the inclusion within the Bill for companies to use accredited technologies to detect CSAM in both public and private channels, at present, there is no technical way for companies to detect this material in End-to-End Encrypted environments.

The IWF is not against strong encryption, but we believe that companies should be proving through their risk assessments that they have pursued other avenues to protect user privacy before pursuing E2EE. We believe that they should have measures in place to detect and report CSAM in the same way they do now in non-encrypted channels if E2EE is to be pursued. This is particularly important for platforms with large numbers of child users.

The impact of E2EE could be devastating for child protection. In 2020, Meta made **20.3 million reports** to the US Mandatory Reporting body, the National Center for Missing and Exploited Children (NCMEC) but, due to the EU being unable to secure a temporary derogation from the e-privacy directive in 2021, Meta stopped scanning their platform for CSAM. This led to a **58% reduction in reports** from EU accounts.[5] **The impact of Meta pursuing E2EE would lead to 20million reports of CSAM and the content (which is vital to law enforcement investigations and preventing it from recirculating) those reports contain being lost.**

Mandatory reporting body for CSE/A content-

There are already effective international collaboration systems in place to deal with CSE/A. Many of the large platforms in scope of this legislation who are US based, are already required to report CSE/A detected on their systems to NCMEC in the United States, under US law. NCMEC then ensures that where there is information pertinent to UK Law Enforcement that this is referred to them for investigation.

The IWF welcomes the introduction of mandatory reporting for companies who do not currently report which, along with greater transparency reports from companies, will help us to better understand the nature of this crime and how it manifests online. However, we do have some concerns about how this will impact on international reporting structures and how particularly Clause 59 of the Bill could be complex and onerous for companies.

Clause 59 requires both UK and non-UK providers to report all UK-linked CSEA content to the NCA. Companies first, will have to ascertain whether there is a link to the UK in any referral they make, and, secondly, this could also duplicate the international reporting structure already in place where UK-linked content would currently already be referred to the NCA from the US National Center for Missing and Exploited Children. This could lead to two reports for the same offence being made to law enforcement which would be inefficient.

The Online Safety Bill must ensure that the introduction of mandatory reporting complements other international reporting structures, including the anticipated forthcoming EU measure which will also introduce a mandatory reporting.

It will also be important to ensure companies are making quality referrals, so appropriate guidance needs to be issued to industry on the types of information required in a referral and to ensure that any referrals relate to illegal content, to ensure that law enforcement is able to prioritise the highest risk and harm cases.

This will require access to quality data sets, which the IWF is able to supply in compliance with UK Sentencing Council Guidelines.

Extra-Territorial Scope-

The Government must also recognise that the progress made to date in the removal of CSAM online is because there is clear legal certainty internationally about what constitutes Child Sexual Abuse Material online. This is an international problem that is complex and requires international collaboration.

---

[5] We Are in Danger of Losing the Global Battle for Child Safety (missingkids.org)

This is an extraterritorial problem, in 2021, the IWF removed **252,000 webpages** containing CSAM (each individual webpage can contain thousands of individual images, so this is millions of images and videos removed.) Less than **1%** were hosted in the UK.

90% of the webpages we actioned for removal last year were hosted in Europe (beyond the UK), predominantly in the Netherlands where the presence of strong infrastructure and bullet proof hosting providers, who refuse to act without a court order, are responsible for a large proportion of the problem. We often find this content on **image hosting boards (81%)** and **cyberlockers (5%)** which would not be in scope of the UK Government Online Safety Bill**.** Many refuse to act on notices for takedown unless a court order has been obtained- which simply isn't possible given the volumes of content we refer to them annually. Many of these companies are small providers, not well known to the public and cause a disproportionate amount of harm.

The Online Safety Bill as drafted, will not address the enforcement issues on these services.

Virtual Private Networks (VPNs)-

The implementation of the enforcement mechanisms within the Bill relies heavily on Ofcom obtaining Court Orders to block access to services that do not conform with the legislation (Clause 124- Interim Service Restriction Orders).

Whilst blocking is currently an effective mechanism for disabling public access to problematic content, such as known Child Sexual Abuse imagery hosted extraterritorially, the Bill needs to ensure that we avoid unintended consequences such as individuals downloading VPNs to easily circumvent blocking or divert them to more extreme parts of the internet such as the dark web.

The Government should ensure services such as VPNs are within the scope of the Bill to place on them an obligation to deploy services such as the IWF's webpage blocking list and image hash list to ensure their users are protected from stumbling across CSAM in the same way they would be by an Internet Service Provider.

Enforcement measures, blocking and the role of the Internet Service Providers (ISPs)-

The IWF has highlighted over the last two years how the internet is changing and evolving and the implications this could have for traditional methods used by technology companies, in particular Internet Service Providers (ISPs), to block or disable public access to Child Sexual Abuse content or to enforce against other forms of content as may be required by Government.

DNS over HTTPs, a technical standard developed by the Internet Engineering Task Force (IETF), will essentially lead to ISPs having less control and ability to intervene in requests made by their customers for web searches as it will lead to the encryption of the Domain Name System (DNS) and prevent the ISP from accessing it. This means the ISP wouldn't be able to block users' access to websites containing CSAM as easily.

Many of the enforcement measures contained within the Online Safety Bill, such as Interim Service Restriction Orders (Clause 124), will require Ofcom to obtain a court order which could disable public access for a service that isn't complying with the regulation. ISPs will then be required to disable or block public access to that provider. **The Government must ensure that the enforcement measures contained within the legislation are future proofed and not easily circumvented.**

Ofcom's ability to levy fees and impact on third sector organisations-

The IWF urges both the Government and Ofcom to take into consideration the impact that a levy may have on companies' voluntary contributions to IWF membership, for example, when setting the threshold figure.

Part 6 of the Bill requires regulated entities to notify Ofcom that they are in scope of the legislation and provides Ofcom with the ability to charge providers of regulated services a fee (Clause 71) which will be defined by a company's "qualifying worldwide revenue" (Clause 72).