[GB] The UK’s Online Safety Bill moves forward on path to becoming law

IRIS 2023-9:1/8

Alexandros K. Antoniou
University of Essex

On 19 September 2023, the UK’s long-debated Online Safety Bill (OSB) received Parliamentary approval and will soon achieve Royal Assent, clearing the way for it to become law. This new legislation represents a seminal milestone in digital and technological policy formulation in the UK’s post-Brexit era. It will introduce a new regulatory regime for online platforms and search engines which target the UK, imposing a set of obligations on in-scope services with consequences for non-compliance.

Main objectives

The Bill, which has become the subject of intense discussion and scrutiny, has five policy objectives: (a) to increase user safety online; (b) to preserve and enhance freedom of speech online; (c) to improve law enforcement’s ability to tackle illegal content online; (d) to improve users’ ability to keep themselves safe online; and (e) to improve society’s understanding of the harm landscape.

Some key provisions

The OSB has had a long and contentious journey through Parliament since its initial publication in March 2022. Having cleared its final parliamentary hurdle on 19 September 2023, it is (at the time of writing) awaiting Royal Assent and will soon enter the statute books as the Online Safety Act 2023 (OSA).

The OSA introduces several provisions that will shape the online landscape in the UK. At its core, this landmark legislation puts an independent regulator (Ofcom, more below) in charge of overseeing a rigorous risk management framework for all social media platforms, with bigger or riskier companies having greater accountability. It requires companies to understand the risks inherent in the design and functionality of their service and mitigate the most serious.

The Act places duties on user-to-user services and search services, thus covering a wide range of services, including social media companies, search engines, forums, gaming services, chat services, dating apps, and messaging services. In addition, the new legislation includes new rules for pornography providers that apply beyond social media and search (i.e., to ‘internet services’ that publish or display “regulated provider pornographic content”), requiring that children in the

UK must not normally be able to encounter such content online through measures like age verification.

Thus, businesses of different types and sizes will therefore be required to comply with the OSA. Any service that targets UK users will be caught, so international services with a relatively modest UK user base will still need to comply. However, certain services are excluded from the Act's scope. This includes e-mail services, texts, internal business services, and services whose only user-to-user interaction is via "below-the-line" content (e.g., comment sections). Broadcast and print media, already regulated or self-regulated, also enjoy a carve-out.

More specifically, the OSA requires in-scope service providers to take proportionate measures to prevent users from encountering "priority" illegal content (such as terrorism and child sexual abuse), minimise the length of time such content is present and promptly remove any illegal content when alerted to it.

To safeguard children online, the OSA imposes stricter obligations on certain services to prevent minors from seeing the 'highest risk' forms of content, such as content that encourages, promotes, or provides instructions for suicide, self-harm and eating disorders. Age verification and age estimation measures must be highly effective in preventing children from accessing pornographic content. The new law also grants greater powers for coroners to access children's data on behalf of bereaved parents, should a tragedy occur.

Moreover, regulated service providers are required to prevent users from encountering fraudulent adverts. Stricter user empowerment provisions have been added to enable adult users of the largest or riskiest platforms to avoid content they do not want to see (including from anonymous accounts, abusive or misogynistic content, etc). The Act also introduces greater protections for women and girls disproportionately affected by online harms, through dedicated Ofcom guidance to services.

Additionally, the OSA requires service providers to allow users to report illegal content easily and maintain transparent complaint procedures. This ensures that users can voice their concerns, including issues related to content takedowns.

The OSA also explicitly emphasises the importance of freedom of expression and privacy laws when implementing online safety measures, aiming to strike a balance between safety and individual rights.

Finally, the Act creates new criminal offences, including the offences of false communications, threatening communications, sending or showing flashing images electronically ("epilepsy trolling"), sending images of genitals ("cyber-flashing"), and sharing intimate images online, including DeepFake pornography.

Ofcom, the online safety regulator

The UK's communications regulator, Ofcom, is appointed as the regulator responsible for online safety under the OSA. Ofcom will play a pivotal role in ensuring the success of the legislation and has been tasked with developing Codes of Practice that will flesh out detail on how regulated services can comply with their duties once the Act is in force. Of note, although alternative approaches can be taken by in-scope services, the Codes are expected to offer the clearest approach to compliance. Ofcom has clarified that requirements will vary for different types of service, and the duties imposed on service providers will be limited to what is proportionate and technically feasible.

Non-compliance with the OSA carries significant consequences. In-scope services that fail to meet their duties could face fines of up to £18 million or 10% of their global annual revenue, whichever is higher. Additionally, senior executives and managers could be held personally criminally liable for specified offences (e.g., failure to comply with children's safety duties, where it is attributable to any neglect on the part of an officer of the regulated entity).

Continuing controversies

Two aspects of the OSA have raised concerns: age verification and end-to-end encryption. The OSA mandates certain businesses to verify the age of online visitors using age verification or estimation software. Critics argue that such systems are unreliable and pose privacy threats. In addition, the OSA's requirements for scanning proactively private messages for illegal content have raised some concerns (particularly by tech companies like WhatsApp and Signal) about the potential erosion of end-to-end encryption. The government has sought to clarify that:

"There is no intention by the Government to weaken the encryption technology used by platforms. As a last resort, on a case-by-case basis, and only when stringent privacy safeguards have been met, Ofcom will have the power to direct companies to make the best efforts to develop or source technology to identify and remove illegal child sexual abuse content. We know that this technology can be developed. Before it can be required by Ofcom, such technology must meet minimum standards of accuracy. If appropriate technology does not exist that meets these requirements, Ofcom cannot require its use. That is why the powers include the ability for Ofcom to require companies to make best endeavours to develop or source a new solution."

The road ahead and the current VSP framework

The OSA represents a significant shift in regulating online safety in the UK. It marks a move from an era of self-regulation, where service providers decide what

amounts to safe design and whether to enforce their terms of service, to regulation under which services are accountable for their choices.

The road ahead is likely to involve consultations, feedback collection, and potential adjustments to ensure that the OSA effectively fulfils its intended purpose. Ofcom will adopt a phased approach to the Act's implementation, with phase one (shortly after the Act's commencement) focusing on illegal content duties, phase two on child safety duties and pornography, and phase three on transparency, user empowerment and other duties on categorised services.

Finally, it should be noted that the existing Video-Sharing Platforms (VSP) regime will remain in force for a transitional period, meaning that all pre-existing, UK-established VSPs will remain subject to the obligations in Part 4B of the Communications Act 2003 until it is repealed through future secondary legislation (see further IRIS 2023-6:1/25). Given the two regimes' shared objective to improve user safety by requiring services to protect users through the adoption of appropriate systems and processes, Ofcom considers that compliance with the VSP regime will assist services in preparing for compliance with the forthcoming online safety regime set out in the OSB.

How Ofcom is preparing to regulate online safety (Ofcom, 15 June 2023)

https://www.ofcom.org.uk/online-safety/information-for-industry/roadmap-to-regulation/0623-update

House of Commons, Online Safety Bill (Hansard, Vol 737, Col 804, 12 September 2023)

https://hansard.parliament.uk/commons/2023-09-12/debates/81853BB7-375E-45C0-8C9D-4169AC36DD12/OnlineSafetyBill#contribution-1BDC6830-E3DB-45BD-B048-393063DB4D32

It's (nearly) here: a short guide to the Online Safety Act (CUKT, 19 September 2023)

https://carnegieuktrust.org.uk/blog-posts/its-nearly-here-a-short-guide-to-the-online-safety-act/