Additional Safety Measures Consultation

Annexes 1-5

Consultation

Published 30 June 2025
Closing date for responses: 20 October 2025

For more information on this publication, please visit ofcom.org.uk

A1. Equality impact assessment and Welsh Language Assessment

This annex outlines our Equality Impact Assessment (EIA) and Welsh Language Assessment for the measures proposed in the Additional Safety Measures Consultation which sets out a package of proposed safety measures under the Online Safety Act 2023 (OSA).

Consultation Questions

58. In relation to our equality impact assessment, do you agree that some of our proposals would have a positive impact on certain groups? Please explain your reasoning and provide supporting evidence where possible.

59: Do you consider that our proposals could have any negative impacts on certain groups? If so, please explain your reasoning.

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

A1.1 The purpose of this EIA is to assess the likely impact of these proposals on individuals and communities with protected characteristics, in accordance with Ofcom's legal obligations under:

a) Section 3 of the Communications Act 2003

   i) To further the interests of citizens in relation to communications matters

   ii) Secure the adequate protection of citizens from harm presented by content on regulated services

b) Section 149 of the Equality Act 2010, requiring public authorities to have due regard to the need to:

   i) Eliminate unlawful discrimination, harassment and victimisation;

   ii) Advance equality of opportunity;

   iii) Foster good relations between different groups.

c) Section 75 of the Northern Ireland Act 1998, which extends these obligations to include political opinion, marital status, and dependants.

A1.2 In preparing this consultation, we have had regard to the potential impacts of our proposals on people sharing protected characteristics (including age, sex, race, disability, religion or belief, sexual orientation, gender reassignment, pregnancy and maternity, and marriage and civil partnership, as well as dependants and political opinion in Northern Ireland). In particular, due to overlap with the protected characteristics in the Equality Act 2010 and the Northern Ireland Act 1998, we have had regard as part of our Equality Impact

Assessment to the vulnerability of those whose circumstances put them in need of special protection and the needs of persons with disabilities and of the elderly.

A1.3 The proposed measures under the Additional Safety Measures Consultation are designed to reduce the risk of illegal harms, and other harms to children, online. The measures include stronger protections against child sexual abuse and exploitation (CSEA), greater use of proactive technologies (including in relation to CSEA and intimate image abuse), and improvements to recommender systems, user safety and reporting systems. We consider these proposals will primarily have positive impacts for people with protected characteristics – and in particular women/girls and children.

A1.4 We do not consider that the proposals will have negative impacts on equality of opportunity or the fostering of good relations. We have also had regard to the different interests of persons living in urban and rural areas, but we do not consider that there is any relevant difference in these interests for the purpose of our proposals.

A1.5 We will update this assessment following the consultation period, to reflect stakeholder feedback and any changes to policy proposals. It is intended as both a decision-making tool and a transparency mechanism.

Measure-specific Equality Considerations

Highly Effective Age Assurance

A1.6 Our proposals for Highly Effective Age Assurance (HEAA) aim to determine which users are adults to better target measures aimed at protecting children, and thereby reduce opportunities for grooming. By creating a clearer boundary between adult and child users, we expect this measure to limit the opportunities for adults to exploit vulnerabilities and help service providers to proactively uphold children's safety online.

A1.7 This is particularly protective for children, especially those with disabilities or care-experienced backgrounds, where evidence shows they are at a greater risk of being targeted by offenders and may face additional barriers to or reporting abuse.

A1.8 Age assurance supports platforms in applying child-specific protections. By introducing HEAA for the purpose of measures in our Illegal Content User-to-user Codes, we expect this to have a positive impact on children, particularly those at heightened risk of harm online. This is because it ensures that our livestreaming measures and existing measures to protect children from grooming are better targeted at children.

A1.9 To the extent that HEAA may involve formal identification, we recognise potential access challenges for certain groups (e.g. care-experienced children, migrant children). In our January 2025 Guidance on Highly Effective Age Assurance, we provide examples of the different kinds of age assurance that could be considered to be highly effective. This list includes methods such as facial age estimation, which may not require users to have access to formal identification documents. We expect that providers adopt privacy-preserving methods in line with data protection laws and recommend inclusive assurance methods to ensure accessibility for users with cognitive and communication disabilities are considered.

U2U settings, functionalities and user support (including livestreaming)

A1.10 We are making various proposals regarding user-to-user settings and functionalities.

A1.11 We intend to increase the effectiveness of the safety defaults (ICU F1) and support for child users (ICU F2) measures, by proposing that providers implement the relevant measures by either:

- Option A – use highly effective age assurance to apply ICU F1 and F2 to all users that have not been determined to be an adult; or
- Option B – apply ICU F1 and F2 to all users of the service.

A1.12 ICU F1 and F2 primarily mitigate the risk of grooming harms against children. Our proposals should help ensure that the measures are more effectively targeted at child user accounts and increase the number of children that benefit from ICU F1 and F2.

A1.13 We are also proposing a measure related to livestreaming (ICU F3). We propose that users are unable to do any of the following in relation to a one-to-many livestream by a child in the UK:

a) Comment on the content of the livestream;
b) Gift to the user broadcasting the livestream;
c) React to the livestream;
d) Use the service to screen capture or record the livestream;
e) Where technically feasible, use other tools outside of the service to screen capture or record the livestream.

A1.14 We are proposing this to address a range of harms, including, but not limited to, grooming.

A1.15 We note that child abuse disproportionately affects women and girls, therefore we consider that our proposals to increase effectiveness of safety defaults and support for child user measures will provide more effective protection to them.

Crisis Response

A1.16 We are proposing measures to ensure that service providers are prepared for crises, in which illegal and harmful material can circulate rapidly. Our proposals should ensure that service providers can act promptly and effectively in reducing the spread of relevant content on their services. This may mitigate the risk of traumatisation for victims and communities affected, including racialised groups and those with mental health conditions.

A1.17 These measures are designed to mitigate risks during periods of public crisis. They are expected to benefit minority ethnic and religious groups that are often targeted during such events, but we envisage such measures will also be beneficial to persons with other protected characteristics.

Proactive Technology

A1.18 Proactive technology enables service providers to detect and act on illegal content such as child sexual abuse material (CSAM) or grooming content before it is reported. This approach shifts the burden away from victims and users, helping to prevent harm at the earliest opportunity

A1.19 Use of proactive tools for identifying illegal or harmful content is likely to benefit users at higher risk of victimisation, including those with protected characteristics. It offers specific benefits for children with disabilities and care-experienced children, who may be less likely or able to report abuse or understand that what they are experiencing is harmful. By

identifying potential abuse proactively, this technology helps close the gap in protection for those most at risk and least likely to seek help.

A1.20 We have acknowledged potential risks of bias in proactive technology. Our measure includes a number of safeguards to ensure that providers only use proactive technology where it is sufficiently accurate, effective and free from bias. For example, providers should ensure that potential biases have been identified and addressed during the design and development process; risks are appropriately managed and addressed throughout the proactive technology's lifecycle; and that systems are monitored for discriminatory outcomes.

Hash matching for Intimate Image Abuse, Terrorism Content and image-based CSAM

A1.21 Hash-matching technology helps detect and prevent the re-upload and spread of known harmful content. We have previously recommended its use to detect CSAM, and are now proposing additional measures about the use of hash-matching technology to detect:

a) Non-consensual intimate imagery, and
b) Terrorism-related material.

A1.22 To the extent that we are proposing to recommend hash matching to detect intimate image abuse, given that this is predominantly perpetrated against women, we expect this measure to provide additional protection for them.

A1.23 We are also proposing to recommend hash matching to detect terrorism content. Characteristics including race and ethnicity, religion, age and gender could lead to an increased risk of harm to individuals from terrorism content as set out in paragraphs 1.37 to 1.42 of the Illegal Harm Register of Risks. We therefore expect our measure to have a positive impact on individuals with these characteristics.

A1.24 There is a risk of hash databases disproportionately focusing on Islamist terrorist groups and material, notwithstanding the wider range of terrorist ideologies. As a consequence, incorrect identification of content as terrorism content may disproportionately affect Muslims if content of a religious or political nature is conflated with that related to terrorism. As part of our proposal, we are recommending that arrangements are in place to ensure that the set of hashes used does not plainly discriminate on the basis of protected characteristics.[1] This guards against potential risks relating to bias.

A1.25 We are also proposing to expand the application of our existing measure recommending hash matching to detect imaged based CSAM. We are proposing to expand this to providers of user-to-user services which are at high risk of image-based CSAM where the principal purpose of the services is the hosting or dissemination of regulated pornographic content. Given that CSAM disproportionately affects women, our proposal will also provide additional protection for them.

Recommender Systems

[1] We explain this risk, and the safeguards in place to mitigate risks of the incorrect detection of content as terrorism content, Chapter 12, Perceptual Hash Matching for Terrorism Content.

A1.26 We propose that where there are indicators that content is potentially illegal – including hate, terrorism, suicide, and foreign interference – is withheld from recommendation feeds unless and until reviewed.

A1.27 This may reduce the virality of content targeting protected groups (e.g. illegal hate speech or terrorism). Characteristics including race and ethnicity, religion, age and gender could lead to an increased risk of harm to individuals from terrorism content. We therefore expect our measure to have a positive impact on individuals with these characteristics.

A1.28 By limiting the amplification of illegal content, this measure helps reduce the speed and scale at which such material can spread – creating a safer and more equitable online environment, especially for those at greater risk.

User Sanctions and CSEA Banning

A1.29 We propose that service providers should be required to ban users who share child sexual abuse material (CSAM) and apply strong, proportionate sanctions against those engaging in other serious illegal behaviours.

User sanctions

A1.30 Proposals relating to imposing sanctions on users who share illegal or harmful content are expected to protect vulnerable groups (e.g., children, survivors of sexual abuse, marginalised communities).

A1.31 By recommending decisive action against known offenders, this measure helps build trust in online safety protections, reinforces accountability, and offers greater assurance to at-risk groups that harmful behaviour will not be tolerated.

A1.32 Enforcement should be proportionate and account for context (e.g. self-generated content shared under coercion). We recommend clear appeal processes and safeguards for misidentification.

A1.33 There is a risk that sanctions may have a particular impact on vulnerable users suffering from suicide ideation, self-harm or an eating disorder, who may be sanctioned for sharing their personal experience (or not share their experience because they are worried about being sanctioned). We propose that, when setting their sanctions policies, providers should have regard to the potential impact of the sanction on the user who is being sanctioned. This may include considering the potential vulnerability of the user.

CSEA Banning

A1.34 We propose that service providers ban users who share, generate or upload CSEA content, and those who receive CSAM. Though viewing CSAM is harmful to users of any age, grooming can only be carried out against children. As such, we expect this measure would have particularly positive impacts for children by protecting them from the harm caused by grooming.

A1.35 That said, we recognise that children may also be disproportionately negatively impacted by this measure if they are banned for sharing self-generated indecent imagery (SGII) because of being groomed. Such children would fall into the category of people who are in need of special protection, to a greater extent than the special protection that children already need by virtue of their age. While producing and sharing SGII is illegal under UK law, banning a child who has been groomed could be perceived as victim blaming and exacerbate the harm already experienced by the child. We have therefore presented an option to allow providers discretion not to ban a child where this exceptional circumstance

applies, which we expect would mitigate the disproportionately negative impact on children in this scenario and recognise their need for special protection. We have also presented the option of permitting providers discretion not to ban children who share SGII consensually as part of an age-appropriate relationship for similar reasons.

A1.36 Though we are proposing that a ban under this measure should in almost all cases be permanent, we recognise that there may be rare circumstances where a permanent ban would not be appropriate. We are therefore proposing that providers have discretion to apply a shorter ban in such circumstances. We expect this discretion could be exercised where a child has shared, generated or uploaded CSEA content, or received CSAM, in the circumstances described at paragraph 2.30, or in recognition of the potentially lower level of culpability of a child when carrying out CSEA harm. We also expect it could be exercised where a disabled person has carried out CSEA but similarly has a lower level of culpability due to their disability. In these circumstances, our view is that the proposed discretion around the duration of the ban could be exercised to mitigate any disproportionate impact the measure may have on these groups of users.

Cross-cutting Considerations

A1.37 Across the consultation, our proposals are underpinned by a commitment to protecting those at greatest risk of harm online, including children, disabled people, those with care experience, and people facing intersecting forms of disadvantage (e.g. race, gender, and sexual orientation).

A1.38 Our proposals support equality in a variety of ways by:

- Embedding safety-by-design to proactively reduce exposure to harmful content at the earliest opportunity.
- Ensuring consistent protections across services, especially for less digitally confident users.
- Increasing trust and participation for groups often excluded or targeted online.
- Sending a clear signal that harmful behaviour won't be tolerated, through stronger enforcement.
- Using automated tools to provide faster, more consistent safeguards for vulnerable users.

A1.39 We expect the greatest positive impacts to be felt by:

- Children;
- Women and girls affected by abuse and CSEA;
- Minority ethnic and religious communities targeted by hate or extremist content;
- LGBTQ plus users;
- Users with disabilities or lower digital literacy.

A1.40 These groups are disproportionately affected by online harms, as evidenced in Ofcom's Risk Profiles and stakeholder engagement.

A1.41 Overall, we consider that the proposals in the ASM consultation will not result in unlawful discrimination or otherwise hinder equality of opportunity. Where we have identified a risk of discrimination (e.g. bias in the operation of hash matching technology or other proactive

technology) we have built-in safeguards to mitigate this risk. Our package of measures will seek to provide and more inclusive online protections.

Conclusion and Next Steps

A1.42 The Equality Impact Assessment has considered how our proposed additional safety measures may affect people with protected characteristics, particularly children, disabled users, and users from disadvantaged or marginalised backgrounds.

A1.43 We consider the measures proposed in the Additional Safety Measures consultation are likely to deliver positive equality outcomes for users with protected characteristics. Where potential negative impacts have been identified, we have sought to mitigate them.

A1.44 We are inviting views from stakeholders, including those representing or working with groups who may be impacted. Where appropriate, we will adjust our proposals or implementation guidance to mitigate any identified risks.

A1.45 We will continue to refine our impact assessment considering consultation feedback including engagement with organisations representing affected groups. Any final decisions will be accompanied by an updated final Equality Impact Assessment.

Welsh Language Assessment

A1.46 The Welsh language has official status in Wales. To give effect to this, certain public bodies, including Ofcom, are required to comply with the Welsh Language Standards. [2] Accordingly, we have considered:

- The potential impact of our policy proposals on opportunities for persons to use the Welsh language;
- The potential impact of our policy proposals on treating the Welsh language no less favourably than the English language; and
- How our proposals could be formulated so as to have, or increase, a positive impact, or not to have adverse effects or to decrease any adverse effects.

A1.47 Ofcom's powers and duties in relation to online safety regulation are set out in the Online Safety Act 2023 and must be exercised in accordance with our general duties under section 3 of the Communications Act 2003. In formulating our proposals in this consultation, where relevant and to the extent we have discretion to do so in the exercise of our functions, we have considered the potential impacts on opportunities to the Welsh language and treating the Welsh language no less favourably than English.

A1.48 We recommended in our December 2024 Illegal Harms and our April 2025 Protection of Children Statements, that service providers should have regard to the needs of their UK user base in considering what languages are needed to effectively resource their content moderation, complaints handling, terms of service and publicly available statements.[3] To the extent that we are proposing to make any changes in these areas, they are not likely to

[2] The Welsh language standards with which Ofcom is required to comply are available on our website here [Date accessed 16.6.25].

[3] Relevant measures are contained within our Codes of Practice which can be accessed via our December 2024 Statement and our April 2025 Statement [Date accessed 16.6.25]

negatively impact on the Welsh language. For example, we are proposing to broaden our appeals measures by recommending that providers consider appeals based on 'proxy' content. In connection with appeals (and all complaints), all users should be able to submit appeals and the functionality to enable this should be easy to find an accessible, having regard to the service's user base. As such, we consider our proposals are likely to continue the overall positive effects of our recommendations in our December 2024 and April 2025 Statements, on opportunities to use the Welsh language and treating the Welsh language no less favourably than English.

A2. Responding to this consultation

How to respond

A2.1 Ofcom would like to receive views and comments on the issues raised in this document, by 5pm on 20 October 2025.

A2.2 You can download a response form from here. You can return this by email or post to the address provided in the response form.

A2.3 If your response is a large file, or has supporting charts, tables or other data, please email it to ASMconsultation@ofcom.org.uk, as an attachment in Microsoft Word format, together with the cover sheet. This email address is for this consultation only and will not be valid after 20 October 2025.

A2.4 Responses may alternatively be posted to the address below, marked with the title of the consultation:

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

A2.5 We welcome responses in formats other than print, for example an audio recording or a British Sign Language video. To respond in BSL:

- send us a recording of you signing your response. This should be no longer than 5 minutes. Suitable file formats are DVDs, wmv or QuickTime files; or
- upload a video of you signing your response directly to YouTube (or another hosting site) and send us the link.

A2.6 We will publish a transcript of any audio or video responses we receive (unless your response is confidential)

A2.7 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt of a response submitted to us by email.

A2.8 You do not have to answer all the questions in the consultation if you do not have a view; a short response on just one point is fine. We also welcome joint responses.

A2.9 It would be helpful if your response could include direct answers to the questions asked in the consultation document. The questions are listed at Annex X. It would also help if you could explain why you hold your views, and what you think the effect of Ofcom's proposals would be.

A2.10 If you want to discuss the issues and questions raised in this consultation, please contact Sinead.Lee@ofcom.org.uk.

Confidentiality

A2.11 Consultations are more effective if we publish the responses before the consultation period closes. This can help people and organisations with limited resources or familiarity with the issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish responses on the Ofcom website at regular intervals during and after the consultation period.

A2.12 If you think your response should be kept confidential, please specify which part(s) this applies to and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.

A2.13 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it. But sometimes we will need to publish all responses, including those that are marked as confidential, in order to meet legal obligations.

A2.14 To fulfil our pre-disclosure duty, we may share a copy of your response with the relevant government department before we publish it on our website.

A2.15 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further in our Terms of Use.

Next steps

A2.16 Following this consultation period, Ofcom plans to publish a statement in XXXX 20xx.

A2.17 If you wish, you can register to receive mail updates alerting you to new Ofcom publications.

Ofcom's consultation processes

A2.18 Ofcom aims to make responding to a consultation as easy as possible. For more information, please see our consultation principles in Annex x.

A2.19 If you have any comments or suggestions on how we manage our consultations, please email us at consult@ofcom.org.uk. We particularly welcome ideas on how Ofcom could more effectively seek the views of groups or individuals, such as small businesses and residential consumers, who are less likely to give their opinions through a formal consultation.

A2.20 If you would like to discuss these issues, or Ofcom's consultation processes more generally, please contact the corporation secretary:

Corporation Secretary
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA
Email: corporationsecretary@ofcom.org.uk

A3. Ofcom's consultation principles

Ofcom has seven principles that it follows for every public written consultation:

Before the consultation

1. Wherever possible, we will hold informal talks with people and organisations before announcing a big consultation, to find out whether we are thinking along the right lines. If we do not have enough time to do this, we will hold an open meeting to explain our proposals, shortly after announcing the consultation.

During the consultation

2. We will be clear about whom we are consulting, why, on what questions and for how long.
3. We will make the consultation document as short and simple as possible, with an overview of no more than two pages. We will try to make it as easy as possible for people to give us a written response.
4. When setting the length of the consultation period, we will consider the nature of our proposals and their potential impact. We will always make clear the closing date for responses.
5. A person within Ofcom will be in charge of making sure we follow our own guidelines and aim to reach the largest possible number of people and organisations who may be interested in the outcome of our decisions. Ofcom's Consultation Champion is the main person to contact if you have views on the way we run our consultations.
6. If we are not able to follow any of these principles, we will explain why.

After the consultation

7. We think it is important that everyone who is interested in an issue can see other people's views, so we usually publish the responses on our website at regular intervals during and after the consultation period. After the consultation we will make our decisions and publish a statement explaining what we are going to do, and why, showing how respondents' views helped to shape these decisions.

A4. Consultation coversheet

Basic details

Consultation title:

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

Confidentiality

Please tick below what part of your response you consider is confidential, giving your reasons why

- Nothing ☐
- Name/contact details/job title ☐
- Whole response ☐
- Organisation ☐
- Part of the response ☐

If you selected 'Part of the response', please specify which parts:

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

Yes ☐ No ☐

Declaration

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom aims to publish responses at regular intervals during and after the consultation period. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name Signed (if hard copy)

A5. Consultation questions

Please tell us how you came across about this consultation.

- ☐ Email from Ofcom
- ☐ Saw it on social media
- ☐ Found it on Ofcom's website
- ☐ Found it on another website
- ☐ Heard about it on TV or radio
- ☐ Read about it in a newspaper or magazine
- ☐ Heard about it at an event
- ☐ Somebody told me or shared it with me
- ☐ Other (please specify)

Livestreaming - Introduction

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?

Question 2:

Do you have further evidence regarding the benefits to users or children from livestreaming?

Livestreaming – our proposals to protect all users

Question 3:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

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.

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.

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.

Livestreaming – our proposals to protect children

Question 7:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

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?

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.

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.

Proactive Technology

Question 11:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

Question 12:

Do you have any comments on the Proactive Technology Draft Guidance?

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.

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?

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.

Amendment to ICJG for CSAM

Question 16:

Do you agree with our proposal?. Please provide your reasoning, and if possible, provide supporting evidence.

Question 17:

Do you have any evidence relevant to the examples given?

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.

Perceptual Hash Matching for IIA

Question 19:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

Question 20:

Do you have any evidence on the relative efficacy of third-party and internal databases for image-based IIA content?

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.

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.

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.

Perceptual Hash Matching for Terror Content

Question 24:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

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);

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;

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?

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).

Proposal to Extend Perceptual Hash Matching for CSAM

Question 29:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

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.

Recommender Systems

Question 31:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

Question 32:

Do you have evidence on what types of content are typically recommended to users as part of concerted foreign interference activity;

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?

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.

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.

User Banning and Preventing Return Following Detection of CSEA Content

Question 36:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

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.

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.

User Sanctions Policy

Question 39:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

Question 40:

Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.

Highly Effective Age Assurance in the Illegal Content User-to-user Codes

Question 41:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

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.

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.

Question 44:

Do you agree with our proposed amendments to the Part 3 Highly Effective Age Assurance Guidance? Please explain your reasoning.

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.

Increasing Effectiveness for U2U Settings, Functionalities, and User Support

Question 46:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

Question 47:

Do you agree with option A and option B in increasing the effectiveness of the ICU F1 and F2 measures?

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.

Crisis Response

Question 49:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

Question 50:

Do you agree with our proposed definition of 'crisis'? Please explain your reasoning, and if possible, provide supporting evidence.

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.

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.

Question 53:

Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.

Broadening Appeals

Question 54:

Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

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.

Combined Impact Assessment

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?

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?

Equality Impact Assessment

Question 58:

In relation to our equality impact assessment, do you agree that some of our proposals would have a positive impact on certain groups? Please explain your reasoning and provide supporting evidence where possible.

Question 59:

Do you consider that our proposals could have any negative impacts on certain groups? If so, please explain your reasoning.

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.