Ofcom Online Safety Team
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

22 February 2024

The Phoenix 11 appreciates the opportunity to respond to Ofcom's Illegal Harms Online Consultation. We are a group of survivors whose child sexual abuse was recorded, and in most cases, is known to be distributed online. We continue to live with the traumatic impacts of the most horrific moments of our lives having been documented by and shared through technology. We, more than anyone else, live with the weight of knowing that the child sexual abuse material (CSAM) created of us while we were raped and tortured as babies and children can be collected and consumed by child predators around the world because the internet does not have international borders.

We, as well as countless other survivors of CSAM, are in a daily battle to create safety and stability for ourselves while continuing to be revictimized by hordes of internet pedophiles. Every upload is a new abuse, every share is a new exploitation. We cannot heal as grown adults while imagery of the abuse we suffered continues to circulate the internet freely, freezing us in time as children who are retraumatized on a never-ending loop. Repeatedly we are told that it is time for tech to step up and act in the best interests of victims and survivors like us, but we have yet to see anyone enforce solutions that we need. It is us in those photos and videos that private user-to-user services are not proactively detecting. We are the ones who live with the real-life harms within the pages of this Consultation, and it is our lives that are directly impacted when tech is not properly held accountable for their lack of action in removing the crime scene documentation of our abuse from their services.

In reviewing Ofcom's Illegal Harms Online Consultation, we found three significant areas of concern that we would like to address below:

1. **Absence of proposals regarding mandatory detection of known child sexual abuse material on end-to-end encrypted services and private communications**

   <u>Detection of known CSAM</u>:
   We are concerned to find that available technology which both protects the privacy of law-abiding citizens and detects known CSAM will not be required for some of the most dangerous spaces online. It is within Ofcom's analysis that file-sharing services and social media play a key role in the spread of child sexual abuse material (CSAM) on the internet. Ofcom has gone as far as to point out functionalities that pose greater risks to child victims such as end-to-end encryption (E2EE) and provides their own example of the use of E2EE services used by perpetrators to circulate CSAM with a reduced risk of detection. We recognize that Ofcom may be constrained in some ways by the Act in regards to E2EE, however as survivors we strongly hope that all available avenues will be pursued to the fullest extent.We feel our concerns about the ways E2EE exponentially increases the risks of sexual exploitation to children and survivors must be documented here.

It is Ofcom's assessment that encrypted messaging enables CSAM to be disseminated more easily and without detection. One can even find statistics from the Internet Watch Foundation in these pages – noting a 58% drop in suspected CSAM reports from Meta between 2020 and 2021 when they stopped voluntarily scanning and predicting a similar outcome when default E2EE is fully enacted on Meta's Messenger services. The very dangers Ofcom identifies such as group and direct messaging, anonymous user profiles and URLs to CSAM are all functionalities of encrypted platforms available in the UK and around the world. Ofcom assesses encrypted platforms as high risk, acknowledging that they are a refuge for child predators. This goes directly against the Online Safety Act's framework of *"safety by design."* Without mandated detection and removal for known CSAM in all online spaces, we are simply pushing perpetrators toward the platforms that protect them. As a direct result child victims who are currently suffering horrific sexual abuse which is then distributed on the internet will continue to be abused and exploited. Abusers will continue to be anonymous and child victims will continue to be unidentified.

<u>Grooming:</u>
Encrypted services pose a direct risk to children who use them. For example, Ofcom notes that encrypted messaging makes detecting perpetrator's contact with children challenging. It is also noted that one of the ways in which grooming manifests online is by perpetrators moving conversations with children to spaces that utilize E2EE to avoid content moderation and detection. This is a huge risk factor that can have immediate and dire consequences for any child in the UK – a risk that can be mitigated with proactive detection in line with the Online Safety Act's framework which requires internet services *"to be designed and operated in such a way that a higher standard of protection is provided for children than adults."*

<u>Solutions for detection of known CSAM on E2EE platforms exist:</u>
We are aware of the argument that the technology to securely detect known CSAM and protect privacy for law-abiding citizens simply does not exist. This is not factual. Not only has the technology has existed for over a decade, but Apple showed us in August 2021 that tech can innovate their own means to detect known CSAM.[1] Apple publicly defended their technology but ultimately chose to backpedal on the use of it -- which we consider an indicator that implementation of these tools is a business decision versus lack of available solutions.

If a user-to-user service is encrypted, transparency from tech regarding protocols currently in place to protect their users from malicious software and harmful URLs should be included in Ofcom's Consultation. The technology used by companies to detect and remove known CSAM uses hashing – the very same kind of hashing technology that is already in use by encrypted services to protect their own users from harmful malware. Tech companies are already scanning their users' conversations for fraudulent website links and viruses within attachments received. This is not a matter of technological advancement but another example of tech choosing profit over the safety of children.

"When you receive a message with, for example, a URL link, and the app believes that link may be malware, it will warn you. How does it do it? It's reading your messages. There's a little piece

[1] Apple, CSAM Detection Technical Summary, https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf

of code on your device that says: this looks suspicious. So, [tech companies] are doing client-side hashing to protect you, not children, but you, and they have no problem with this. Why, by the way? Well, because if you're using WhatsApp and people send you URLs and you keep clicking them, [and] it's malware, you're going to stop using WhatsApp . . . these platforms have decided that client-side hashing to protect the user, their business, [is] fine. Client-side hashing to protect children . . . this is an outrage and a fundamental violation of privacy. I'm not buying the story and you shouldn't either."- Dr. Hany Farid, co-creator of PhotoDNA[2]

2. **Enabling tech companies to determine implementation of Ofcom proposals**
   Child sexual abuse material and child sexual exploitation should be treated as a global virus of the internet, an ongoing cyberattack to harm as many child victims as possible. The Phoenix 11 was present in March 2020 when the Five Country Ministerial announced their Voluntary Principles to Counter Online Child Exploitation and Abuse.[3] Four years later we see how when the choice is made to allow tech to decide for themselves how to tackle the epidemic of child rape and abuse imagery on their platforms, they opt not to do so.

   We appreciate the need to establish first steps when considering internet regulation. We consider the Voluntary Principles to have been those first steps, and in the four years since they were released, we have seen a massive effort by tech to sidestep standards and recommendations put forth all while the crisis of CSAM on the internet explodes into an unprecedented number of victims. Ofcom must be specific when mandating tech to prioritize child safety and cannot leave gaps that companies can use to continue to sidestep action.

3. **Consultation with survivors and civil society organizations**
   The internet has been enabled to function as a lawless and untouchable entity for far too long. This is evident by the sheer number of adult survivors, including us, whose child sexual abuse is still uploaded and traded on internet platforms; depicting hands-on abuse that, for some, ended decades ago. Given the nature of the crimes perpetrated against us, victims of CSAM have exactly one tool toward ending our ongoing abuse and exploitation via the internet: proactive hash detection and removal of known CSAM on all internet platforms, encrypted or not. Tools that tech proclaims as solutions such as parental controls for minor accounts or "Take It Down" services do not help us or the other countless victims and survivors who have been sexually abused and exploited by trusted adults and/or family members. Parental controls are not relevant if the adults who are supposed to be taking care of you are the very same adults who are abusing and exploiting you. "Take It Down" tools are not a sufficient response to the circulation of abuse imagery that we never had ownership over.

   The perpetrators who facilitate the creation and dissemination of CSAM are tech savvy, up to date on service provider protocols, and they are always aiming to be one step ahead of those trying remove this content. They have been ready for the Online Safety Act to pass, and they will try to pivot accordingly. For these reasons, Ofcom must urgently prioritize thorough consultation with survivors and civil society organizations specializing in child safety to better

[2] Dr. Hany Farid, video titled "A Conversation with Dr. Hany Farid: The fight against online child sexual abuse material (CSAM)", https://protectchildren.ca/en/resources-research/hany-farid-photodna/
[3] UK Home Office, Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, https://www.gov.uk/government/publications/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse

understand the full scope of harms to victims and survivors of child sexual abuse material, and the technology that exists to combat it.

Society and governments have too generously held the hands of tech for many years while taking tech at their word when they assert that they simply do not have the proper resources to combat these issues. If anyone has the resources and means, it is the tech companies who make billions of dollars off their users every single year — users who include multitudes of child predators. We can no longer accept tech platforms being allowed to maintain or create protected spaces for child abusers without being met by a global force of governments and regulators who demand the use of technology available at tech's fingertips and enforce laws against those who continue to prioritize profit over children. We are simply asking that Ofcom does not make the same choices that tech has made in denying us our basic rights to safety as it continues to build a path forward.