JENNER & BLOCK

A New Era in Online Safety: What Global Companies Need to Know About the UK's Online Safety Act

Client Alerts

June 24, 2025
By: Lucy Blake, Joanna Ludlam, Will Jones, Karam Jardaneh

Over the course of 2025, the United Kingdom's Online Safety Act (**OSA**) has been gradually coming into force reshaping the online safety landscape globally. The OSA requires in-scope companies to identify, mitigate, and manage the risks of harm from illegal content, as well as content that is harmful to children. While its stated intention is to make the United Kingdom one of the safest places in the world to use the internet, the OSA will impact companies globally. This is despite the United States' opposition to such rules, in light of their impact on US-headquartered tech companies[1] .

Non-compliance with the OSA has potentially serious consequences, including penalties of up to £18 million or 10% of providers' worldwide turnover (whichever is greater), criminal liability for providers' directors for failing to comply with notices under the OSA, and the risk of being blocked from the UK market.

The OSA is a complex piece of legislation, introducing extensive and novel obligations for companies. As a result, there is some uncertainty in how the OSA will be interpreted and enforced. This is likely to generate litigation, particularly in the public law realm, as companies challenge regulatory decisions and seek clarity on their obligations. Below, we break down this complexity into the Act's basic building blocks and set out the four key things companies need to know about the OSA.

1. Who needs to comply with the OSA?

The OSA applies to providers of:

- search services (e.g. search engines); and
- user-to-user services that allow users to post content or to interact with each other (e.g. social media services, online gaming platforms, online forums, consumer file cloud storage and sharing sites, video-sharing platforms, dating services, and online instant messaging services).

The OSA applies to providers that are either based in the United Kingdom or outside the United Kingdom but where:

- the service has a "significant number"[2] of UK users;
- the United Kingdom is a target market for the service; or
- the service is capable of being accessed by UK users **and** there is a material risk of significant harm to such users.

2. What are the requirements?

The OSA imposes system-related duties to assess and manage risks of illegal and certain other types of harmful content, rather than to directly police specific pieces of content.

All in-scope providers of regulated services are expected to comply with duties relating to illegal content and content which is harmful to children. Certain "categorised" providers will also need to comply with more onerous duties. Notably, however, the OSA is focused on narrow pockets of content and unlike its European counterpart, the Digital Services Act, it does not directly tackle disinformation.

Duties relating to illegal content ***(in force***[3] **)**

The OSA requires in-scope providers to take robust action in preventing access to "illegal content"[4] on their services. This includes:

- conducting risk assessments as to how likely users are to encounter illegal content and the nature and severity of harm likely to be caused;
- adopting proportionate safety measures to manage and mitigate those harms (such as preventing users from encountering illegal content and swiftly removing it).

The Office of Communications (Ofcom) has published the Illegal Content Codes[5] detailing the recommended safety measures for providers to comply with illegal content duties. In particular, it includes recommendations regarding the requirements to:

- balance OSA compliance with protecting users' rights to freedom of expression and privacy; and
- have in place mechanisms for users to report illegal content, and to include provisions in providers' terms of service for users to make complaints and bring contractual claims if they are suspended, banned, or if their content is withdrawn, in breach of the service's terms.

Duties relating to content harmful to children ***(partly in force with remaining duties expected to come into force in July 2025***[6] ***)***

Some of the responsibilities to protect children are covered under the illegal content duties – such as tackling the risk of child sexual exploitation and abuse offences. However, the OSA also requires providers to take action to protect children from content which does not amount to "illegal content", but which may nonetheless cause harm to children. These include pornographic, suicide, self-injury, and eating disorder content (defined as "primary priority content") and abusive, violent, bullying, dangerous stunts, or harmful substances content (defined as "priority content"), as well as other content which presents a material risk of harm to an appreciable number of children in the United Kingdom (defined as "non-designated content"). Harm may arise not only from the content of the material itself, but also the way content is disseminated (e.g. whereby an algorithm or other aspect of a system's design and operation pushes content to a child in high volumes over a short period).

The OSA requires in-scope providers to take action including:

- carrying out an assessment as to whether children are likely to access providers' services (following the Children's Access Assessment Guidance);
- conducting risk assessments as to whether children are likely to encounter and be harmed by content (again following the Children's Risk Assessment Guidance); and
- adopting proportionate measures to mitigate the risks to children. Ofcom published Guidance on Content Harmful to Children and draft[7] Protection of Children Codes detailing the recommended safety measures. The Codes of Practice take into account children's different age groups – with some measures designed to protect all children from "primary priority content" and others to protect younger age groups from "priority content" and "non-designated content".

Separately, since January 2025, platforms that publish their own pornographic content are required to take steps immediately to introduce robust age checks that meet Ofcom's guidance.

Duties for categorised providers ***(not in force before 2026)***

The OSA imposes additional and more onerous duties on "categorised" providers. These are services with higher risk functionalities and/or large numbers of users.

Categorised service providers will be subject to additional requirements to protect users from online harms, such as transparency reporting and disclosure of information about use of the service by a deceased child user, with further requirements imposed on the higher risk categories on a sliding scale (e.g. enhanced requirements on risk assessments, measures to prevent fraudulent advertising and, in the case of the highest risk category of service providers, additional terms of service duties, protections for journalistic content/content of democratic importance, and user empowerment and identity verification options).

Ofcom is expected to publish a register setting out the services that fall into these categories in summer 2025 and will publish further codes of practice for consultation and, where relevant, guidance for the additional duties on categorised services by early 2026.

3. How is the OSA regulated?

The United Kingdom's Office of Communications, known as Ofcom, is the regulator with powers to enforce the OSA.

Ofcom is also responsible for setting codes of practice and issuing guidance for providers on how they can comply with their OSA duties. Providers that implement the safety measures recommended in Ofcom's Codes of Practice (known as "safe harbours") will be deemed to have complied with the relevant duties. Providers may otherwise use what the OSA refers to as "alternative measures" to protect users. However, the onus will be on the service providers to demonstrate that such measures are sufficiently effective to ensure compliance.

4. What are the consequences of non-compliance with the OSA?

Ofcom's enforcement toolkit is very significant and includes:

- fining providers up to £18 million or 10% of global annual turnover – whichever is higher;
- blocking access to non-compliant services in the United Kingdom by requiring payment providers, advertisers, and internet service providers to stop working with a site, preventing it from generating money or being accessed from the United Kingdom;
- prosecuting senior managers if they fail to ensure companies follow information requests from Ofcom or comply with Ofcom's enforcement notices in relation to specific child safety duties or child sexual abuse and exploitation offences[8] .

Providers may challenge this enforcement action by way of an appeal to the Upper Tribunal, who will decide the cased based on the principles applicable to an application for judicial review in the High Court. In very broad terms, therefore, enforcement action may be subject to a valid challenge if it is illegal (including on grounds under the Human Rights Act 1998), irrational, or the decision-making process was procedurally unfair.

Ofcom's enforcement director, Suzanne Cater, commented: "*make no mistake, any provider who fails to introduce the necessary protections can expect to face the full force of our enforcement action.*" Indeed, Ofcom has already announced two investigations into Kick Online Entertainment S.A for failure to respond to an information request and to comply with its illegal content duties and a further seven investigations into child sexual abuse imagery on file sharing services, an investigation into a company's compliance with the illegal content duties and a porn providers' compliance with age-check rules to protect children".

Given the serious potential consequences of non-compliance, companies may find that the best way to immunise themselves against legal risks is to double down on safety processes, especially considering the softly formulated duties to "*have regard to the importance*" of freedom of expression and privacy laws. Arguably this may have the unintended consequence of more censorship and a less rich and informative online world. It may also give rise to complex tripartite disputes between providers, Ofcom, and online actors seeking to protect their rights to free expression and privacy.

The OSA marks a turning point not only in how the online landscape is regulated in the United Kingdom but how it is regulated globally. Taking proactive steps now will help providers avoid regulatory enforcement in the United Kingdom and also prepare them to face other regulatory requirements globally in the future. However, given the extensive and novel obligations under the OSA, well-intentioned companies might still find themselves in Ofcom's crosshairs. Our experienced team of lawyers at Jenner & Block is ready to help you navigate and comply with the OSA and face any governmental scrutiny that may arise.

Footnotes

[1] Although recent media reports have speculated that online safety rules are on the table for trade talks between the United Kingdom and the United States, the implementation of the OSA duties appear to be moving full steam ahead.

[2] The OSA does not set out how many UK users is considered "significant". Ofcom guidance indicates that providers should be able to explain their judgement, especially if they have determined that they do not have a significant number of UK users.

[3] Providers were required to complete their illegal content risk assessments by 16 March 2025 and must now comply with the illegal content duties.

[4] "Illegal content" is defined as content (which may consist of certain words, images, speech, or sounds) that amounts to a "relevant offence". The list of "relevant offences" for the purposes of the OSA includes (but is not limited to) terrorism and child sexual exploitation and abuse (CSEA) offences as well as hate offences, intimate image abuse, and extreme pornography.

[5] There are two separate Codes of Practice for regulated user-to-user service providers and regulated search service providers (together the "Illegal Content Codes").

[6] Ofcom published Children's Access Assessment Guidance requiring providers to have conducted their children's access assessment by 16 April 2025. If a provider concludes that the service is likely to be accessed by children, they will need to complete a children's risk assessment by 24 July 2025 and adopt appropriate safety measures to protect children.

[7] Like, the Illegal Content Codes, there are two separate codes for regulated user-to-user service providers and regulated search service providers (together the "Protection of Children Codes"). The Protection of Children Codes have been published in draft form, as submitted to the UK Secretary of State for approval and are expected to be finalised and come into effect from 25 July 2025.

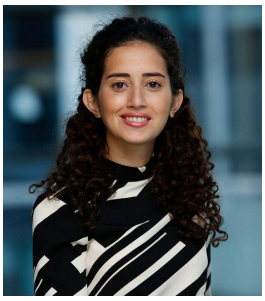
[8] An officer of a provider also commits an offence where they have consented or connived in the commission of offences, or it is attributable to neglect on the part of the officer. Such offences are not uncommon in the context of other UK regulations.

Related Attorneys

Lucy Blake
Partner
lblake@jenner.com
+44 330 060 5409

Joanna Ludlam
Partner
jludlam@jenner.com
+44 330 060 5465

Will Jones
Special Counsel
wjones@jenner.com
+44 330 060 5457



Karam Jardaneh
Senior Associate
kjardaneh@jenner.com
+44 330 060 5512

Related Capabilities

Investigations, Compliance, and Defense

© 2026 Jenner & Block LLP. Attorney Advertising. Jenner & Block LLP is an Illinois Limited Liability Partnership including professional corporations. This publication, presentation, or event is not intended to provide legal advice but to provide information on legal matters and/or firm news of interest to our clients and colleagues. Readers or attendees should seek specific legal advice before taking any action with respect to matters mentioned in this publication or at this event. The attorney responsible for this communication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome. Jenner & Block London LLP, an affiliate of Jenner & Block LLP, is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed →