Consultation response form

Please complete this form in full and return to technologynotices@ofcom.org.uk

Consultation title	Consultation: Technology Notices
Full name	Hannah Swirsky
Contact phone number	+44 (0) 7377 449342
Representing (delete as appropriate)	Organisation
Organisation name	Internet Watch Foundation
Email address	hannah@iwf.org.uk

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how Ofcom handles your personal information and your corresponding rights, see Ofcom's General Privacy Statement.

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? Delete as appropriate.	Nothing
Your response: Please indicate how much of your response you want to keep confidential. Delete as appropriate.	None
For confidential responses, can Ofcom publish a reference to the contents of your response?	N/A

Your response

About the Internet Watch Foundation

The Internet Watch Foundation (IWF) is a charity that works in partnership with the internet industry, law enforcement and government to remove from the internet Child Sexual Abuse Material (CSAM). The IWF exists for public benefit and performs two unique functions in the UK:

1. We provide a secure and anonymous place for the public to report suspected online Child Sexual Abuse (CSA) images and videos and;

2. Use the latest technology to search the internet proactively for CSA images and videos.

The IWF has a Memorandum of Understanding between the National Police Chiefs' Council and Crown Prosecution Service that governs our operations. This ensures immunity from prosecution for our analysts and recognises our role as the "appropriate authority" for the issuing of Takedown Notices in the UK.

The IWF plays a vital role in providing the internet industry with several quality-assured technical services to prevent the spread of known CSA images and videos online and to stop the uploading of new images in the first place. These include image hashing utilising Microsoft's PhotoDNA, a URL blocking list of live webpages, keywords list, domain alerts, payment brand alerts, newsgroup alerts and simultaneous alerts (for US companies only). Key to this is our trusted relationship with the internet industry which enables us to act as a broker between them and government and law enforcement.

Our members include some of the biggest companies in the world – Amazon, Apple, Google, Meta, Microsoft, Snap, X, and Discord. We also have the largest ISPs and mobile operators in the UK (BT, Talk-Talk, Sky, Virgin Media, the Internet Service Providers Association), as well as smaller operators which are still able to access the technical services and tools we have to offer.

Overview

The Online Safety Act (the Act) is a crucial child protection measure with the potential to transform children's safety online.

Following the publication of the Illegal Harms Codes, platforms will be legally required to detect and remove known child sexual abuse imagery, such as through hash matching. The IWF stands ready to support platforms to meet this obligation.

As recognised by Ofcom[1], End-to-End Encrypted (E2EE) is a functionality which poses specific risks, particularly in relation to enabling perpetrators to spread CSAM. We were therefore pleased that Ofcom has expanded its interpretation of 'public' and 'private' in its Illegal Harms Codes to confirm that communications can be publicly shared within E2EE environments.

It is crucial that Ofcom fully leverages its powers under Section 121 of the Act to compel companies to use their best endeavours to prevent images from circulating in public E2EE environments. Ofcom must exercise this power at the earliest opportunity to address the escalating risk posed by E2EE and private messaging environments and ensure these services cannot evade responsibility.

[1] https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/volume-1-governance-and-risks-management.pdf?v=387545 pg. 7

Recommendations

- Encourage a diverse range of technologies to apply for accreditation, including through the introduction of a pre-accreditation stage for emerging technologies to encourage participation.
- Acknowledge the benefits of deploying complementary safety measures and consider issuing Technology Notices that require a provider to use multiple accredited technologies to deal with CSAM.
- Publicly recognise successfully accredited technologies, offering certifications to highlight the effectiveness of these solutions.
- Avoid communicating Ofcom's powers in a way that diminishes the threat of the Technology Notice, as a high threshold for action may discourage compliance from services.
- Broaden the interpretation of "technically feasible" to include innovative safety measures, not just measures already well-used across the industry. A risk-based regulatory approach should drive innovation and address gaps in current safety practices.
- Encourage the use of technology that can detect and block CSAM prior to an image being shared within an E2EE environment – known as client-side scanning, pre-screening or upload prevention.
- Retain Ofcom's emphasis on the right to privacy for victims of child sexual abuse, particularly in balancing this right with the protection of their personal data.
- When considering whether to issue a Technology Notice to develop or source technology, we strongly encourage Ofcom be explicit that it will consult not only with industry stakeholders but also with civil society, academics, and other experts to assess the true state of development of these technologies.
- De-prioritise the potential loss of customers in the financial cost evaluations when deciding whether it is necessary and proportionate to issue a Technology Notice.

Question	Your response
Question 1: Do you have any views on our audit-based assessment, including our proposed principles, objectives, and the scoring system? Please provide evidence to support your response	Confidential? – N 1.1. We are broadly in agreement with Ofcom's proposals for the audit-based assessment. It is important that the accreditation process is robust to avoid a scenario where Ofcom issues a Technology Notice, only for the accredited technology to be demonstrated as ineffective by the service provider. For any technology to be accredited, it must have a

Question	Your response
	high level of credibility and proven effectiveness. 1.2. We also share Ofcom's concern that an unreasonably high minimum standard could result in no technologies qualifying for accreditation, weakening Ofcom's ability to effectively exercise its Technology Notice powers. 1.3. Additionally, it is crucial to strike a balance between ensuring robustness and fostering innovation. For example, overly stringent standards could potentially exclude technologies already in use within the industry from qualifying for accreditation. We therefore urge caution in setting the accreditation standards too high, as this may discourage technology providers from applying. While it is crucial that the technologies Ofcom accredit strongly adhere to the four principles set out in the consultation, we also believe that a wide range of technologies should be eligible for accreditation. 1.4. In the best-case scenario, multiple accredited technologies should be deployed in combination to deal with illegal content most effectively.
Question 2: Do you have any views on our proposals for independent performance testing, including the two mechanisms for setting thresholds; the approach to testing technologies in categories against particular metrics; and data considerations? Please provide evidence to support your response.	N/A
Question 3: Do you have any comments on what Ofcom might consider in terms of how long technologies	Confidential? – N

Question	Your response
should be accredited for and how often technologies should be given the opportunity to apply for accreditation? Is there any further evidence we should consider?	3.1. As stated in Q1, it is important that the process of accreditation is flexible and accessible to avoid stifling innovation and encourage growth in the safety-tech sector. Considering this, we recommend striking a balance that ensures technology providers are not overburdened, which will likely dissuade services from engaging with the accreditation process. 3.2. The timeframe for accreditation must also keep pace with technological developments to ensure that the most effective technologies are accredited and avoid outdated technologies holding accredited status. 3.3. Additionally, certain circumstances may require the accreditation of specific technologies to be reviewed. For instance, if an accredited technology was being used by a service but known Child Sexual Exploitation and Abuse (CSEA) content was then identified after going undetected, Ofcom may need to consider whether the technology provider should be required to reapply for accreditation. This consideration is crucial to maintain the integrity and credibility of Ofcom's accreditation process.
Question 4: Do you have any views on how to turn these proposals into an operational accreditation scheme, including the practicalities of submitting technology for accreditation? Is there any additional evidence that you think we should consider? Please provide any information that may be relevant.	Confidential? – N 4.1. The accreditation process could present a significant hurdle for technology providers, so it is crucial to have mechanisms in place that encourage investment and foster innovation in safety technology. 4.2. For technologies that are not widely in use, it is essential to acknowledge the investment required for their testing and deployment. We suggest considering a pre-accreditation stage for emerging technologies, allowing Ofcom to

Question	Your response
	assess the technology's potential for accreditation. Given the resources, and corporate investment involved in preparing for and undergoing the accreditation process, this pre-accreditation stage could help mitigate those risks and encourage more technology services to engage with the process. It may also help to secure further investment to complete the development of new technologies. Incentivising accreditation 4.3. Given the resources required for accreditation, we recommend that Ofcom consider how it can incentivise technologies to undergo the accreditation process. In addition to PUBLIC's consideration that the process should not be overly burdensome[2], we also suggest that technologies that are successfully accredited be publicly recognised. This could involve the creation of a certification to showcase that the technology has passed the accreditation process, similar to the BSI Kitemark[3]. 4.4. Additionally, if the Technology Notice is rarely used or has an overly high threshold for implementation, it may diminish the incentive for technologies to undergo the process. In such a scenario, the risks of association may outweigh the potential benefits for technology providers. Operational challenges 4.5. We would like to acknowledge the operational challenges of the proposed accreditation process, particularly regarding the testing of technologies on Child Sexual Exploitation and Abuse (CSEA) datasets.

[2] https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-technology-notices/annexes/annex-9---ofcom-tech-accreditation-final-deliverable.pdf?v=387589

[3] https://www.bsigroup.com/en-GB/products-and-services/assessment-and-certification/kitemark/ The Kitemark is most frequently used to identify products where safety is paramount, such as crash helmets, smoke alarms and flood defences.

Question	Your response
	4.6. The IWF is committed to preventing the spread of Child Sexual Abuse Material (CSAM) and we will continue to work with Ofcom in its efforts to protect children online. We are willing to assist in testing technologies using our datasets, leveraging our expertise to provide an objective assessment of technologies accredited to detect CSAM.
Question 5: Do you have any comments on our draft Technology Notice Guidance?	Confidential? – N 5.1. All platforms have a duty to ensure they are not safe havens for criminals to target children and share Child Sexual Abuse Material (CSAM). The powers granted to Ofcom under Section 121 to issue notices regarding terrorism or Child Sexual Exploitation and Abuse (CSEA) content are essential in compelling companies to take all reasonable steps to prevent the circulation of such material, especially in end-to-end encrypted (E2EE) environments. 5.2. The Technology Notice should serve as a deterrence to ensure that technology to detect CSAM is deployed by services to maximise child safety. If it is communicated that there is an extremely high threshold for issuing a Technology Notice, this could undermine its effectiveness. If companies are not threatened by the consequence of noncompliance, it may discourage them from adopting the necessary technologies to protect children online. 5.3. Ultimately, the notice should act as a clear deterrent, compelling services to deploy technologies that detect and remove known CSAM before it is uploaded, to protect users and children online. <u>Best endeavours</u>

Question	Your response
	5.4. It is appropriate for Ofcom to challenge companies to develop technologies that align with the aims and objectives of the Act. If the legislative powers are in place, Ofcom must explore ways to utilise them to ensure that services have the means to meet their obligations. 5.5. When considering whether to issue a Technology Notice to develop or source technology, Ofcom has indicated that it will take into account the current state of development of technologies that could help identify or prevent users from encountering CSEA content. 5.6. We ask that Ofcom provides further clarity on how it plans to assess the state of development of such technologies. There is concern that services may not share details of their efforts or progress in developing technologies to prevent users from encountering CSAM. 5.7. We know technology exists that can detect and block CSAM prior to an image being shared within an E2EE environment – known as client-side scanning, pre-screening or upload prevention. It is not technically correct to suggest that such technology "breaks encryption" and we ask Ofcom to reject any assertions to the contrary. 5.8. There are several examples where large technology platforms in the scope of the Act are already using client-side scanning in technical solutions, which they claim do not break encryption or violate privacy rights. A notable example is Instagram's protections for minors, which enables teenagers to turn on a control which blurs photos of nudity[4]. This approach has also been mirrored by Apple[5] and

[4] https://about.fb.com/news/2024/01/teen-protections-age-appropriate-experiences-on-our-apps/

[5] https://support.apple.com/en-us/HT212850

Question	Your response
	Google[6]. However, we believe there is scope for further action, based on the expanded protections for child protection Apple announced in August 2021, which they stated in the FAQs had the support of both privacy and child protection organisations[7]. 5.9. WhatsApp, an E2EE service, already deploys pre-encryption technology to detect suspicious links without 'compromising E2EE'[8]. However, it does not yet use technology to prevent the upload of CSEA content. This is despite innovative solutions from companies such as Cyacomb and SafeToNet which demonstrate that effective, privacy-respecting technologies to prevent CSAM, including upload prevention, are already achievable. 5.10. We encourage Ofcom to discuss with companies as part of the supervision process, what steps are being taken to explore the potential solutions outlined by Ian Levy and Crispin Robinson, two of the world's leading cryptographers[9]. 5.11. We also recommend that Ofcom are explicit that they will consult not only with industry stakeholders, but also with civil society, academics, and other experts to assess the true state of development of these technologies. Additionally, Ofcom should use its evidence-gathering powers to investigate the developments that companies like Apple and Meta have been pursuing to prevent the upload of CSAM from E2EE environments so that they can be evaluated.

[6] https://support.google.com/families/answer/7101025?sjid=12474792458695885851-EU#zippy=%2Csupervise-your-childs-device%2Cmanage-your-childs-google-account%2Cgoogle-services-your-childs-google-account%2Chow-account-management-works

[7] https://www.apple.com/child-safety/pdf/Expanded_Protections_for_Children_Frequently_Asked_Questions.pdf

[8] https://faq.whatsapp.com/393169153028916/?cms_platform=web

[9] https://arxiv.org/abs/2207.09506

Question	Your response
	Technical feasibility 5.12. While we acknowledge that the Act states Ofcom can only direct services to remove illegal content only when it is 'technically feasible', we urge Ofcom to reframe its interpretation of technical feasibility to adopt a risk-based regulatory approach based on outcomes. 5.13. The current interpretation of 'technically feasible' means that only measures that have been tried and tested by industry can be used. As a result, this omits safety measures that regulated companies have not been willing to try and leaves a significant gap between risk and mitigation. 5.14. With this formulation, we are concerned the Act will not achieve its fundamental purpose of driving safer practice and encouraging innovation if services are only ever required to implement measures which are already well-used across industry. We urge Ofcom to reconsider its parameters of technically feasible to maximise safety for children. Any impact on other rights protected by the ECHR 5.15. While the right to privacy is fundamental, it is not absolute, and the relationship between privacy and safety is complex. Mechanisms, such as upload prevention technologies, already exist to help achieve this balance while preventing CSAM. This risk-based approach aligns with Ofcom's proposals and the intent of the Act, weighing the potential impact of any loss of privacy against the significant harm that could result from not implementing appropriate safety measures. In this context, Ofcom must prioritise addressing the severity of harm, especially when children's safety is at stake.

Question	Your response
	5.16. We welcome Ofcom's emphasis on the right to privacy for victims of child sexual abuse, particularly in balancing this right with the protection of their personal data. It is encouraging to see that Ofcom has adopted our recommendation to the draft Illegal Harms Codes and refined the language in the guidance to better highlight the rights of victims, as demonstrated in the final version of the Illegal Harm Codes. <u>The likely financial cost to the service provider of complying with the Technology Notice</u> 5.17. We recognise the need for Ofcom to factor in the financial cost to the service. However, we would like to highlight that companies will have to change the design or operation of their service to comply with the notice. 5.18. For instance, if a Technology Notice is issued to an E2EE communications provider, the associated financial impact could be significant due to potential loss of customers as users may oppose the deployment of such technology and choose to discontinue using the service. 5.19. The potential loss of customers should not be given undue weight when assessing the financial cost of complying with a Technology Notice. While it is integral that the accreditation process fosters innovation and does not unduly burden providers that could undergo the process, proportionality considerations when issuing Technology Notices must not give weight to services that profit from CSEA. The safety of a service must take precedence over the profit derived from creating a market that could enable illegal activities.

Question	Your response

Please complete this form in full and return to technologynotices@ofcom.org.uk