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	Confidential? N N/A
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 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?	N/A
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.	Big Brother Watch believes that any technology mandated for use by Ofcom must be robustly assessed for bias, accuracy, efficacy and its impact on rights. The introduction of an accreditation scheme to ensure technologies meet the minimum standard of accuracy as set out in the OSA is welcome, provided that the accreditation scheme puts appropriate emphasis on users' rights to privacy and freedom of expression. We are deeply concerned by the potential for Ofcom to mandate the use of technologies which pose significant threats to these rights. Ofcom must never mandate the use of technologies that breach end-to-end encryption, such as client side scanning, or which use automated systems to scan and take down content before it is uploaded (upload filters).

Question	Your response
	Primary legislation and international law protect the right to freedom of expression and the right to privacy . They cannot be considered a 'tick box' consideration as part of an audit, but rather a framework through which any interference with online speech or privacy must be considered. Failure to do so risks unlawful interference with UK citizens' human rights. We recommend that
Question 5: Do you have any comments on our draft Technology Notice Guidance?	As stated, we are deeply concerned that Technology Notices will result in the use of technologies that limit UK users of online platforms' ability to communicate safely and privately and to express themselves online. When the OSA was passing through Parliament, Big Brother Watch and other human rights organisations warned that Technology Notices posed a risk to rights online and supported amendments that explicitly removed private messaging from the scope of Technology Notices. While private messaging services remain in scope for Technology Notices, Ofcom must still consider users' expectations of and rights to privacy when communicating privately. As it stands, private messaging services such as WhatsApp are end-to-end encrypted, which means that third parties (such as the social media companies who offer the service and state governments) cannot access users' direct messages to one another. We, and other civil society groups, are deeply concerned that the government will compel service providers that offer end-to-end encryption to remove or weaken the encryption they offer by introducing scanning technology onto their platforms. Such scanning technology works by comparing individuals' messages to a database of content (e.g. CSEA images) to see if there is a match either before it is sent, (when it is still on the user's phone),or after it is sent, (when it is on the platform's server, before it is received by the intended user.) These practices are broadly referred to as 'client-side scanning'. Artificial intelligence powers client side scanning – intercepting people's private messages and running algorithms over their images in search of prohibited content. Crucially, these tools would not just flag illegal content – they check every message and every image

Question	Your response
	from everyone on the system. If Ofcom were to require social media companies to scan people's private messages en masse, it would pose significant human rights implications for the more than 40 million people in the UK who use end-to-end encrypted messaging services every day. The United Nations High Commissioner for Human Rights has also voiced concerns about the drastic effect that client-side scanning might have on privacy and free expression: "*Imposing general client-side scanning would constitute a paradigm shift that raises a host of serious problems with potentially dire consequences for the enjoyment of the right to privacy and other rights. Unlike other interventions, mandating general client-side scanning would inevitably affect everyone using modern means of communication, not only people involved in crime and serious security threats.* *Given the possibility of such impacts, indiscriminate surveillance is likely to have a significant chilling effect on free expression and association, with people limiting the ways they communicate and interact with others and engaging in self-censorship.*"[1] Much of the focus of the debate on end-to-end encryption in the Online Safety Act has been on the negative effects of encrypted messaging on children, particularly in facilitating online child sexual abuse and exploitation. However, as demonstrated in a recent report by Child Rights International Network and defenddigtalme, the children's rights implications of encryption are nuanced, and there are vital ways that

1 The right to privacy in the digital age – UN High Commissioner for Human Rights, A/HRC/51/17, 4 August 2022, para 28: https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age

Question	Your response
	encryption can act to protect children's rights, including children who are marginalised and vulnerable.[2] The UN Committee on the Rights of the Child has also noted that measures designed to detect and tackle CSEA content must be "strictly limited according to the principles of legality, necessity and proportionality" and suggested that routine and indiscriminate measures may not be necessary and proportionate.[3] In August 2021, Apple proposed the introduction of client-side scanning in order to scan for images of child abuse in text messages. This move was met with opposition from over 90 civil society organisations, who criticised Apple for considering surveillance capabilities onto its devices and highlighted the potential for the technology to actually put young people at risk by eroding their rights to privacy – for example, LGBTQ+ young people or children subject to abuse on family accounts, who may no longer be able to communicate safely and securely. Experts also warned that once scanning technology is introduced to people's devices the scope of the targeted content could be easily broadened,thus enabling greater surveillance and erosions of individuals' privacy and free expression rights.[4] Eventually, Apple scrapped its proposal in response to these concerns. Well-intentioned efforts to protect people from prohibited content could open the door to wider harms, including making UK businesses and individuals less safe online, with criminals, domestic abusers, and hostile foreign states being just some of the bad actors that

2 Privacy and Protection: A children's rights approach to encryption – Child Rights International Network and Defenddigitalme, 2023: https://home.crin.org/readlistenwatch/stories/privacy-and-protection

3 General comment No. 25 (2021) on children's rights in relation to the digital environment – UN Committee on the Rights of the Child, CRC/C/GC/25, 2 March 2021, para. 75

4 International Coalition Calls on Apple to Abandon Plan to Build Surveillance Capabilities into iPhones, iPads, and other Products – Sharon Bradford Franklin and Greg Nojeim, Center for Democracy and Technology, 19 August 2021: https://cdt.org/insights/international-coalition-calls-on-apple-to-abandon-plan-to-build-surveillance-capabilities-into-iphones-ipads-and-other-products/#:~:text=An%20international%20coalition%20of%2090,iPads%20and%20other%20Apple%20products

Question	Your response
	could exploit backdoors into our private communications. Seventy civil society organisations, companies, elected officials, and cybersecurity experts including members of the Global Encryption Coalition (GEC) have also warned that eroding end-to-end encryption will make UK businesses less safe by leaving them more susceptible to cyber-attacks and intellectual property theft.[5] The GEC noted one study which found that when Australia passed a similar law undermining end-to-end encryption in 2018 the Australian digital industry lost an estimated $AUS 1 billion in current and forecast sales and further losses in foreign investment as a result of decreased trust in their products.[6] In a legal opinion commissioned by the free expression organisation Index on Censorship Matthew Ryder KC and Aidan Wills of Matrix Chambers found that mandating these general screening of users' private communications through technology such as CSS would be a disproportionate interference with the rights to privacy and freedom of expression unless the state is "confronted with a serious threat to national security which is shown to be genuine and present or foreseeable" (and other criteria are satisfied) (La Quadrature; *Ekimdzhiev v Bulgaria* (2022) 75 EHRR 8, [138] – [139], [168]).[7] The surveillance of millions of lawful users of private messaging apps has been found to require an extremely high threshold of legal justification, which content moderation purposes would be highly likely to meet. Currently, this level of mass scale, state mandated surveillance would only be possible under the Investigatory Powers Act if there is a credible threat to national security.

5 70 organizations, cyber security experts, and elected officials sign open letter expressing dangers of the UK's Online Safety Bill – Global Encryption Coalition, 24 November 2022: https://www.globalencryption.org/2022/11/70-organizations-cyber-security-experts-and-elected-officials-sign-open-letter-expressing-dangers-of-the-uks-online-safety-bill

6 New Study Finds Australia's TOLA Law Poses Long-Term Risks to Australian Economy – Internet Society, 2 June 2021: https://www.internetsociety.org/news/press-releases/2021/new-study-finds-australias-tola-law-poses-long-term-risks-to-australian-economy/

7 Surveilled and Exposed: How the Online Safety Bill Creates Insecurity – Index on Censorship, November 2022: https://indexoncensorship.org/wp-content/uploads/2022/11/Surveilled-Exposed-Index-on-Censorship-report-Nov-2022.pdf

Question	Your response
	Indeed, the European Court of Human Rights ('ECtHR') considered how measures which undermine end-to-end encryption may affect human rights for the first time in February 2024. In *Podchasov v Russia*, *a* Telegram user brought a case to the ECtHR after Russia had ordered the messaging services to disclose "technical information" including encryption keys, which would "facilitate 'the decryption of communications since 12 July 2017 in respect of Telegram users who were suspected of terrorism-related activities'." The Court concluded: "*Encryption … appears to help citizens and businesses to defend themselves against abuses of information technologies, such as hacking, identity and personal data theft, fraud and the improper disclosure of confidential information. This should be given due consideration when assessing measures which may weaken encryption.* *"The Court accepts that encryption can also be used by criminals, which may complicate criminal investigations … However, it takes note in this connection of the calls for alternative "solutions to decryption without weakening the protective mechanisms, both in legislation and through continuous technical evolution""* *"in the present case the … statutory obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued"*[8] A recent legal opinion from Phillippa Kaufmann KC and Aidan Wills on the subject of encryption notes: "In the light of this reasoning of the ECtHR, it is difficult to see how any state-mandated measures to undermine encryption on a messaging service, in circumstances where that risks weakening [end-to-end encryption] for all users, could be regarded as necessary in a democratic society for the purposes of Article 8(2) of the Convention." We concur, and urge Ofcom to ensure that safeguards are introduced to its Technology Notice regime to ensure that any technologies which

8 *Podchasov v Russia*, App No. 33696/19, [76-9]

Question	Your response
	compromise end-to-end encryption are not mandated.

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