techUK

techUK Submission to Ofcom's Call for Evidence: Second Phase of Online Safety Regulation

techUK is submitting a written response to Ofcom's call for evidence on the second phase of online safety regulation. techUK is the trade body for digital tech in the UK, representing over 900 members, many of which are SMEs. techUK's membership is made up of a range of companies which include some of the services and platforms which will be within scope of the Online Safety Bill and required to protect children from harmful content, as well as member companies who offer a range of age assurance and age verification technologies and services. While not responding to each question individually, techUK's response follows the key topics and structure of the call for evidence.

techUK welcomes Ofcom's work as the regulator within this space following the Online Safety Bill. There is significant ongoing work within the sector to improve child safety. It is important that legislative and regulatory activity in this space allows for flexibility in the tools and approaches used by the broad variety of services as well as future services. We believe that nuance is also an important principle that should be considered to ensure that any solutions applied to services are appropriate for their different needs and uses.

Children's Access to Services

- There are a number of mechanisms and services which some techUK members offer to identify children in different age groups. Some techUK member platforms have already implemented age assurance technologies, requiring users to either upload an identity document or provide a video to prove their age. Other members have age-gated portions of their service that are not suitable for children through asking users to prove they are an adult, although there is still a child-safe part of their service that is appropriate to be access and used by children. Alternatively, age-gating for 18+ experiences through credit reference agency checks or alternative measures is easier for some services to implement than the measures that can show whether a user is a child.

- Although some members have already implemented age assurance and verification technologies on platforms which help to verify identity including age and address, the costs associated with implementing such measures can be significant and limits their accessibility for some SME businesses wishing to utilise them.
- As techUK has previously highlighted, identity verification methods are not a 'one size fits all' approach and therefore there needs to be a level of nuance applied to different services that implement different measures that are suited to their platform. Further, while it is important to maintain flexibility in the range of appropriate measures, ensuring children's privacy should consistently be taken into account.

- There has been an increased focus on potentially bringing the Online Safety Bill in line with the Age Appropriate Design Code, in making a services risk assessment reliant on whether it is "likely to be accessed by a child". There are concerns from across industry that this definition is ambiguous and will bring services not designed for, or targeted towards, children into scope as it is extremely difficult to prove a child cannot and never will be able to access the service.

- We are particularly keen to understand how Ofcom will ask for services to prove that children are not able to access their service, or the proportion of users that are children, thus impacting the risk that a service may pose to child safety. Similarly, we are keen to understand the principles

Ofcom will be using to assess methods such as age assurance and age verification that are used by services as part of services risk assessments.

Risk Assessment and Management

- There is a significant difference in terms of risk and user experience across different platforms. The likelihood of a service being accessed by a child differs greatly across different services, as well as the risk of harm. More broadly, there will be a great variety of user experiences on the same platform. It is important these nuances are considered by Ofcom as they draft risk assessment guidance and throughout the ongoing process.

- Members are also keen that services that are not designed for children, are low risk due to their functionalities, or effectively already protect children from accessing harmful content, should be able to demonstrate this through their risk assessments.

- Overall, guidance from Ofcom should acknowledge work being done by platforms to protect children and allow for this to be reflected in guidance and risk assessments.

Terms of Service and Policy Statements

- It is not in the best interest of services to allow for harms to widely exist or proliferate on their platforms. Responsible services in scope of the Bill already feature provisions to prevent or limit online harms.

- In terms of commercial interests, many services rely on advertising or investment from other organisations, who would not continue to invest in them should they be associated with proliferating online harms.

Design and operation of the service, including functionalities and algorithms

- When considering future-proofing such detection technologies, there needs to be consideration for how malicious actors are able to evade detection on platforms, using sophisticated methods to continue targeting children even once they have been flagged as being a concern for a service. This will become even more challenging considering the future proliferation of AI generated imagery and text communications.

- The way in which content spreads varies greatly between platforms. Consequently, there are a range of different solutions which could mitigate risk. Ofcom guidance on this issue must take a nuanced approach.

- Some members already have in place content warnings based on algorithms that flag when a particularly harmful piece of content has been searched for, including those which breach a platform's terms of service. This can prove beneficial in making users aware of the harmful content they are about to engage with and can limit their exposure to such content.

Moderation

- Human moderators are currently used by some members to review content flagged by detection systems, including user reporting. When it comes to improvements in system detection and moderation to reduce the level of human moderation needed, more accurate detection for images and contextual messages may help. For some SMEs however, resources or capacity to develop and maintain this technology internally may be limited.