Articles + Publications | April 12, 2023

UK Online Safety Bill

Privacy & Cybersecurity Newsletter

WRITTEN BY

Nick Elwell-Sutton

RELATED OFFICES

London

The UK Online Safety Bill (OSB) is still before Parliament, but if passed, it would implement a transformative change to the legal responsibilities and accountability of online providers of user-generated content and search engines. The main objectives of the OSB are to protect children, prevent illegal content, provide users with greater control over what they see and how they interact with other users, require service providers to remove material that breaches their own terms of service, and establish a duty to prevent fraudulent advertising. New regulatory and enforcement powers will be provided to the Office of Communications (OFCOM) and this is backed up by the risk of fines of up to 10% of global turnover and, controversially, the availability of criminal penalties for defaulting senior managers for certain failures. While much of the finer details will be set out in separate regulations and codes of practice to be issued in due course, the broad framework is starting to take shape.

Which services will it apply to?

OSB is very broad and would apply to an *"internet service that allows content generated directly on the service, or uploaded to or shared on the service, by a user, to be encountered by another user, or other users"* as well as conventional search engines. In practice, this means any service that hosts user-generated content whether videos, images, or comments, or which allow users in the UK to communicate with other people online and so it includes messaging applications and chat forums. It will therefore apply to the well-known social media sources: Twitter; TikTok; Facebook; Instagram; BeReal; Snapchat, WhatsApp; YouTube; Google; and Bing as well as more specialist user forums and chatboards. It would apply if the service provider targets UK consumers even if the service provider is not based in the UK. The precise obligations depend on service-provider size with more onerous requirements for the larger and most popular sites. The thresholds for each will be set later.

What is the purpose?

Broadly, OSB is aimed at preventing not only illegal material (such as terrorist material and child sexual images) but also "harmful but lawful" content. While applicable to all users, OSB introduces specific measures to protect children. What constitutes "illegal" content will be set out in a code of practice after feedback from service providers as well as setting out what constitutes "harmful but lawful" content for children and adults, respectively.

What is required?

In respect of children, providers will be required to assess whether the service is likely to be accessed by children

and carry out a risk assessment. Whether age verification for children will be a mandatory requirement is still the subject of ongoing consultation, but many service providers may voluntarily seek to implement verification at age 18 to avoid the more stringent child safety requirements. Providers will be required to ensure children do not access “harmful but lawful” content — what this will comprise will be set out in the forthcoming code of practice and be the subject of separate regulations in due course. The overarching premise is that it poses a *“significant physical or psychological harm to children”*. Examples of this are likely to include, promotion of anorexia, suicide and self-harm content, drug use, and content promoting bullying. It remains to be seen whether it will also extend to disinformation, particularly on controversial subjects where there are a range of viewpoints. Services in scope will need to take steps to prevent access to such material by children and enhance their reporting and removal procedures and develop their complaints mechanisms.

For adults, the types of legal material the service contains or restricts will need to be set out clearly in their terms of service and provide options for adults to limit or restrict the types of lawful material they see and who they interact with.

In addition there will be a specific duty on major providers to take steps to prevent fraudulent adverts such as “get rich quick” and other scams, minimise the time they are present and to remove them promptly.

Service providers will also have to provide adults the ability to verify their profile. Whether mandatory age verification for adults accessing pornographic material will be required is still the subject of legislative debate, but adult content providers will need to ensure that children are not able to encounter pornographic material and which may, by default, lead to mandatory age-verification by the provider to ensure compliance.

Enforcement

OFCOM, the statutory regulator, will have significant powers both to monitor and to take enforcement action. This includes the ability to mandate the use of approved technology to identify and remove illegal content such as that relating to terrorism or child sexual exploitation. In addition it will have the ability to compel providers within scope to disclose the algorithms used in selecting and displaying content so that it can assess how platforms prevent users from seeing harmful material. It can also require them to undergo external audits of their compliance.

In addition OFCOM will be able to enter premises either on prior notice or without notice but with a warrant to access data and equipment and to request interviews with provider employees.

Penalties

Penalties available include fines of up to £18m or, if higher, 10% of global turnover and which for the larger providers could be significant sums. In addition it can impose business interruption measures including, ultimately, service restrictions.

A particularly controversial measure has been the availability of up to two years imprisonment for senior managers who suppress, destroy or alter information requested by OFCOM, who fail to comply with, obstruct or delay OFCOM when exercising its powers of entry, audit and inspection, for providing false information or for employees

who fail to attend or provide false information at an interview. A recent amendment also provides a further offence where a senior manager has *"consented or connived in ignoring enforceable requirements, risking serious harm to children"*.

For these purposes a "senior manager" is if the individual plays a *"significant role in (a) the making of decisions about how the entity's relevant activities are to be managed or organised, or (b) the actual managing or organising of the entity's relevant activities."*

The OSB is in the latter stages of the legislative process and while substantive amendments may still be made, it is likely to receive Royal Assent by mid-year. However much of the granular detail will follow after that in codes of practice and separate regulations and which will need to grapple with some difficult concepts around what exactly constitutes *"legal but harmful"* content. Like an elephant, you know it when you see it, but transcribing this to legal text is likely to prove challenging.

The OSB may also be have the unintended effect of causing terms of service to be watered down as to what content a service may contain. Ultimately, some providers may decide it is simply too difficult to comply with and instead block UK users.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber