THE UK ONLINE SAFETY REGIME

After being in the works for half a decade, the Online Safety Act 2023 (OSA) received Royal Assent last week. It will join the EU's Digital Services Act (EU DSA) as one of the newest and boldest tech regulations in Europe and is aimed at making the UK 'the safest place to be online'.

The OSA will deploy a diverse set of rules, obligations, and regulatory powers designed to protect users, particularly children, from online harms. Whether the OSA, and its regulator, Ofcom, will be successful in striking the balance between freedom of speech and other rights, and the need for online safety, will remain in contention for years to come.

In this first of a series of three articles on the online safety regime in the UK, we will provide an overview of the OSA and what it entails for the 100,000 services estimated to be in scope. The following articles in this series will unpack compliance obligations and practical guidance for businesses in more detail.

A very brief history of platform regulation

The 20-year-old EU E-Commerce Directive (2000/31/EC) set out to regulate the internal market for online services, by removing obstacles and adopting a balanced framework. It provides broad exemptions from liability for service providers who solely host content or who act as 'mere conduits'. It also prohibits EU Member States from imposing a general obligation on service providers or online intermediaries to actively monitor their platform for illegal content. At heart, the Directive and similar rules in the US were concerned with balancing the chilling effect of imposing content removal obligations on internet intermediaries on the one hand, and the technical difficulty in monitoring and evaluating content and online safety (and who should do so) on the other. The result was a focus on reactive measures for content removal rather than a proactive monitoring and takedown regime.

A lot has changed since then. The proliferation of online platforms, social media and digital communication tools has resulted in an exponential increase in user-generated content and interactions. These changes have also brought about new challenges related to online safety, the spread of harmful content, hate speech, and misinformation. The internet is now a much more complex ecosystem, and the OSA is the UK's response to these transformational changes.

The new normal: the Online Safety Act

The OSA seeks to create a regulatory framework that requires companies to improve online safety for individuals, including elevated duties in respect of the protection of children. The UK's communications regulator, Ofcom, will oversee regulatory enforcement of the OSA with a host of new powers.

The where and who: territorial and material scope

The new framework applies to user-to-user (U2U) services and search services (i.e. search engines) to the extent that the service has 'links' with the United Kingdom. This can involve having a significant number of UK users, having the UK as a target market, or the service is capable of being used in the UK by individuals and may present a 'material risk of significant harm' (s. 4(5)-(6)).

- The definition of U2U services is broad, referring to internet services where content is either generated directly on the service by a user or uploaded by a user, and this user-generated content is shared with or accessible to other users (s. 55(3)). The government estimates that some 100,000 services will be in scope of the new regulations, with between 30-40 amongst them that pose the highest risk being subject to additional obligations under the OSA.

- All in-scope service providers will fall into one of three categories (s. 95(10)):

  – Category 1 – services with the highest risk and highest reach user to user, e.g. the largest social media sites and pornography sites. These services will have additional duties compared to Category 2B U2U services;

  – Category 2A – search services; and

  – Category 2B – U2U services that do not meet the Category 1 threshold. The majority of service providers will fall into this category.

Where a service provides both U2U and search services, it may be categorised under multiple categories. The thresholds for these categories will be set out in secondary legislation.

The what: the duties and obligations

The OSA creates a long list of wide-ranging duties that apply to in-scope providers depending on which category they fall into. Each provider will have a core duty to prevent UGC or activity on their services which causes "physical or psychological harm" to individuals. The range of these duties largely covers "illegal content" (see ss. 9-10, 26-27), where sharing such content might amount to criminal offences.

Additional duties apply to providers of certain kinds of service, such as services that are likely to be accessed by children and services that have high risk functionalities and/or reach a large number of individuals. The additional category of "lawful but harmful" content applies in this context, where providers will have a duty to *use proportionate systems and processes* to prevent children from encountering the most harmful content relating to suicide, deliberate self-injury, and eating disorders (*primary priority content that is harmful to children*) and mitigate the risks posed by other types of harmful content, including bullying and abusive content (s. 12).

The OSA also empowers individuals, but does not go so far as to create new, directly enforceable rights *per se*. Providers will have to create mechanisms to allow users to report harmful content or activity (s. 20) and to appeal removal of their content (s. 21). ID verification (s. 64) and content control features in relation to harmful content (s. 15) must also be provided in certain cases.

The government is also able to make substantive amendments to the law itself by secondary regulation. For example, s. 220 allows the Secretary of State for Science, Innovation and Technology (SS for DSIT), by secondary regulation, to amend the definition of certain types of content (under s. 55), if there is a risk of harm to individuals.

Finally, all providers will be required to complete risk assessments of their services and take reasonable steps to reduce the risks identified (ss. 9-10, 26-27). This goes beyond the EU DSA, which only requires a systemic risk assessment of the largest in-scope services (EU DSA, article 34). This requirement is onerous, requiring service providers to take into account a large range of considerations under s. 9(5), such as the level of risk of functionalities of the service facilitating the presence or dissemination of illegal content, the different ways in which the service is used and the impact of such use on the level of risk of harm.

The when: implementation and entry into force

The OSA envisages that most of its operative provisions will come into effect only when secondary legislation has been passed by the SS for DSIT. Additionally, Ofcom is required to produce guidance and codes of practice. Interestingly, unlike certain other regimes such as the UK GDPR, the OSA expressly recognises that compliance with codes of practice will be deemed to be compliance with the OSA itself (s. 49(1)).

Ofcom launched its Online Safety Group on 1 April 2023, in preparation for the Bill's passage through Parliament, with Gill Whitehead as Group Director. It has also updated its regulatory **roadmap**, which includes, *inter alia*:

- consultations on illegal harms, age verification and protection of children from Q4 2023 through Q2 2024;
- estimated publication of categorisation thresholds in Q3 2024 (by the SS for DSIT);
- publication of codes of practice and guidance from Q4 2024 onwards; and
- establishing a public consultation process for secondary legislation on categorisation of services and associated additional duties, likely to take at least 6 months.

The OSA will therefore come into effect in its entirety only some time in 2024 – or later.

The (legal) why: enforcement powers

The OSA creates powers for Ofcom to impose a penalty of the greater of £18 million or 10% of global annual revenue. Ofcom is also granted a range of other enforcement powers (Part 7), including:

- requiring a service provider to give information (via an information notice) for the purpose of assessing compliance with any duty or requirement under the OSA (s. 100);

- requiring the provider to name an individual who the provider considers to be a senior manager, a person in a position to ensure compliance with the requirements of the notice (s. 103);

- appointing a skilled person, or requiring a provider to appoint one, in order to provide Ofcom with a report on relevant matters to assist Ofcom in assessing a failure to comply with a requirement or to develop Ofcom's understanding of the risk of failing to comply and ways to mitigate that risk (s. 104); and

- powers to require interviews (s. 106), and of entry, inspection and audit (s. 107).

In addition, Ofcom can also apply to the Court for orders to restrict a service entirely – known as business disruption measures (ss. 144-147).

Finally, the OSA introduces a criminal liability regime and creates several offences. These include a range of information offences, such as where a person provides information that is false in a material respect in response to an information notice (s. 109(3)). Akin to the senior managers regime in the Financial Services and Markets Act 2000, the OSA also creates a requirement for providers to name a senior manager of the entity "*who may reasonably be expected to be in a position to ensure compliance with the requirements of [a] notice*" (s. 103). Should the entity be found to commit an offence under s. 109 (comprising a range of offences relating to responding to information notices), and if the senior manager has "*failed to take all reasonable steps to prevent that offence being committed*", then that individual will have committed an offence (s. 110). A range of defences is available.

The debate on end-to-end encryption

One of the most controversial provisions of the OSA is the power of Ofcom to issue notices to deal with terrorism content or child sexual exploitation and abuse (CSEA) content, or both, under s. 121. A notice under s. 121 will require a provider to use technology to deal with content found on or in its services, including (for example) identifying and taking down terrorist or CSEA content.

Critics have noted that this will, in effect, endanger end-to-end encryption, a key pillar of digital privacy, since to identify and take down content requires intercepting the communication between the sender and the recipient, between whom content is encrypted. More practically speaking, the technology required by the OSA to do so is not known to exist, yet Ofcom's power under s. 121 is unfettered, save that the technology must meet minimum standards of accuracy and have appropriate safeguards in place. For now, Lord Parkinson, an Under Secretary of State in the Department of Culture, Media and Sport, has indicated as follows: "*I am happy to make clear, as I have, what that means: if the appropriate technology does not exist that meets these requirements, then Ofcom will not be able to use [section 121] to require its use.*"

Our takeaways: the good, the bad, and the ugly

Without formal (or draft) guidance from Ofcom or the mandated secondary legislation on key topics such as service categorisation, much of the 'meat on the bones' of the OSA remains to be created.

It is clear, however, that this is a new direction in the regulation of digital services: the OSA creates a novel regulatory regime that cuts across traditional areas of legislation, from human rights to consumer law, data protection, and criminal law. Quite rightly so, perhaps, since along with its cousin the EU DSA, the OSA seeks to regulate a disparate group of largely heterogenous services catering for the full range of online users.

On a practical level, companies will have to keep a close watch on how Ofcom and the government develops the regulatory framework through guidance and secondary legislation. It is unclear, for example, if the regulatory and quasi-legislative steps they take to flesh out the regime may be subject to judicial review. The EU DSA, for example, has already come under attack on multiple fronts. The OSA also does not appear to confer new rights upon individuals to enforce against service providers, such as under the data protection or competition law regimes, where private enforcement by way of individual litigation might run in parallel to public enforcement by the regulator.

More fundamentally, will the Internet be safer?

There has always been an inherent tension between safety and security on the one hand and rights and freedoms on the other. The OSA does not address these hard questions head on, choosing instead to delegate them to Ofcom and the executive. Change remains some way off.

CLIFFORD

CHANCE

CONTACTS

Simon Persoff
Partner
London
T: +44 207006 3060
E: simon.persoff@cliffordchance.com

Ioana Burtea
Lawyer
London
T: +44 207006 1699
E: ioana.burtea@cliffordchance.com

Richard Jones
Senior Associate
Knowledge Lawyer
London
T: +44 207006 8238
E: richard.jones@cliffordchance.com

Arnav Joshi
Senior Associate
London
T: +44 207006 1303
E: arnav.joshi@cliffordchance.com

Oscar Tang
Senior Associate
London
T: +44 207006 3749
E: oscar.tang@cliffordchance.com

CONTRIBUTOR

Ieva Eringyte
Trainee Solicitor
London
T: +44 207006 1975
E: ieva.eringyte@cliffordchance.com

2311-008552