



Consultation response form

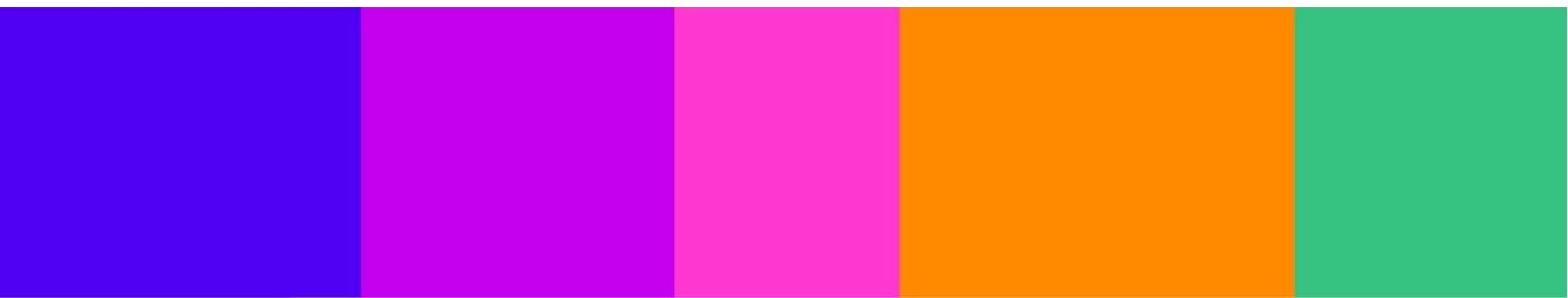
Please complete this form in full and return to ASMconsultation@ofcom.org.uk

Consultation title	Additional Safety Measures Consultation
Full name	Stephen Tulip
Contact phone number	
Representing (delete as appropriate)	Organisation
Organisation name	ACT The App Association
Email address	STulip@actonline.org

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?	Yes



Your response

Question	Your response
<p>Question 1: Do you have further evidence regarding the harms and risks to users from livestreamed illegal content or content harmful to children, or harms and risks to children from broadcasting livestreams?</p>	<p>Confidential? – Y / N</p> <p>ACT The App Association ('The App Association') appreciates the need to address harms from livestreamed illegal content; however, any enforcement approach must not undermine encryption protections that secure private communications across livestreams and other digital interactions. While Ofcom has not expressly proposed requiring backdoors or other measures to weaken encryption, we are concerned that the requirement to scan for material identified through hash matching, if applied to encrypted files or communications, could imply a requirement to break encryption in some manner. Encryption is crucial for SMEs to ensure user privacy and trust in their digital services, forming a foundation for customer retention and compliance with data protection obligations. Weakening encryption to allow intrusive monitoring would erode this trust and expose users and smaller businesses to greater risks, undermining the broader digital economy.</p>
<p>Question 2: Do you have further evidence regarding the benefits to users or children from livestreaming?</p>	<p>Confidential? – Y / N</p>
<p>Question 3: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p> <p>The App Association does not agree with proposals to the extent that they may undermine end-to-end encryption (E2EE). Encryption is fundamental to securing user data and fostering consumer trust, particularly for SMEs relying on secure communications to grow and compete globally. Weakening encryption to allow scanning of private messages risks exposing all users to increased cybersecurity threats and undermines digital trust. This erosion of privacy can deter users from interacting with services, harming small businesses that cannot afford the reputational damage or compliance complexities from diminished security. Secure encryption enables innovation while protecting fundamental privacy rights and should remain uncompromised. Evidence consistently shows that strong encryption is a cornerstone of secure online services and digital economic growth.</p>

Question	Your response
<p>Question 4: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.</p>	<p>Confidential? – Y / N</p> <p>We urge Ofcom to carefully evaluate the disproportionate impact of encryption-weakening measures on SMEs due to the complexity and expense of redesigning secure communications. SMEs depend heavily on encryption technologies to maintain consumer confidence and competitively participate in the digital economy. Proposals that could force SMEs to weaken or break encryption will increase cybersecurity risks, compliance burdens, and operational costs, potentially stifling innovation and growth if not balanced with privacy protections.</p>
<p>Question 5: Do you have any views on the optimal design of reporting functions and choice categories for users to report content that depicts the risk of imminent physical harm ? Include any evidence, such as, testing to optimise wording, design of tools to support users to submit accurate and timely reports and how these may be used to support moderation actions.</p>	<p>Confidential? – Y / N</p>
<p>Question 6: Do you consider that there are alternative measures which would materially reduce the risks to users from livestreaming such as preventive safety by design frictions, prompts or restrictions? If so, please detail them and provide evidence on the costs and efficacy.</p>	<p>Confidential? – Y / N</p> <p>We support adopting safety-by-design strategies, such as user education, friction mechanisms, and contextual content moderation, that do not compromise encryption. These alternative approaches respect the technical realities of encryption, which cannot be bypassed without creating security vulnerabilities. For SMEs, such privacy-preserving methods are feasible and cost-effective ways to enhance safety while maintaining consumer trust in secure communications.</p>
<p>Question 7: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p>

Question	Your response
<p>Question 8: If you are a service provider, what measures do you currently undertake to moderate livestreams and protect children who undertake livestream broadcasts, and what is your evidence on the effectiveness of such measures?</p>	<p>Confidential? – Y / N</p>
<p>Question 9: Do you consider that there are alternative measures which would materially reduce the risks children face when livestreaming, both in general and in relation to operation of the supporting functionalities of comments, reactions, gifting and content capture? If so, please detail them and provide evidence on the costs and efficacy.</p>	<p>Confidential? – Y / N</p> <p>We support adopting safety-by-design strategies, such as user education, friction mechanisms, and contextual content moderation, that do not compromise encryption. These alternative approaches respect the technical realities of encryption, which cannot be bypassed without creating security vulnerabilities. For SMEs, such privacy-preserving methods are feasible and cost-effective ways to enhance safety while maintaining consumer trust in secure communications.</p>
<p>Question 10: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.</p>	<p>Confidential? – Y / N</p>
<p>Question 11: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p>
<p>Question 12: Do you have any comments on the Proactive Technology Draft Guidance?</p>	<p>Confidential? – Y / N</p> <p>While proactive technologies are important for detecting illegal content, the draft guidance's encouragement of scanning encrypted content raises serious privacy concerns. For SMEs, E2EE is critical in establishing customer trust by guaranteeing confidentiality. Mandating proactive scanning methods that undermine encryption risks weakening this trust and discouraging adoption of encrypted communications. The technological reality is that scanning content in encrypted channels without weakening encryption is currently impossible. Therefore, guidance should prioritise solutions that respect encryption</p>

Question	Your response
	integrity and seek alternative approaches that do not compromise user privacy or increase operational risk for small providers.
<p>Question 13: Do you agree with the harms currently in scope of these measures? Are there any additional harms that these measures should capture? Please provide the underlying arguments and evidence that support your views, including evidence regarding the availability of accurate and effective proactive technology.</p>	<p>Confidential? – Y / N</p> <p>While the harms targeted, such as child sexual abuse material, are grave and deserve decisive action, the measures risk an unintended harm: weakening encryption that protects millions of users' personal data daily. Encryption safeguards against identity theft, fraud, and cyberattacks, all harms that disproportionately affect SMEs and their customers. The digital economy depends on preserving these protections. Any trade-off should not disproportionately sacrifice encryption's privacy and security benefits for broad surveillance or scanning mandates. The approach should include harm reduction strategies that work alongside encryption, not at its expense.</p>
<p>Question 14: Do you agree with who we propose should implement these measures? Are there any other services that should be captured for some or all of the relevant harms?</p>	<p>Confidential? – Y / N</p> <p>We urge caution in expanding mandates broadly, especially to smaller digital services that rely on encryption to compete and build consumer confidence. Imposing encryption-weakening requirements on diverse service providers could stifle innovation and disproportionately burden SMEs lacking extensive compliance resources. Enforcement should be narrowly scoped, technologically feasible, and respectful of encryption's role in securing digital interactions.</p>
<p>Question 15: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.</p>	<p>Confidential? – Y / N</p>
<p>Question 16: Do you agree with our proposal?. Please provide your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p> <p>With respect to AI tools or emerging regulations, we support a balanced regulatory approach for AI that promotes innovation while managing risk. Overly prescriptive rules risk stifling SMEs essential to the app ecosys-</p>

Question	Your response
	tem. We advocate for flexible, principles-based regulation encouraging transparency, human oversight, and robust R&D investment. Ofcom should provide clear guidelines that adapt to evolving technology without imposing disproportionate compliance costs on small developers.
<p>Question 17: Do you have any evidence relevant to the examples given?</p>	Confidential? – Y / N
<p>Question 18: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.</p>	Confidential? – Y / N
<p>Question 19: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	Confidential? – Y / N
<p>Question 20: Do you have any evidence on the relative efficacy of third-party and internal databases for image-based IIA content?</p>	Confidential? – Y / N
<p>Question 21: Do you consider this measure to be effective for file-sharing and file-storage services? Please explain your reasoning and, if possible, provide supporting evidence.</p>	Confidential? – Y / N
<p>Question 22: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.</p>	Confidential? – Y / N
<p>Question 23: Do you consider this measure to be effective for large general search services? Please explain your reasoning and, if possible, provide supporting evidence.</p>	Confidential? – Y / N

Question	Your response
<p>Question 24: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p> <p>We caution against broadly extending scanning or monitoring requirements across diverse service types, especially encrypted user-to-user platforms critical for secure communication. Such extension risks overwhelming SMEs with compliance obligations that threaten encryption integrity, harm innovation, and could inadvertently remove secure options from the market, diminishing consumer choice.</p>
<p>Question 25: Do you have evidence regarding the accuracy and effectiveness of hash matching solutions for detection of terrorism content specifically (including their false positive and false negative rates);</p>	<p>Confidential? – Y / N</p>
<p>Question 26: Do you have evidence on the extent to which a hash matching solution can identify terrorism content accurately when applied in different contexts from that in which the hash was created, noting the potential implications for freedom of expression;</p>	<p>Confidential? – Y / N</p>
<p>Question 27: Do you have a view on the degree of human oversight required to support the use of hash matching in relation to terrorism content?</p>	<p>Confidential? – Y / N</p>
<p>Question 28: Do you have evidence or views on the impact assessment (including costs) associated with implementing and maintaining hash matching technology for the detection of terrorism content (such as the impacts and costs of setting up an internal database, connecting to an external provider, and moderation costs).</p>	<p>Confidential? – Y / N</p>

Question	Your response
<p>Question 29: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p>
<p>Question 30: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.</p>	<p>Confidential? – Y / N</p>
<p>Question 31: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p> <p>We caution against broadly extending scanning or monitoring requirements across diverse service types, especially encrypted user-to-user platforms critical for secure communication. Such extension risks overwhelming SMEs with compliance obligations that threaten encryption integrity, harm innovation, and could inadvertently remove secure options from the market, diminishing consumer choice.</p>
<p>Question 32: Do you have evidence on what types of content are typically recommended to users as part of concerted foreign interference activity;</p>	<p>Confidential? – Y / N</p>
<p>Question 33: Do you have evidence on whether services track the extent of algorithmic amplification, such as impressions and reach, of content that is later deemed illegal/violating. If so, do they (or does your service) use this information to enhance the safety of their systems?</p>	<p>Confidential? – Y / N</p>
<p>Question 34: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.</p>	<p>Confidential? – Y / N</p> <p>We support pragmatic privacy and cybersecurity requirements aligned with international standards. A risk-based approach and harmonised rules reduce complexity, benefiting SMEs struggling with fragmented regulatory environments. Clear breach notification processes, practical</p>

Question	Your response
	safeguards, and collaborative governance foster trust and compliance without imposing undue costs or innovation barriers. Data protection frameworks must balance user safety with technical feasibility and innovation incentives.
<p>Question 35: Are there any impacts of the proposed measure that we have not identified? Please provide the rationale and any supporting evidence for your response.</p>	Confidential? – Y / N
<p>Question 36: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	Confidential? – Y / N
<p>Question 37: What is your assessment of the options we set out in relation to the treatment of child users and which option do you consider to be most appropriate? Please provide any supporting evidence to support your arguments.</p>	<p>Confidential? – Y / N</p> <p>While child protection is paramount, mechanisms that require intrusive scanning or weaken encryption for age verification threaten underlying privacy guarantees essential to secure digital service use by all users, including minors. The App Association advocates for privacy-respecting age assurance methods that do not undermine encryption and seek balanced, technologically viable solutions tailored to SMEs' capacities.</p>
<p>Question 38: Do you agree with our assessment of the impacts (including costs) associated with this proposal? Please provide any relevant evidence which supports your position.</p>	Confidential? – Y / N
<p>Question 39: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	Confidential? – Y / N
<p>Question 40: Do you agree with our assessment of the impacts (including costs) associated with this proposal?</p>	Confidential? – Y / N

Question	Your response
<p>please provide any relevant evidence which supports your position.</p>	
<p>Question 41: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p>
<p>Question 42: Do you agree with our proposal to introduce age assessment appeals measures into the Illegal Content User-to-user Codes (ICU D15 and D16)? Please explain your reasoning.</p>	<p>Confidential? – Y / N</p> <p>We support age assurance approaches that respect privacy and user autonomy without mandating invasive data collection or compromising security. Privacy-enhancing technologies enabling age verification without breaking encryption or collecting excessive data align with the App Association’s principle of user control. Measures should be scalable and accessible for SMEs, minimising compliance burdens while effectively protecting minors.</p>
<p>Question 43: Do you agree with our proposed amendments to codify the definition of highly effective age assurance in the Protection of Children User-to-user Code? Please explain your reasoning.</p>	<p>Confidential? – Y / N</p>
<p>Question 44: Do you agree with our proposed amendments to the Part 3 Highly Effective Age Assurance Guidance? Please explain your reasoning.</p>	<p>Confidential? – Y / N</p>
<p>Question 45: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.</p>	<p>Confidential? – Y / N</p>
<p>Question 46: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p>

Question	Your response
<p>Question 47: Do you agree with option A and option B in increasing the effectiveness of the ICU F1 and F2 measures?</p>	<p>Confidential? – Y / N</p>
<p>Question 48: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.</p>	<p>Confidential? – Y / N</p>
<p>Question 49: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p>
<p>Question 50: Do you agree with our proposed definition of ‘crisis’? Please explain your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p>
<p>Question 51: Do you consider these measures to be effective for services that are not large services? Please provide any evidence on the role of services that are not large services during crises.</p>	<p>Confidential? – Y / N</p> <p>We emphasise that policies accelerating digital infrastructure deployment are critical to SMEs’ market participation. Simplified permitting, incentivised investments, and support for affordable broadband/5G enable startups and SMEs to innovate and compete globally. Effective connectivity expands market opportunity and drives economic recovery, underscoring the need for infrastructure-focused, innovation-friendly policies adaptable to providers of all sizes.</p>
<p>Question 52: Is there any evidence of best practice in responding to a crisis that we have not identified? Please explain your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p>
<p>Question 53: Do you agree with our assessment of the impacts (including costs) associated with this proposal?</p>	<p>Confidential? – Y / N</p>

Question	Your response
<p>please provide any relevant evidence which supports your position.</p>	
<p>Question 54: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.</p>	<p>Confidential? – Y / N</p>
<p>Question 55: Do you agree with our assessment of the impacts (including costs) associated with this proposal? Please provide any relevant evidence which supports your position.</p>	<p>Confidential? – Y / N</p>
<p>Question 56: Do you think our package of proposed measures is proportionate for services in scope of the Illegal Content User-to-User Codes, taking into account the existing package of measures, the impact on reducing the risk of relevant harms and the implications on different kinds of services?</p>	<p>Confidential? – Y / N</p> <p>The current package risks disproportionately impacting smaller services and those deploying encrypted communications, which are vital for privacy, security, and trust-building. We urge a proportionate approach that balances harm reduction with preserving encryption, to avoid chilling innovation and digital competition, especially for SMEs. Proposals that implicitly pressure providers to weaken encryption undermine the very trust and safety they seek to enhance.</p>
<p>Question 57: Do you think our package of proposed measures is proportionate for services in scope of the Protection of Children User-to-User Code, taking into account the existing package of measures, the impact on reducing the risk of relevant harms and the implications on different kinds of services?</p>	<p>Confidential? – Y / N</p> <p>We call for proportionate regulation that considers the varying capabilities of services, especially SMEs, avoiding measures that impose blanket encryption weakening or unnecessary scanning burdens. Proportionality requires maintaining encryption’s privacy and security roles while targeting harms with targeted, privacy-conscious approaches to protect innovation and user trust.</p>
<p>Question 58: In relation to our equality impact assessment, do you agree that some of our proposals would have a positive impact on certain</p>	<p>Confidential? – Y / N</p>

Question	Your response
<p>groups? Please explain your reasoning and provide supporting evidence where possible.</p>	
<p>Question 59: Do you consider that our proposals could have any negative impacts on certain groups? If so, please explain your reasoning.</p>	<p>Confidential? – Y / N</p> <p>Weakening encryption disproportionately harms marginalised communities, activists, and vulnerable individuals who rely on strong encryption to communicate safely and exercise free expression. The App Association urges Ofcom to recognise these groups’ reliance on encryption and the broader societal risks from degraded privacy and security protections.</p>
<p>Question 60: In relation to our Welsh language assessment, do you agree that our proposals are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English? If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.</p>	<p>Confidential? – Y / N</p>

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