BCLP. Client Intelligent

Insights

GOVERNMENT BREAKS NEW GROUND WITH REVISED ONLINE SAFETY BILL

DIGITAL SPEAKS SERIES

Mar 28, 2022

SUMMARY

The latest version of the Online Safety Bill was introduced in the UK's Parliament on 16 March 2022. It now begins the process of being scrutinised, amended and debated on but it is anticipated that this is the version that will ultimately be passed and made into law in the UK. What does this mean for the technology sector, especially those offering online user-to-user services and online search services in the UK, and abroad? If passed in its current form, the Bill will create what the UK government claims is a world-first online safety regulatory framework – backed up by sanctions, including heavy financial penalties and new criminal offences, marking a significant change for certain online businesses. Senior managers will be handed responsibility for overseeing compliance with the regulator's requests for disclosure and subject to potential criminal sanctions, where they fall short, and the Bill will result in the need to devise and implement compliance systems and processes in accordance with the risk-based approach, that underpins the new regulatory regime.

What are the aims behind the new regime?

The key focus of the legislation is on removal of illegal content (such as material relating to terrorism and child sexual exploitation and abuse ("CSEA") – building on earlier EU legislative initiatives in this area requiring EU member states to take greater action to limit the display of, and access to, such materials). The target is technology providers who profit from hosting user-generated, advertising content and databases and the goal is to require them to take more responsibility for harmful content presented to users of their services – to make them, effectively, police this sector.

Who will be in scope of the regulatory regime?

The remit of the Bill is to regulate: (i) those firms which allow users of its services to encounter other users' user-generated content (e.g. hosting service providers, user-generated content sharing

platforms) and (ii) online search engines. The legislation is intended to be extra-territorial and will apply to regulated services with 'links' to the UK: (i) either it has a significant number of users in the UK (and the concept of 'significant' is not defined in the legislation) or is being targeted towards UK users; or (ii) is capable of being used by individuals in the UK and gives rise to a material risk of significant harm to individuals in the UK arising from content on/via the service.

How will the legislation achieve its aim?

In its current form, those services falling within the scope of the Bill would need to operate the services in such a way as to minimise the presence of certain categories of content (e.g. illegal content, terrorist content and content that is harmful to children). The Bill imposes a series of legal requirements requiring providers to assess and take steps to mitigate risks to end users and put systems and processes in place to facilitate reporting of harmful content types and more effective oversight by those responsible for enforcing online safety. The regulatory regime created by the Bill adopts a risk-based regulatory approach, dividing service providers into categories, with the Secretary of State to issue regulations to determine the threshold conditions for each category, with those providers in Category 1 subject to the most intensive regulatory oversight. Categorisation will be determined by the numbers of users of the service and the functionalities offered by the service, as well as the level of risk of harm posed by content disseminated by the service. This will then dictate if a particular service provider needs to produce annual compliance / transparency reports (and pay a fee to Ofcom). At present no guidance has been provided as to how the categorisation will work – these will be specified in later regulations, but will be determined by numbers of users and functionalities of the particular service (Schedule 10 of the Bill). 'Category 1' services will be subject to the widest controls and will be those services with the largest number of users.

What positive actions will be required?

The new duties on service providers regulated by the Online Safety Bill include the following:

- the need to undertake an illegal content risk assessment;
- the taking of proportionate steps to mitigate and effectively manage the risks of harm to individuals as identified in the illegal content risk assessment;
- use of proportionate systems and processes designed to minimise the presence of priority illegal content, the length of time it is present, and its dissemination;
- use of proportionate systems and processes designed to swiftly take down illegal content when notified or otherwise aware of it; and
- specifying clearly in terms and conditions how individuals are to be protected from illegal content, addressing terrorism and CSEA content, priority illegal content, and other illegal content separately.

Platforms will be under an express duty to report CSEA content to the National Crime Agency (replacing the formerly voluntary notification process).

The general duty of care in the Bill requires in-scope companies to put in place systems and processes to remove illegal content as soon as they become aware of it and take additional, proactive measures with regards to the most harmful 'priority' forms of online illegal content. Schedule 7 sets out the (long) list of criminal content which in-scope firms will be required to remove as a priority. New additions this iteration include criminal content relating to online drug and weapons dealing, people smuggling, revenge porn, fraud, promoting suicide and inciting or controlling prostitution for gain. The government's Consultation Response suggests that the systems and processes services may use to minimise illegal or harmful content could include user tools, content moderation and recommendation procedures. Note: the legislation does not specifically provide for content minimisation duties for terrorism and CSEA content. It is understood that these will be included in the mandatory codes of practice to be issued by Ofcom that will replace the current interim voluntary codes for these categories of content.

Services will also need to minimise the length of time for which these types of content is present and minimise the dissemination of it (and, once it is aware of the presence of such content, 'swiftly take down such content'). No guidance has been provided as to what 'swiftly' will entail. In the current legislation, "user-to-user services" are internet services by means of which content that is generated by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service. "Encounter" is defined as meaning, in relation to content, reading, viewing, hearing or otherwise experiencing content. And "content" means anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description.

Service providers whose services are likely to be accessible by children will have additional duties to protect young people from accessing legal but harmful material. Providers who publish or place pornographic content on their services will be required to prevent children from accessing that content. And those services which are deemed to be the largest / highest risk platforms will also be under a duty to address content which is legal but harmful, and accessible by adults. This may involve greater enforcement of the terms and conditions of use of such services, as well as allowing users more control about who they interact with and potentially identity verification tools. Larger platforms will also be required to put in place measures to prevent their services being used to display fraudulent advertisements. For example, the Bill contains a requirement to operate in a way designed to prevent individuals from encountering fraudulent advertisements – this term being widely defined and includes advertisements which would contravene the prohibitions on carrying out regulated activity under the UK's financial services regulatory regime, as well as advertisements which are fraudulent. This part of the Bill alone creates a huge area of risk for those businesses operating in the UK, who aren't familiar with the regulatory regime for financial services in the UK.

The legislation also prescribes that service providers regulated under the Bill implement a formal system of notification to allow users to notify the operator of illegal / harmful content.

How will the regulatory regime be enforced?

Failure to comply with a regulatory requirement created under the legislation will lead to regulatory intervention and turnover-based fines (the greater of £18 million or 10% of qualifying worldwide revenue) and potentially such services being blocked. The Bill also creates senior management responsibilities for compliance with these information notices and consequent criminal offences in respect of those senior managers to fail to take steps to ensure compliance.

Ofcom will have its regulatory remit extended, to include the power to impose financial penalties for non-compliance and investigatory powers. This includes the power to compel disclosure by issuing information notices and/or to bring proceedings for criminal offences against technology companies. Ofcom will also be empowered to: (i) charge fees to service providers; (ii) establish a register of regulated service providers; and (iii) conduct risk assessments to identify and assess the risks of harm presented by services of different kinds (and looking at harm posed to both adults and children of both illegal and harmful content).

The Bill aims to replace the offences that can currently be committed by those posting illegal or harmful content by creating three new communications offences: a harmful communications offence, a false communications offence and a threatening communications offence, as well as the creation of a new "cyberflashing" offence. The Bill in its current form creates a number of other new criminal offences, such as, failing to comply with the requirement to report child sexual exploitation and abuse content. Failing to comply with a notice from the regulator requiring the provider to provider information, which it considers necessary to enable it to carry out its regulatory oversight functions, is also an offence, as is providing such information where it is recklessly false, or providing it but failing to decrypt it so the regulator can read it or destroying the material.

Conclusion

The UK's Online Safety Bill should also be seen in the context of EU regulatory reform – with the EU's proposed Digital Services Act also introducing increased responsibilities for online platforms to notify law enforcement of criminal offences. Separately, there is also the French loi Avia (which requires online platforms to inform the competent public authorities of any content reported to them that may constitute one of a number of criminal offences, including hate speech, and to provide data which would help the authorities to identify the user who posted the content) and the German Network Enforcement Act (NetzDG) which has recently been amended so that from 1 February 2022, platforms will be required to report certain types of unlawful content to the Federal Criminal Police Office, such as online threats and hate crime content. The publication of the revised draft Bill marks an important step, but there are some important questions left unanswered – namely what legal but harmful content a service provider would be required to remove or block and the

thresholds at which the various compliance obligations will kick in. We expect the Bill to transition through Parliament in accordance with the usual legislative timescales (not to be fast-tracked) but we could see some of these provisions be brought into force by the Autumn.

RELATED CAPABILITIES

- White Collar
- Technology Transactions
- Intellectual Property & Technology Disputes
- Commercial Transactions
- Regulation, Compliance & Advisory
- Marketing & Advertising

MEET THE TEAM

Anna Blest

London

anna.blest@bclplaw.com
+44 (0) 20 3400 4475