COVINGTON

UK Government Plans for an Online Safety Bill

December 17, 2020

UK Public Policy and Tech Regulatory

In April 2019, the UK Government published its Online Harms White Paper and launched a Consultation. In February 2020, the Government published its initial response to that Consultation. In its 15 December 2020 full response to the Online Harms White Paper Consultation, the Government outlined its vision for tackling harmful content online through a new regulatory framework, to be set out in a new Online Safety Bill ("OSB").

This development comes at a time of heightened scrutiny of, and regulatory changes to, digital services and markets. Earlier this month, the UK Competition and Markets Authority published recommendations to the UK Government on the design and implementation of a new regulatory regime for digital markets (see our update here).

The UK Government is keen to ensure that policy initiatives in this sector are coordinated with similar legislation, including those in the U.S. and the EU. The European Commission also published its proposal for a Digital Services Act on 15 December, proposing a somewhat similar system for regulating illegal online content that puts greater responsibilities on technology companies.

Key points of the UK Government's plans for the OSB are set out below.

Proposed Scope of Application

- The legislation will apply to companies:
  - whose services host user-generated content that can be accessed by users in the UK; and/or
  - that facilitate public or private online interaction between service users, one or more of whom is in the UK.
- The legislation will impose a duty of care on a broad range of services including, but not limited to:
  - Social media services; consumer cloud storage sites; video sharing platforms; online forums; dating services; online instant messaging services; peer-to-peer services; video games which enable interaction with other users online; and online market places.
  - Search engines.

  - User-generated content encompassing organic and influencer ads posted on social media platforms or other services (including images or text posted from users' accounts to promote a product, service or brand, and which may or may not be paid for).
- Although services that play merely a functional role in enabling online activity, such as internet service providers, will be exempt from the duty of care, they will have duties to cooperate with the regulator on business disruption measures.
- The legislation will exempt the following services from scope:
  - Any service where the risk of harm is sufficiently low that regulatory requirements would be disproportionate.
  - Advertisements placed on an in-scope service via a direct contract between an advertiser and an advertising service.
  - Business-to-business and email services.
  - Content published by a news publisher on its own site (e.g. on a newspaper or broadcaster's website) and user comments on that content.
  - Harms resulting from: breaches of intellectual property rights; breaches of data protection legislation; fraud; breaches of consumer protection law; or cyber security breaches or hacking.

Different Expectations Depending on Activity

The OSB will establish a two-tier system that distinguishes between obligations that apply to companies that offer "Category 1 services" and those that offer "Category 2 services," with more onerous requirements on companies that offer Category 1 services.

[NB The Government anticipates that most services will be Category 2 services.]

Whether a service falls into Category 1 will be determined through a three-step process:

- Primary legislation will set out the relevant factors—the size of a service's audience and the functionalities it offers (e.g., ability to share content widely).
- Ofcom will provide advice to the Government on thresholds for each factor. On the basis of that advice, the Government will determine and publish thresholds for each of the factors.
- Ofcom will assess and publish a register of all of the services which meet the required thresholds. (If a company believes its service has wrongly been designated as Category 1, then it can appeal to an appropriate tribunal.)

Ofcom will advise the Government if it considers a threshold change is necessary.

Definition of Harmful Content

- The OSB will set out a general definition of the harmful content and activity that is in scope of the regime.
- A limited number of priority categories of harmful content will be set out in secondary legislation, which will cover:
  - criminal offences (including child sexual exploitation and abuse, terrorism, hate crime and the sale of illegal drugs and weapons);
  - harmful content and activity affecting children (such as pornography and violent content); and
  - harmful content and activity that is legal when accessed by adults but may be harmful to them (such as abuse and content about eating disorders, self-harm or suicide).
- The legislation does not define what constitutes harmful content, and leaves ambiguity about online material that, while legal, may still be problematic (including, for example, whether the promotion of self-harm should be made illegal).

Duties on Companies

- All companies will be required to take action with regard to illegal content and activity.
- All companies will be required to assess the likelihood of children accessing their services. If they assess that children are likely to access their services, they will be required to provide additional protections for children using them. This may include recommending the use of age assurance or verification technologies. [NB the process for enforcing this requirement is unclear.]
- All companies will have additional duties beyond the core duty of care, including providing mechanisms to allow users to report harmful content or activity (such as reporting child sexual exploitation and abuse identified on their services to a designated body) and to appeal the takedown of their content.
- All companies will be required to address disinformation and misinformation that poses a reasonably foreseeable risk of significant harm to individuals (e.g., relating to public health). Where disinformation and misinformation present a significant threat to public safety, public health or national security, the regulator will have the power to act.
- Only companies that offer Category 1 services will be required to take action with regards to legal but harmful content and activity accessed by adults.
- Category 1 companies will be required to assess the reasonably foreseeable risk of causing significant physical or psychological harm to adults.
- Category 1 companies will be required to make clear what type of “legal but harmful” content is acceptable on their platforms in their terms and conditions and they will be responsible for transparent and consistent enforcement.
- Category 1 companies will be required to publish transparency reports containing information about the steps they are taking to tackle online harms on those services. The Secretary of State will have the discretionary power to extend this obligation to companies beyond Category 1 companies.

Role and Duty of Ofcom

- The Government has confirmed that Ofcom will be the online harms regulator.
- Ofcom will have the power to impose fines of up to £18m, or 10% of global revenue (whichever is higher), on companies for failing to stop illegal and harmful content from reaching their online users.
- Ofcom will have the power to enforce the fines and will have the power to block non-compliant services from being accessed in the UK.
- If the deterrent of fines and other punishments does not work, Ofcom will have the power to impose criminal sanctions against senior managers for repeat offences.
- Ofcom will also have a range of specific powers, including (but not limited to):
  - establishing codes of practice for companies;
  - requiring companies to use automated technology to identify illegal child sexual exploitation and abuse or terrorist content or activity on their services, including, where proportionate, on private channels; and
  - intervening if disinformation and misinformation present a significant threat to public safety, public health or national security.
- Ofcom will set out how companies can fulfil their duty of care in codes of practice, including with regards to private communications and limiting the ability for anonymous adults to contact children. Ofcom will consult on the content of the codes.
- If the deterrent of fines and other punishments does not work, Ofcom will have the power to impose criminal sanctions against senior managers for repeat offences.
- Ofcom's costs will be paid by companies falling under the scope of the law, above a (yet to be determined) threshold based on global annual revenue.

What is not Envisaged in the OSB

The UK Government has expressly reserved some elements from the OSB:

- Any requirement to force services to break their encryption to reveal the contents of messages.
- Any requirement to retain child sexual exploitation and abuse data [NB the government is considering whether to introduce this requirement through alternative legislation].
- Any requirement for companies to retain data relating to terrorist content and activity—although the government expects companies to report to law enforcement where they consider there is a threat to life or risk of imminent attack.

Next Steps

- The text of the OSB is expected to become available in 2021, and we anticipate that it will enter into law in the second half of the year.
- The Government expects the Law Commission to produce recommendations concerning the reform of the criminal offences relating to harmful online communications (for example, cyber-flashing and 'pile-on' harassment) in early 2021. The Law Commission is currently consulting on its proposals.
- The Secretary of State will undertake a review of the effectiveness of the regime 2-5 years after its entry into force.
- The Government will produce voluntary best practice guidance for internet infrastructure service providers that is separate from the online harms regime.
- The Government will publish Interim Codes of Practice to provide guidance for companies on tackling terrorist activity and online child sexual exploitation prior to the introduction of legislation.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Public Policy and Government Affairs practice:

Thomas Reilly	+44 20 7067 2357	treilly@cov.com
Marty Hansen	+44 20 7067 2239	mhansen@cov.com
Lisa Peets	+44 20 7067 2031	lpeets@cov.com
Sam Choi	+44 20 7067 2054	jchoi@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.