ALLEN & OVERY

UK government publishes details of digital regulation to combat 'Online Harms'

20 January 2021

On 15 December 2020, the UK government published its long-awaited proposals "to make the UK a safer place to be online" through its final response to the Online Harms White Paper. Proposing a new regulatory framework for online companies, it targets a wide range of illegal or harmful content affecting individual users. Committing to introducing the Online Safety Bill in 2021, the proposals would mark the end of the "era of self-regulation", instead placing significant legal and practical responsibility on online companies.

Having launched the Online Harms White Paper in April 2019, calls for details of the government's final proposals intensified over 2020 as increasing aspects of everyday life were conducted online during the Covid-19 pandemic. However, this is just one aspect of the current wave of international digital regulation, with the UK Digital Markets Taskforce recently publishing its recommendations for a new regime in the UK to govern the behaviour of digital firms with market power and the European Commission releasing its Digital Services Act package, also on 15 December 2020.

In this article, we consider the key provisions in the government's final consultation response and outline the next steps on the road to regulation.

Speed read

– The regime will apply to companies anywhere in the world whose services host user-generated content and/or facilitate public or private online interaction between users, which can be accessed by users in the UK, as well as to search engines. There will be a differentiated expectation on companies depending on their size and scope of their activities.

– At the heart of the proposals is a new duty of care on companies to improve the safety of their users online. However, the proposed "*proportionate and risk based*" regulation is essentially one of systems and controls – the government's intention is that online platforms should have appropriate systems and processes in place to protect users, and that action should be taken against them if they fall short.

– Ofcom has been confirmed as the regulator for online harms in the UK, building on its experience of its role regulating TV and radio programmes and video sharing platforms established in the UK. Its running costs will be paid by certain in-scope companies.

– Ofcom will have a broad range of powers to enforce compliance with the duty of care, including issuing fines of up to 10% of a company's annual global turnover or GBP18 million, whichever is higher, and imposing business disruption measures.

– A draft Online Safety Bill is expected during 2021, so legislation could still be some time off by the time that the draft Bill passes through Parliament. In the meantime, companies within scope should give thought to how the new rules would apply to them, including compliance with voluntary interim Codes of Practice published by government on how to tackle online terrorist and child sexual exploitation and abuse content and activity.

Background to the Online Harms White Paper and final consultation response

The Online Harms White Paper acknowledged the various voluntary initiatives by industry to tackle online illegal and harmful activity but noted that the government felt it necessary to intervene to drive further behavioural change. In its full consultation response, the government also focused on the effects of Covid-19 which it said shone a spotlight on the risks posed by harmful activity and content online, particularly regarding disinformation and misinformation, and the risks posed to children online.

The government cites a lack of public confidence in online safety and aims to set a global benchmark by introducing a single regulatory framework for the UK. As regulator, it is said that Ofcom will take an international approach, working with other international regulators, to ensure effective enforcement and promote best practice at a global level. Particular reference is made to broadly similar recent online safety proposals in Australia and Ireland, as well as the European Commission's Digital Services Act package.

What services and companies are in scope?

The scope is fairly wide and, controversially, extra-territorial. It will apply to companies whose services host user-generated content which can be accessed by users in the UK and/or facilitate public or private online interaction between service users, one or more of whom is in the UK. It will also apply to search engines.

In practice, this covers a broad range of services provided by companies anywhere in the world. Some of the largest internet platforms and social media companies that are clearly within scope have already been engaging with the government's proposals, but the breadth of the new framework means that many other businesses, who may not have expected to be caught by the legislation, are also in scope. This includes 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 users online, and online marketplaces.

However, there are some notable exceptions eg for internet service providers, business to business services, email services, news websites (including "below the line" comments on news articles) and lower-risk services such as reviews and comments on retail websites. These exemptions are said to be driven by a desire to protect freedom of speech and an approach which is proportionate which the risk posed by certain businesses.

The government believes that less than 3% of UK businesses will be in scope, with the vast majority being "Category 2 services" considered below.

What duties are imposed on online companies?

All in-scope companies will have a duty of care towards their users, supplemented by various Codes of Practice issued by Ofcom explaining what is required to fulfil the duty of care in practice.

The duty involves a tiered approach depending on whether in-scope companies provide "Category 1 services" (a small group of high-risk, high-reach services with the largest online presence) or "Category 2 services" (the remainder), with the majority expected to be Category 2. Designation will determined on a threshold basis by reference to companies' size and activities, with details yet to be published.

The tiered approach recognises the focus on illegal content and protecting children at the heart of the proposals:

– **Illegal content:** All companies will be required to take action with regard to relevant illegal content and activity. Priority offences, which pose the greatest risk of harm, will be identified in secondary legislation, such as child sexual exploitation and abuse and terrorism. For these offences, companies will need to consider what systems and processes are necessary to identify, assess and address the harms and, more controversially, may be required to proactively identify (such as through use of automated technology) and block or remove this type of illegal material if other steps have not been effective and provided safeguards are in place.

– **Legal content harmful to children:** All companies will be required to assess the likelihood of children accessing their services. If likely, they will be required to provide additional protections for children using them, including regarding legal but harmful content. Priority categories of harmful content will be identified in secondary legislation and are likely to include cyberbullying and access to age-inappropriate content such as online pornography. Companies will be required to undertake regular child safety risk assessments to identify legal but harmful material on their services impacting children and to assess the risks that material on their services poses, as well as putting in place age-appropriate protective measures.

– **Legal content harmful to adults:** Only companies with Category 1 services will be required to take action with regard to legal but harmful content accessed by adults. Again, priority categories will be set out in secondary legislation and are likely to include content promoting self-harm or eating disorders, hate content, online abuse, and disinformation and misinformation that could cause harm to individuals, such as anti-vaccination content. Affected companies will have to undertake regular risk assessments to identify such harmful material on their services and their terms and conditions will have to explicitly address how they will handle the material. These companies will not be required by law to remove such content, unless they do so because it breaches their terms and conditions, but they must consider the impacts of their decisions regarding moderation and design choices on user safety.

– **Transparency reporting:** Companies with Category 1 services will need to produce transparency reports containing information about the steps they are taking to tackle online harms. Further details on the reporting requirements will be published by Ofcom in due course, building on the recommendations of a multi-stakeholder Transparency Working Group, including representatives from civil society and industry, set out in the government's Report on Transparency Reporting in relation to Online Harms[1] published alongside its full consultation response.

– **Appeals mechanisms:** All companies will be required to have effective and accessible user reporting and redress mechanisms. They will also be required to have mechanisms for users to report broader concerns about a company's compliance with its duties, including by reporting their concerns to the regulator. However, the regulator will not investigate or decide on individual cases.

Further details on how companies can fulfil the duty of care will be provided in Codes of Practice to be published by Ofcom. These should take into account the nature of the affected service and what the duty requires in that context. For example, for services where users can expect a greater degree of privacy, such as private communication channels, it is said that more emphasis may be placed on safety by design measures such as limiting the ability for anonymous adults to contact children. Similarly, consideration should also be given to how freedom of expression can be protected in the context of the duty of care.

Obligations with respect to certain harms are specifically excluded from the new rules, including harms suffered by companies, and financial harms such as fraud. To avoid duplication, the government has also excluded harms which are addressed by other legislative regimes such as data protection, consumer protection or the protection of IP rights. As anticipated in the white paper, the proposals do not provide for election law reform. While disinformation is an aspect of online harms, specific changes to the regulation of online political campaigning and advertising are not addressed in the new regime.

It is also worth noting that the government has said that it may use the proposed legislation in this area also to address the outcome of the Law Commission's ongoing work on the reform of criminal offense relating to harmful content in online communications, whose recommendations are expected in early 2021. If so, then the scope of relevant illegal content within the online harms framework may expand further.

[1] https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/government-transparency-report

Role of Ofcom as regulator

Ofcom's primary duty under the new regime is to improve the safety of users of online services. In practice, this means that it will set Codes of Practice, establish a transparency, trust and accountability framework and require all in-scope companies to have effective and accessible mechanisms for users to report concerns. It will also have a legal duty to pay due regard to innovation, comparable to its existing obligation under the Communications Act 2003. Ofcom has said that it will set out its thinking on its approach to regulating online harms during 2021.

Although its stated aim is to secure compliance through engagement with industry, Ofcom will be given significant enforcement tools to deploy in line with its promise of a proportionate and risk-based approach to enforcement. These include:

– **Non-financial sanctions**: Issuing directions for improvement and notices of non-compliance.

– **Fines:** Issuing fines of up to 10% of a company's annual global turnover or GBP18m, whichever is higher. This exceeds the already significant maximum fines under the GDPR of the higher of 4% of global turnover or EUR20m (GBP17.5m in the UK from 1 January 2021).

– **Business disruption measures:** As a measure of last resort, Ofcom will be able to take measures to disrupt a company's business activities in the UK, including (after obtaining a court order) blocking access to services in the UK in the most serious circumstances.

– **Future potential for senior manager liability:** The new law will provide for the possibility of future secondary legislation (not for at least two years after the regulatory framework comes into effect) to impose criminal sanctions on senior managers. This will be introduced as a further measure of last resort, and only if industry is considered to have failed to meet their responsibilities under the regime.

In support of its enforcement activity, Ofcom will have powers to enter companies' premises and access documentation, data and equipment and to interview employees, where there are reasonable grounds to suggest that a company may be non-compliant.

Companies and individuals will have the right to challenge Ofcom's decisions under a statutory appeals mechanism to an appropriate (but as yet unnamed) tribunal, on the basis of judicial review principles.

Given the extra-territorial effect of the new regime, enforcement in an international context will undoubtedly be a challenge. Due to concerns that it might have a detrimental effect on smaller businesses, companies will not be required to nominate UK or EEA representatives to assist with enforcement action and instead the government is relying upon intended cooperation with international regulators and law enforcement.

The rules will not introduce express new rights for individuals to sue companies. However, the government is alive to (and indeed encouraging of) the possibility that a statutory duty of care may help individuals bring private law claims eg for negligence. The White Paper envisaged that a statutory regime may help establish the relevant duty of care and demonstrate a causal link between the online companies' activities and harm suffered by users, and the government's final response acknowledged that users can use public regulatory decisions as evidence in legal actions. While the practical effect of this remains to be seen, the possibility of follow-on actions after a finding of regulatory breach cannot be excluded.

Commentary

While a statutory duty of care is not itself a new concept and has been used with success in (for example) health and safety and occupiers' liability legislation in the UK, its efficacy depends on what it actually requires. Companies need clarity and Ofcom's Codes of Practice will have to provide sufficient transparency and predictability in practice. Any ambiguity risks placing a number of difficult balancing decisions at the doors of the internet companies themselves. Given the potentially serious sanctions for breach, there is concern that this will lead to over blocking of content or have a deterrent effect on innovation or new entrants.

Although broadly consistent with its earlier proposals, the government's final response to the Online Harms White Paper does take on board certain concerns raised by industry and commentators. For example, in its approach to enforcement, the government has rowed back on the suggestion that internet service providers could voluntarily choose to block websites or apps of companies in breach.

However, some early criticism remains, such as precisely what legal but harmful content entails. Further clarity is anticipated in draft legislation and it will be important for the government to set clear definitions that can be applied across the industry.

Next steps

The government has committed to publishing the draft Online Safety Bill that would give effect to the new proposals during 2021. There is also important secondary legislation and Ofcom guidance required to bring the framework into effect. Given the current Conservative majority and broad cross-party support for the initiative, it is likely that these measures will approved with relativity little resistance.

Although new law is still some time off, the Online Harms White Paper was intended to be an immediate call to action for companies to tackle harmful content or activity on their sites. In-scope companies should consider their processes and procedures in light of the proposed new rules, and have regard to the principles of the proposed safety by design framework when developing new products and services. In particular, companies likely to provide Category 1 services could consider how the transparency regime may still alongside any existing transparency reporting, and all companies should have regard to the voluntary interim Codes of Practice published by government on online terrorist and child sexual exploitation and abuse content and activity.

Author

Maeve Hanna
Senior Associate
Tel +44 20 3088 1844
maeve.hanna@allenovery.com