LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

UK Online Safety Bill Delayed, But Firms Should Still Prepare

By **Caroline Black, Laura Manson and Marjolein De Backer** (July 19, 2022, 8:42 AM BST)

Caroline Black

Laura Manson

Marjolein De Backer

The Online Safety Bill was recently introduced with the intention of establishing a new online safety regulatory regime in the U.K. Until last week, the bill was on track to be enacted in early 2023, having been scrutinized by a committee of members of Parliament in June, and due to move to report stage later this month.

As a result of Conservative Party leader and Prime Minister Boris Johnson's resignation, and the decision to prioritize enacting other legislation before parliament's summer recess this week, the timetable for the bill has now been delayed.

This is not the end of the bill. It is likely to be reintroduced during the next parliamentary session later this year. What remains to be seen is the final form of the bill, which has undergone numerous revisions since it was first drafted.

While the ultimate form of the bill remains uncertain, Ofcom, the U.K.'s communications regulator, has clearly stated that it expects tech firms to start preparing now for the new regime.

If enacted, the bill as currently drafted will create a new regulatory and enforcement framework requiring online content providers, or OCPs, to tackle illegal and other harmful content on their services.

The bill mirrors laws recently proposed in the EU and U.S., and has the potential to be a leading legislative model for other countries seeking to improve online safety by regulating OCPs.

Here we summarize the main elements of the U.K. bill in its present form and examine the global trend toward increased regulation of OCPs, and how that will have an impact on OCPs that provide online services around the world.[1]

New Regulatory Obligations

As a minimum, the bill will impose statutory duties of care on social media platforms, online forums and search engines that host user-generated content, or OCPs, to:

- Assess their user base and the risk of harm to users from content on the service, and update their risk profile as and when risk profile changes;

- Take active steps to mitigate the risk of harm to individuals arising from illegal content and activity, and for services accessed by children, activity that is harmful to children — what will amount to harmful activity will be defined in regulations;[2]

- Implement systems and processes to allow the reporting of specified types of content;

- Establish adequate complaints procedures for specified content; and

- Put in place systems and processes to ensure that criminal content is reported to the U.K. National Crime Agency.[3]

The bill also requires the secretary of state to pass regulations specifying threshold conditions by which OCPs' services will be categorized as Category 1, Category 2A or Category 2B.

Additional duties will be imposed on OCPs providing Category 1 services, including a duty to carry out and record adults users' safety risk assessments, a duty to protect adult users' online safety, a duty to empower users to take greater control over their exposure to harmful content, and duties to protect content of democratic importance and journalistic content.[4]

The threshold conditions will be set with reference to the OCP's number of users and the functionality of its services.[5]

The bill also imposes various duties relating to transparency, reporting, user identity verification and payment of fees.

The administrative burden on OCPs will be substantial, and the government estimates that OCPs will collectively spend anything from £50 million ($59 million) to £95 million ($113 million) on transition costs, followed by an estimated £290 million ($344 million) in annual costs thereafter.[6]

Investigation, Enforcement and Penalties

The bill appoints Ofcom, the U.K. regulator responsible for regulating communications services, with responsibility for enforcement and oversight of the regime.

It gives Ofcom new criminal investigatory and enforcement powers including the power to compel OCPs to provide information and witnesses to attend interviews. It also gives Ofcom new powers of entry, inspection and audit.[7]

It creates criminal offenses relating to failure to cooperate with Ofcom investigatory measures, and provides for the possibility of joint liability for parent and subsidiary companies in certain cases where Ofcom deems it appropriate.[8]

It will also allow Ofcom to apply to the English courts for business disruption orders, requiring OCPs to withdraw services or, in extreme cases, blocking access to noncompliant OCP services.[9]

The bill stops short of imposing criminal liability on OCPs for failing to comply with their statutory duties, but in such cases Ofcom may impose financial penalties of up to £18 million ($21 million) or 10% of the OCP's qualifying worldwide revenue in the most recent complete accounting period, whichever is the greater.[10]

Where two or more entities are jointly and severally liable for a penalty, the maximum penalty will be the greater of either £18 million or 10% of the qualifying worldwide revenue for the group.[11]

Separately, the bill updates some of the existing communications offices in England and Wales, creating three new communications offenses for:

- Sending online threats and harassment;

- Sending false communications with intent to cause psychological or physical harm; and

- Sending unsolicited sexual pictures and videos.

The purpose of the new offenses is to enhance the protection of vulnerable users and to reduce online

abuse.

The offense of sending false communications will require prosecutors to show that the person sending the message knew at the time of sending that the message was false, and that it was likely to cause nontrivial psychological or physical harm to its audience.[12]

The offense cannot therefore be committed by OCPs whose users publish false information on their platform, unless the prosecution could show that the OCP knew at the time the message was sent that it was false and likely to cause nontrivial psychological or physical harm to its audience.

Public Response

The response to the bill has been varied, with complaints that the bill either does not sufficiently protect vulnerable persons from online abuse and harm, or that it erodes freedom of speech and is too complex and restrictive.

There is no denying that the bill will impose an enormous administrative and financial burden on OCPs.

Further Developments

During the committee stage, opposition to the government proposed a number of significant amendments to the bill, which the Public Bill Committee rejected.

Ahead of the report stage in the House of Commons, which has now been delayed until September at the earliest, further notable amendments have been proposed:

- The Digital, Culture, Media and Sport Committee has tabled amendments to the bill intended to safeguard the independence and integrity of Ofcom by removing the power of the secretary of state to direct or block Ofcom from issuing codes of practice to OCPs before Parliament considers them.[13]

- Further, the government has proposed an amendment that would provide Ofcom with enhanced powers to require, on provision of a notice, companies to use their best endeavors to deploy or develop new technology to address child sexual exploitation content.[14]

- The government has also stated that it will table an amendment to add foreign interference as a priority offense under the bill to strengthen internet safety laws to fight Russian and hostile state disinformation.[15]

On July 6, Ofcom noted that it expects firms to start preparing for the implementation of the bill now and set out a road map for Ofcom's role going forward, including a 100-day plan after the bill passes in order to get the online safety regime up and running.[16]

The impending change in Conservative party leadership may have an impact on the timing and content of the bill. However, it has been reported that government insiders do not anticipate that the delay of the report stage until September will prevent the legislation from being enacted.[17]

While OCPs should expect that there will be further changes to the bill, in our view, the enactment of the bill in some form remains inevitable.

Global Outlook

The U.K. is not alone in legislating to regulate OCPs. In April, the EU agreed the text of a new Digital Services Act, which, similarly to the U.K. bill, aims to increase accountability for online platforms regarding illegal and harmful content.[18]

Separately, the EU has agreed the text of a new Digital Markets Act, which will increase competition by forcing companies who provide browsers, social networks and search engines designated as gatekeepers — in that they have at least 45 million monthly end users and at least 10,000 yearly active business users in

the EU — to allow users greater flexibility in terms of uninstalling pre-installed apps, achieve interconnectivity between different apps and services, and curtailing targeted advertising.[19]

The Digital Markets and Digital Services Acts will be enforced by the European Commission, and are currently awaiting formal approval by the council, later this year, having been approved by the EU Parliament on July 5.[20]

The two acts have both been criticized by some as impeding innovation and creating too far-reaching monitoring systems, while other stakeholders have criticized them for being insufficient to ensure fair competition and protect consumers.

Both acts will have a significant impact on companies falling within their scope; equally effective enforcement will require reorganization and also additional resources for dedicated teams within the European Commission itself. The European Parliament is seeking to increase the budget for that purpose.

European consumer organization BEUC recently commented that:

> Consumers will be better protected online thanks to these new measures, but there is unfinished business when it comes to online marketplaces and the products that are sold on them … The proper enforcement of the DSA will now be crucial to ensure consumers are adequately protected.[21]

Further afield, the U.S. is also making inroads in this area, following criticism that it has historically failed to regulate big platform companies operating in its own backyard.[22]

In February, U.S. senators introduced the Kids Online Safety Act to Congress, seeking to impose a duty on OCPs to prevent the promotion of harmful and criminal activity, and limit exposure to harmful behaviors like suicide, self-harm, eating disorders and substance abuse.

In fact, the U.S. bill goes further than the U.K. bill, in that it will require OCPs to give parents greater control to opt out of data mining and algorithmic recommendations.[23]

Concluding Remarks

Some critics of the EU and U.K. legislators argue that the trend leans toward protectionism but, as the U.S. introduces its own draft legislation at a federal level, that argument is falling away.

The financial costs and administrative burden of complying with the regulatory regime will be significant. The U.K. government intends to raise the funds to cover the costs of regulation in the U.K. from industry in the form of fees.[24]

Add to that the costs of risk assessments, implementation of mitigation measures, transparency reporting and cooperating with regulatory investigations, the financial cost to OCPs will increase sharply as and when these bills become law.

OCPs are already feeling the pinch as investors get nervous about the potential impact of the proposed laws on OCP profitability.

Nevertheless, it is clear that OCP regulation in the near future is a legal certainty, and OCPs would be well advised to start planning for compliance now.

Caroline Black is a partner and Laura Manson and Marjolein de Backer are associates at Dechert LLP.

Dechert partners Alec Burnside and Hayden Coleman and associate Tom Stroud contributed to this article.

[1] Unless specified, all provisions cited are taken from the Online Safety Bill, Bill 4, 53/8.

[2] Section 53.

[3] Online Safety Bill Explanatory Notes, Bill 258-EN ("Explanatory Notes"), paragraph 19.

[4] Part 3, ss 12–16.

[5] Schedule 10, Paragraph 1.

[6] Online Safety Bill Impact Assessment, Full Economic Assessment, Page 2, https://publications.parliament.uk/pa/bills/cbill/58-02/0285/onlineimpact.pdf.

[7] Schedule 11.

[8] Section 161 and Schedule 14.

[9] Explanatory Notes, paragraph 573.

[10] Section 122(4)(1).

[11] Section 122(5)(2).

[12] Section 151.

[13] https://committees.parliament.uk/committee/378/digital-culture-media-and-sport-committee/news/171833/mps-propose-amendments-to-online-safety-bill-to-ensure-ofcom-independence/.

[14] https://publications.parliament.uk/pa/bills/cbill/58-03/0121/amend/onlinesafety_rm_rep_0706.pdf.

[15] https://www.gov.uk/government/news/internet-safety-laws-strengthened-to-fight-russian-and-hostile-state-disinformation.

[16] https://www.ofcom.org.uk/news-centre/2022/tech-firms-should-start-preparing-for-regulation?utm_source=twitter&utm_medium=social.

[17] https://www.ft.com/content/46252e7c-d369-4242-84fe-12bcc63cc67a

[18] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545.

[19] https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users.

[20] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

[21] DMA enforcement needs proper resources, consumer groups say, Official statement from BEUC dated July 5, 2022.

[22] For example see Brookings' online article "U.S. regulatory inaction opened the doors for the EU to step up on internet," March 29, 2022, https://www.brookings.edu/blog/techtank/2022/03/29/u-s-regulatory-inaction-opened-the-doors-for-the-eu-to-step-up-on-internet/.

[23] https://www.protocol.com/bulletins/senate-kids-online-safety-act.

[24] https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response#part-3-the-regulator para 3.21.