Making the internet safe for children: Ofcom's latest consultation

On 8 May 2024, Ofcom launched its second major consultation as regulator under the Online Safety Act 2023 (2023 Act) (the consultation). Titled "Protecting children from harms online", the consultation sets out Ofcom's proposals for how organisations providing online services should comply with their wide-ranging duties under the 2023 Act to assess and mitigate the risk of harm to users under the age of 18 in the UK.

Ofcom has a vital role in bringing the 2023 Act into force (*see feature article "Online Safety Act 2023: a revolution in regulation", www.practicallaw.com/w-041-4411*). Once it publishes its guidance and codes of practice in their final forms, the duties in the 2023 Act will come into force and organisations within scope will need to take steps to comply. Ofcom estimates that more than 100,000 online services, ranging from micro businesses to very large online platforms, will fall within the scope of these obligations and that most of these services will be required to take specific steps to safeguard children online.

A focus on children's access

Ofcom's first major consultation under the 2023 Act focused on the duties set out in the legislation that require organisations providing online services to take steps to to protect all UK users, including children, from illegal content (*www.ofcom.org.uk/consultations-and-statements/category-1/protecting-people-from-illegal-content-online*). In the second consultation, Ofcom focuses on the duties that the 2023 Act will impose on organisations to identify whether their service is likely to be accessed by children, assess what types of harmful, but not necessarily illegal, content are available to those children, and implement measures to mitigate and manage the risk of that harmful content being available to children.

Children's access assessments

All organisations within scope of the 2023 Act will be required to consider whether their service is "likely to be accessed by children" by completing a children's access assessment (CAA). There are two key steps in this process:

- Identify whether it is possible for child users to access the service. Organisations can only conclude that their service is not accessible to children if they implement highly effective age assurance, effectively age-gating their service to all users under the age of 18. The consultation provides guidance on the forms of age assurance that Ofcom considers capable of being "highly effective" (*see box "Highly effective age assurance"*). The 2023 Act provides that organisations cannot rely on self-declared information, such as a user providing their date of birth, for this purpose.

Highly effective age assurance

Examples of potentially highly effective methods of age assurance include:

- Open banking.
- Photo-ID matching.
- Facial age estimation.
- Mobile network operator age checks.
- Credit cards checks.
- Reusable digital identity services.

Examples of age assurance methods that are not considered to be highly effective include:

- Self-declaration.
- Payment methods that do not require a minimum age; such as debit, Solo or Electron cards.
- General contractual restrictions on the use of the service by children.

- Assess whether their service is currently used by a significant number of child users under the age of 18 or is likely to attract such users. In the consultation, Ofcom does not seek to define what amounts to a "significant" number of users by reference to any particular figure but states that the term means "a number or proportion that is material in the context of [a] service". Organisations will need to consider the context of their service and the information available to them when carrying out this assessment. An organisation can, alternatively or additionally, consider whether its service is "likely to attract" child users by reference to factors including whether the service benefits children or is appealing to children, whether children form part of the business model, or whether there is evidence from internal or external sources that children are users.

Ofcom expects most services to conclude that they are likely to be accessed by children. In all cases, the outcome of the CAA should be recorded and organisations that conclude that their service is not likely to be accessed by children should be prepared to justify their findings. All services, including those that conclude they are not likely to be accessed by children, should repeat the CAA at least annually or in the case of a trigger event, such as before making a significant change to the design of their services. Organisations that do not conduct a CAA will automatically be considered "likely to be accessed by children" under the 2023 Act.

Children's risk assessment

Organisations whose services are likely to be accessed by children must assess the risk of those children encountering each type of regulated content that is identified in the 2023 Act (*see box "Content harmful to children"*). Ofcom outlines the following four-stage process for conducting a children's risk assessment (CRA):

- Understand the kinds of content harmful to children. Organisations need to identify the types of harmful content that may be available on their service. They must also consult Ofcom's children's risk profiles, which identify specific risks that can arise based on certain features and functionalities of a service; for example, risks that can arise specifically for messaging services.

- Assess the risks of harm. The likelihood and impact of children encountering harmful content should be assessed, with a risk rating assigned to each category. This assessment should take into account the design and functionalities of a service and how these may amplify any harm. The assessment should consider the risk of harm by reference to specific age groups.

- Decide measures, implement and record. Any measures implemented to address existing risks should be reviewed and additional measures should be implemented where a risk to children has been identified. Ofcom's children's safety codes provide guidance to assist with this (*see "Safety measures to protect children online" below*).

- Report, review, and update assessments. The assessment outcome should be reported within an organisation in line with its governance structures. The effectiveness of controls and measures to reduce risk should be monitored on an ongoing basis and the CRA should be kept up to date, particularly in light of any changes to the design or operation of a service.

Content harmful to children

There are three broad categories of "content that is harmful to children" under the Online Safety Act 2023, and organisations must assess each type, including individual subtypes, when completing the children's risk assessment:

- "Primary priority content that is harmful to children" covers content that is considered the most harmful, including pornographic content and content that encourages, promotes, or provides instructions for suicide, self-harm and eating disorders.

- "Priority content that is harmful to children" includes content that is abusive or incites hatred, bullying content, and content that encourages, promotes or provides instructions for violence, dangerous stunts or challenges, and self-administering harmful substances.

- Non-designated content that presents a material risk of harm to children is any content that does not fall within the first two categories but presents a "material risk of significant harm to an appreciable number of children."

Safety measures to protect children online

Ofcom's children's safety codes set out the measures that it proposes organisations take to mitigate the risk of harm to children. These most significant measures include:

Age assurance. Ofcom expects to see much greater use of age assurance in the future, so that organisations know when children use their platform.

Safer algorithms. Organisations that are at a high risk of hosting harmful content will be expected to know who their child users are and configure algorithms to filter out the most harmful content.

Effective moderation. All organisations will be expected to implement effective content moderation systems, which can rely either on automated technologies or human intervention. Where content that is harmful to children is flagged, swift action will be expected.

Governance and accountability. Ofcom proposes that organisations appoint a person responsible for compliance with children's safety duties and that risk management activities be reviewed annually by a senior body at the organisation. An employee code of conduct should also be adopted, setting standards for employees around protecting children.

More choice and support for children. Children should be provided with clear and accessible information about the operation of the service and the safety measures that are in place to protect them, such as a complaints process.

Next steps

The consultation has been published in line with Ofcom's ambitious regulatory roadmap. The codes of practice and guidance are forecast to be finalised by spring 2025 and organisations will then have three months to complete their first CAA; that is, by summer 2025. The other relevant duties will likely apply immediately after.

Cédric Burton is a partner, Tom Evans is Of Counsel, and Hattie Watson is a trainee solicitor, at Wilson Sonsini Goodrich & Rosati.

The consultation is available at www.ofcom.org.uk/consultations-and-statements/category-1/protecting-children-from-harms-online. It closes for comments on 17 July 2024.