Your response

Ofcom's Register of Risks

Question 1:	
i)	Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?

TechUK has spoken to this previously in our response to the Illegal Harms Consultation [link].

While understanding the need for effective moderation, we emphasize the challenges associated with real-time content moderation for some services. Striking a balance between mitigating online harms and preserving user freedom is crucial. A collaborative approach with the industry can help find practical and effective solutions that do not unduly burden platforms. Having less prescriptive content moderation practices will allow platforms to implement solutions that are more effective in addressing illegal content while accounting for their level of risk, business model and nature of their content.

Evidence Base

The evidence referenced in Vol. 2 of the Illegal Harms Consultation forms the basis of Ofcom's register of risks, which companies are expected to have reference to when carrying out their own risk assessments. We therefore agree with Ofcom that it is important to take steps to ensure that evidence sources for these risks are robust and reliable.

As part of the consultation, Ofcom have asked services whether they have comments on Ofcom's assessment of the causes and impacts of online harms. We have noted instances where Ofcom have relied on evidence which has previously been questioned by peers. It would therefore be helpful to understand Ofcom's approach to selecting evidence sources, and the steps that have been taken to ensure that these are robust and reliable.

TechUK advocates for any evidence base or research Ofcom seeks to rely upon to be in line with Ofcom's own rules for research, and have a published methodology and peer review.

Some of the research cited in Volume 2 has cited evidence that is either out of date and no longer reflective of the market or harms, is inaccurate or has a poor methodology or lacks the relevant evidence altogether, in relation to the measures proposed.

ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

Some providers may not be clear as to whether their services are in scope and the analysis omits to explain how providers will acquire certainty in this regard. TechUK recommends that Ofcom creates further time and safe space to complete this step before finalising codes, carrying out additional targeted consultation where needed.

TechUK rejects the proposal that Ofcom publicly 'name and shame[1]" providers as a lever to secure compliance. While techUK members expect Ofcom to publish formal enforcement decisions, they also expect the day-to-day operation of the online safety framework and Ofcom's conduct to match the aspirations previously set out. techUK asks that Ofcom establish a clear and predictable hierarchy of interventions from the outset, consistently starting with direct engagement with a provider and driving towards workable compliance that addresses identified risks.

In addition, Ofcom should adopt a 'no surprises' approach to research by publishing its programme and providing reasonable opportunities for relevant providers to comment before research is commissioned. This will give effect to the collaborative approach Ofcom has presented, avoid Ofcom resources being wasted on flawed or misleading research and build trust between Ofcom and regulated companies.

More generally, TechUK suggests a continuous dialogue between regulators and the tech industry to address emerging challenges promptly. Collaboration and shared insights, even with similar international regimes, can enhance the effectiveness of the proposed measures

Finally, it is important to highlight the benefits of encryption to public safety and security. TechUK welcomes Ofcom's acknowledgment that encryption plays a vital role in keeping communications safe and secure. We urge Ofcom to make a stronger and more explicit statement in this section, especially considering their recognition of encryption as a 'particular risk' when used on services. Highlighting the benefits of encryption is essential for maintaining a balance between privacy and security concerns, and it is imperative that Ofcom's position reflects the positive contributions encryption makes to public safety.

[1] *"....using our research and our transparency reporting powers to shine a light on what services are doing to tackle online harms and generating reputational incentives for them to make improvements", p6*

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 2:	
i)	Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.
TechUK encourages a nuanced understanding of risk factors, considering the diversity of tech services. The risk assessment framework should be flexible to accommodate various business models and service types. End to end encryption for example, is described as 'high risk'. However, E2EE needs to be considered with all the benefits it brings in reducing other illegal and harmful online harms in mind. Similarly, for artistic content, a more nuanced approach is needed to balance the protection of users with the preservation of artistic freedom and freedom of expression Further, when making an assessment on harm, it is vital that the risk and type of harm is factored in and mitigation measures that would reduce risk are effectively considered. The scale and focus of services' prioritisation and mitigation measures should be taken into account. Additionally, Ofcom should reserve the most significant obligations for services with the highest risk of harm. We are concerned current draft proposals could lose sight of the OSA's emphasis on risk and proportionality, and instead adopt an approach which has an undue focus on size.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Service's risk assessment

Question 3:	
i)	Do you have any comments on our approach to amending the draft Risk Profiles or our proposed risk factors for animal cruelty?
Response: N/a	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/a	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/a	

Question 4:	
i)	Are the draft Risk Profiles for illegal content sufficiently clear in presenting the relationships between the risk factors and the risk of harm posed by animal cruelty content?
Response: N/a	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/a	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/a	

Question 5:	
i)	Do the draft Risk Profiles for illegal content include the risk factors that are most strongly linked to the risk of harm posed by animal cruelty content?
Response: N/a	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/a	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/a	

The Illegal Content Judgements Guidance (ICJG)

Question 6:	
i)	Do you agree with our proposals? Please provide the underlying arguments and evidence that inform your view.
Response: N/a	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/a	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/a	

Question 7:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for providers with limited access to legal expertise?
Response: N/a	

ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/a	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/a	

Question 8:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response: N/a	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: N/a	