Your response

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	1,. **Scoring System May Not Ensure Protection of Legal rights to Free Expression, or right to privacy.** Technologies can pass with a minimum aggregated score of 60/100, which means a solution could still be accredited even if it performs poorly on some objectives.One of these objectives is Fairness. If poor Fairness results in people's private messages being wrongly censored then this could interfere with people's legal right to free expression, and right to privacy as protected by the Human Rights Act and ECHR. As such a threshold for fairness should be set to ensure people's privacy rights and free expression rights are not infringed. It is particularly important for OFCOM to consider a recent milestone judgment—Podchasov v. Russia. As the European Court of Human Rights (ECtHR) has ruled that weakening of encryption can lead to general and indiscriminate surveillance of the communications of *all* users and violates the human right to privacy. Assessment should therefore consider whether a technology weakens encryption. **2. Limited Transparency and Accountability** The document does not clarify whether assessment results will be made publicly available. As such consumers might be unknowingly exposed to products with a poor level of fairness. 3. **Difficulties with assessing real-world deployment** In the real-world threats react to the systems put in place to detect them. Yet OFCOM only scores 10% towards maintainbilty. This will present problems when flawed technologies are deployed that start infringing people's rights because their performance in real-world situations does not reflect testing.

Question	Your response
	Lack of consideration of cybersecurity risks from technologies. Technologies that exist to scan for CSAM or Terrorist content might exposure users to other cybersecurity risks. They might also inadvertently faciliate the spread of CSAM if poorly implemented. As such technologies should be scored by the extent to which they introduce new harms and risks to users. These risks include Economic costs of undermining and back-dooring E2EE. Cybercrime costs the UK economy is estimated at £37Bn pa (The Cost of Cyber Crime – A Detica report in partnership with the office of cyber Security and Information Assurance in the Cabinet Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf)including over £7Bn pa from industrial espionage. Some of these technologies have the potential to undermine the security of E2EE messaging systems that protect British industrial, social and intelligence interests. OFCOM should have a robust systems for determining the wider societal risks any new technology poses to the cybersecurity of personal messaging services. Other risks from client-side scanning technologies have been detailed in a research paper '**Bugs in their pockets': the risks of client-side scanning published in *Journal of Cybersecurity*, Volume 10, Issue 1, 2024. https://academic.oup.com/cybersecurity/article/10/1/tyad020/7590463** These include but are not limited to • Evasion attacks on machine learning • False-positive attacks • False-positive attacks on perceptual hashing • False-positive attacks via poisoning and back-dooring

Question	Your response
	The possibility of false positive attacks (distribution of innocent images that trigger alarms)have led to researchers concluding that ″current designs of perceptual hash function are completely unsuitable for large-scale client scanning,as they would result in an unacceptably high false positive rate″ https://eprint.iacr.org/2024/1869.pdf Furthermore there are risks that people might recreate CSAM images from the perceptual hashes of these images. These attacks are known as 'Perceptual Hash Inversion Attacks on Image-Based Sexual Abuse Removal Tools'. Details of research into this new type of attack were published in IEEE Security & Privacy Magazine 2024. https://arxiv.org/html/2412.06056v1 OFCOM needs to put in place robust systems to ensure that it does not approve a technology that is vulnerable to such an attack.
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.	
Question 3: Do you have any comments on what Ofcom might consider in terms of how long technologies 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?	Threats respond rapidly to changes in technology. Hostile actors are constantly looking to exploit cybersecurity vulnerabilities in any deployed technologies. As such any deployed technology should be reviewed regularly. Consideration should be given to how systems are operating in real-world environments and OFCOM should have a procedure in place for people to raise concerns about any technology deployed that might be exposing users to new cybersecurity risks or infringing on their fundamental rights.

Question	Your response
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.	Parliament has tasked OFCOM with an impossible role of requiring providers develop and deploying technology that does not, or may not ever exist to meet the desired policy goals. It is unclear whether any technology can accurately detect and preventing CSAM or Terrorist content on private messaging services without infringing people's legal rights to both privacy and freedom of expression. Several of the current technologies are very vulnerable to circumvention techniques by hostile actors. For example injecting extra data into an image to change its encrypted perceptual hash. On the other hand machine learning technologies are prone to wrongfully categorising and censoring images and high volumes of false positives. Any attempt to backdoor encryption for example with client-side scanning introduces a whole new set of cybersecurity vulnerabilities that expose users to more harms while likely pushing CSAM or Terrorist related content distribution into other channels. When trying to create an accreditation scheme OFCOM should consider wider social impact. To take a recent example Apple has recently withdrawn a data protection feature from the UK market upon receiving a request from the Home Office to backdoor their encryption on icloud phone back-ups. The wider consequences of the Home Office's actions have been to deprive people of a useful security feature. In judging proportionality OFCOM have to consider the consequences of providers simply withdrawing products from UK markets, and the wider social harms that come from a loss of privacy or freedom of expression rights.
Question 5: Do you have any comments on our draft Technology Notice Guidance?	The guidance proposes that companies have just 20 working days to respond to a technology notice. This does not seem a very large amount of time to make a detailed and often technical response.

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