Cooley

Decoding the UK Online Safety Act 2023: Latest Draft Guidance, Key Features and Insights

November 29, 2023

On 9 November 2023, the UK Office of Communications (Ofcom) issued its first set of draft guidance on the UK's long-anticipated Online Safety Act (OSA), which aims to protect online users against illegal and harmful content. While the OSA officially became law in the UK on 26 October 2023, Ofcom – the UK's communications regulator – will now take a three-year phased approach to implementation and enforcement. The latest draft guidance from Ofcom focuses on how certain online service providers must approach their duties regarding 'illegal content' and is the first of four major consultations that Ofcom will conduct in the coming months.

At a high level, the OSA introduces a new UK regulatory regime to address online safety. It imposes extensive new obligations on online service providers to identify, mitigate and manage the risks of harm to users from illegal and harmful content. With a focus on the protection of children, the OSA builds on the age appropriate design code of the Information Commissioner's Office and confers special obligations on service providers whose platforms are likely to be accessed by children.

More broadly, the OSA is one of several new global regulatory developments focused on addressing online safety. The OSA is distinct from the European Union's Digital Services Act (see our February 2023 blog on the DSA); however, it bears similarities, as it also adopts a risk-based approach to content regulation with large or higher-risk online platforms subject to more extensive obligations, as explained in more detail below.

Which services are subject to the OSA?

There are three types of online service providers which are intended to be subject to the OSA, provided each have links with the UK:

- 'User-to-user' services (U2U services).
- Search services.
- Services that publish or display certain pornographic content.

The OSA, therefore, applies to qualifying service providers – wherever they are located.

Links with the UK

Services are considered to have links with the UK if they have a significant number of UK users **or** if the UK forms one of its target markets. The OSA does not specify the number of users that qualifies as 'significant', although Ofcom has advised organisations to be ready to explain their decisions, especially where they believe that their UK user base is not significant.

In addition, regulated U2U and search services are considered to have links with the UK if they are capable of being used in the UK, **and** there are reasonable grounds to believe that there is a material risk of significant harm to UK individuals presented by content associated with the service. This provision appears to be designed to capture high-risk services which might not otherwise be captured by the OSA – e.g., because the number of UK user numbers would not otherwise meet the 'significant user number' or 'target market' thresholds.

U2U and search services

U2U and search services are likely to be subject to the OSA if they have links with the UK (see above) and are not exempt. The OSA outlines certain services that are exempt – for instance, services will not be subject to the OSA if emails, SMS messages (texts) or one-to-one live aural communications are the only user-generated content enabled by the service.

Providers of pornographic content

Service providers that publish or display pornographic content are likely to be regulated by the OSA if they have links with the UK (see above). However, some types of services – such as 'internal business services' and 'on-demand programme services' – may be exempt under certain conditions.

How will the OSA impact in-scope services?

Categorisation

For regulated U2U and search services, the OSA takes a tiered approach to regulation by dividing certain services into categories ('categorised services'). Ofcom has stated that only a small proportion of services will be designated as categorised services. Categorised services are subject to additional duties – see the Obligations ('duties of care') section below.

Although the category thresholds have not yet been set, Ofcom has stated it will advise the government on the thresholds in early 2024. Ofcom anticipates that the government will pass the necessary legislation by summer 2024, and – assuming such legislation is passed – Ofcom will:

- Publish the register of categorised services by the end of 2024 (and, in any event, 'as soon as reasonably practicable').
- Publish draft proposals on the additional duties that categorised services will be subject to in early 2025.
- In mid-2025, start issuing categorised services with an annual notice requiring them to produce a transparency report.

The service categories are defined as follows:

- **Category 1. Regulated U2U services** that meet the Category 1 threshold conditions, which relate to the following factors:
  - Number of users.
  - Service functionalities.
  - Any other characteristics of the service that the government may consider relevant.

  The thresholds also will account for the likely impact of the number of users and the service's functionalities on how easily, quickly and widely content may be disseminated.

- **Category 2A. Regulated search or 'combined' services** (i.e., a regulated U2U service that also includes a public search service) that meet the Category 2A threshold conditions, which relate to:
  - Number of users.
  - Any other characteristics of the service that the government may consider relevant.
- **Category 2B. Regulated U2U services** that meet the Category 2B threshold conditions, which will be set by reference to the same factors as Category 1 services, i.e.:
  - Number of users.
  - Service functionalities.
  - Any other characteristics of the service that the government may consider relevant.

The exact threshold conditions for each category will vary and will be defined in secondary legislation, expected to be enacted by summer 2024.

Providers of pornographic content will not be categorised, but nevertheless do have duties of care, as set out below.

Obligations ('duties of care')

The OSA imposes obligations, or 'duties of care', which vary depending on both the type (i.e., U2U, search or pornographic) and category of service. To illustrate, we summarise some of the key duties below. Ofcom has stated its intention to produce guidance on each of these duties and the many others that are contained in the OSA over the next 18 months.

Duty	Service type/category	Summary	Reference

Protection from illegal content*	Regulated U2U services	Take proportionate measures (according to the size of the service and the assessment of risk associated with it) **to prevent** individuals from encountering 'priority illegal content' –meaning terrorism, child sexual exploitation and abuse (CSEA), or any offence listed in Schedule 7 of the OSA, such as threats to kill, harassment or stalking.	Part 3
Protection from illegal content*	Regulated search services	Take proportionate measures (according to the size of the service and the assessment of risk associated with it) **to minimise the risk of** individuals encountering priority illegal content or other illegal content that the provider knows about (having been alerted to it by another person or becoming aware of it in any other way).	Part 3
Protection of children	Regulated U2U services likely to be accessed by children	Take proportionate measures to: • **Prevent** (including through age verification or age estimation) children of any age from encountering 'primary priority content that is harmful to children' (e.g., pornographic content or content which encourages suicide). • **Protect** children in age groups judged to be at risk of harm from encountering other 'content that is harmful to children' (e.g., abusive content and content which incites hatred, bullying and/or unsafe challenges/stunts).	Part 3
Protection of children	Regulated search services likely to be accessed by children	Take proportionate measures (including age verification or age estimation) to: • **Minimise the risk of** children of any age from encountering primary priority content that is harmful to children. • **Minimise the risk of** children judged to be at risk of harm from	Part 3

		encountering harmful content.	
Empowerment of adults	Category 1 services	To the extent it is proportionate, provide adult users with controls for specified types of content – including content which encourages, promotes or provides instructions for harmful acts, e.g., suicide, self-injury or eating disorders. Controls must be easy to access and available to all adult users. Controls also must include the ability to filter out nonverified users (i.e., individual users who have not verified their identity to the service provider).	Part 3
Fraudulent advertising	Category 1 and Category 2A services	Use proportionate systems and processes to prevent users of all ages from encountering fraudulent ads, minimise the length of time such ads are available to users and swiftly react to user alerts about them.	Part 3
User identity verification	Category 1 services	Offer all adult users the option to verify their identity. Services may use any kind of verification process, and it need not require documentation to be provided. The primary use of this identification is for purposes of adult user empowerment (see above).	Part 4
Pornographic content	U2U and search services that publish certain pornographic content	Use age verification or age estimation (or both) to ensure that children are not able to encounter regulated pornographic content on the service. The age verification or age estimation must be highly effective at determining whether the user is a child.	Part 5

*Ofcom produced detailed draft guidance on illegal content as part of its first major consultation.

What are the key practical implications of the OSA?

Risk identification

One of Ofcom's priorities is for services to understand and prioritise the risk of harm and build the structures necessary to embed user safety. To achieve this, services will need to conduct risk assessments and put in place proportionate, risk-based systems and processes to improve user safety. Ofcom has published draft

guidance on how to conduct illegal content risk assessments, and the duty will come into force for most regulated services once Ofcom finalises this guidance (expected in autumn 2024).

Risk mitigation

Service providers will need to ensure that their services are structured to mitigate the risk of harm to users – including by designing features, functionalities and algorithms appropriately, starting with the areas of greatest risk (e.g., by taking proportionate measures to protect children).

The OSA requires services to use 'all relevant information that is reasonably available' to identify illegal content, which will be interpreted according to the size and capacity of the service, and whether the service used human moderators or automated systems (or both). Ofcom's draft guidance on illegal harms notes that whatever measures are proposed must be proportionate and technically feasible. However, the risk of erroneous takedown of legitimate content and potential implications for users' privacy (e.g., which could arise from scanning users' content to identify illegal material) have the potential to make this a challenging area for services.

How will the OSA be enforced?

Ofcom is responsible for enforcing the regime and is in the process of publishing guidance and codes of practice intended to help regulated companies comply with their duties under the OSA. The OSA provides Ofcom with several enforcement mechanisms against companies, including (but not limited to):

- **Fines,** which may be up to £18 million or 10% of worldwide revenue (whichever is higher).
- **Service restriction orders.** Ofcom may apply to the court for a service restriction order requiring ancillary services (e.g., payments providers) to withdraw their services.
- **Powers of entry, inspection and audit.** Ofcom will have powers of entry and inspection, including without a warrant in certain circumstances (but with seven days' notice).
- **Notices to deal with terrorism or CSEA content (or both).** Ofcom may require services to use accredited technology to identify and swiftly take down CSEA content and/or identify and swiftly secure terrorism content. Ofcom also may require services to use their 'best endeavours' to develop or source technology to satisfy such a notice.

Ofcom also may require services to name a senior manager who may reasonably be expected to be capable of ensuring compliance with the requirements of a notice. Under certain circumstances, senior managers could face criminal prosecution if, under the OSA, they fail to comply with an Ofcom information notice. Corporate officers (e.g., directors, managers, associates or secretaries) also may be criminally liable if a false or threatening communication offence is attributable to their neglect.

Conclusion

The OSA is broad in scope. Ofcom projects that it will encompass more than 100,000 online service providers. Similar to the UK General Data Protection Regulation, and as noted above, the OSA has extraterritorial reach, so it will likely regulate thousands of organisations located outside of – but with links to – the UK.

Services are strongly advised to start building effective compliance plans now. Initial steps to think about include:

- Participating in upcoming consultations on draft guidance and codes of practice with Ofcom.
- Considering how to address harmful and illegal content and apply age verification/age estimation (or both).
- Ensuring that internal processes and teams are in place to communicate with Ofcom, including in respect of any information requests, audits, inspections or interviews.
- Assessing whether there may be a need to use automated content moderation or content scanning tools, and how to resolve any associated privacy risks that may exist relating to such tools.
- If applicable, ensuring that current adult content control tools meet the requirements of the OSA.

For further information, or to assess how the OSA will affect your business, please contact Cooley lawyers James Maton, Joanne Elieli, Edward Turtle, Corina Demeter-Olive, Carol Holley, Morgan McCormack or Carolina Ljungwaldh.

We will be publishing further overviews of Ofcom's guidance as it is published by the regulator, so please stay tuned for updates and insights as matters develop.

Cooley trainee solicitor Mo Swart also contributed to this alert.

Key Contacts

James Maton London	jmaton@cooley.com +44 20 7556 4547
Morgan McCormack London	mmccormack@cooley.com +44 20 7556 4584