

Policing the Digital Space – New Rules Require Platforms to Take Responsibility for Users’ Content

January 27, 2023 – The TMCA

by Ron Moscona and Tessa Adams



Related People

- Ron Moscona

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

Since the emergence of the Internet, under current European Union rules, services that host user-generated or user-contributed content have enjoyed legal immunity from liability, provided they take down unlawful content once notified of it. This existing regime gave online platforms, such as search engines, social media platforms, e-commerce sites and numerous other digital services, the freedom to determine their own rules on how their services can be used and – most importantly – the freedom to decide to what

extent they wished to enforce their terms and conditions and user policies. This hands-off approach is now set to change dramatically with the introduction of new regulatory frameworks in the European Union and the United Kingdom for the operation of digital platforms designed to protect users from unlawful and unsafe content, which means significant new compliance obligations for the operators of such services.

Each of the UK and the EU have recently produced new regimes for combatting online harm and protecting the safety of online users. In the EU, the Digital Services Act (**DSA**) has been accepted as law and will come into force in February 2023. While the UK's parallel Online Safety Bill (**OSB**) is still the subject of parliamentary debate, it is also expected to become law in April 2023 and intends to make the UK the "safest place in the world to be online".

These new regimes will drastically change the way digital platforms need to regulate their services and reduce online harm to users. They consist of wide-reaching measures designed to minimize unlawful content and to protect children in particular from harm online, and will introduce a serious compliance burden on any online platform, regardless of size, provided it has more than a negligible UK or EU presence. The laws will apply to almost all social media and content sharing platforms. The overall intention of the regimes is to minimize the presentation of harmful content to users by placing a duty of care on the providers of that content. Once in force, it is hoped these will create a safer environment for internet users, but this will come at a cost of more onerous obligations for platforms that host user-generated content, and harsh penalties if they do not comply.

These new regulatory frameworks will supplement, rather than replace, the existing rules that have governed content dissemination in both the UK and the EU since 2000 and which provide hosting services with immunity from liability for user-contributed content (subject to take-down obligations). Platforms will continue to enjoy legal immunity in respect of content posted by users; however, regulatory obligations will now require service providers to take proactive measures to keep their platforms lawful and safe rather than simply respond to takedown obligations initiated by others. For businesses operating online, understanding the applicability of the legislation and the obligations imposed will be very important: large fines, business suspension and even imprisonment can result.

Territorial application of the legislation

Importantly, the new regimes extend to businesses outside of the UK and EU. The obligations apply regardless of the place of establishment of the company running the service, instead focusing on the location of its users. The UK's OSB will apply to services that have "links with the UK" – meaning a "significant number" of UK users – or those where the UK is a target market. Similarly, the EU's DSA applies insofar as a platform offers services with a "substantial connection" to the EU, and notably requires such businesses having no establishment in the EU to appoint a legal representative there (who, where necessary, would be the target of regulatory enforcement action and liable for the service provider's failures to meet its regulatory obligations).

Types of digital services covered

The OSB covers search engines and any user-to-user platform, which has a wide definition, encompassing any online service that allows user-generated content to be shared between users. This will extend to any app or website that has this functionality, such as those that allow users to talk with each other through messaging, comments and forums, as well as those that host users' images, videos and other content. This means, for example, that certain online games and storage platforms may be covered, as well as the obvious messaging and content sharing apps and sites. The only platforms exempted are those that allow solely for emails, SMS, MMS and voice calling functionality, and this exemption does not extend to over-the-top messaging apps like WhatsApp. There are also exemptions for recognized news publisher content, and for sites where the only user-to-user content posted is in the form of comments or reviews.

Under the DSA, search engines and intermediary services that are simply hosting, caching or functioning as a mere conduit, have some obligations. But, similar to the UK's OSB, the most onerous obligations under the EU legislation are placed on those services that are deemed "online platforms", being those that host and disseminate user content such as marketplaces and social media platforms.

Each of the two regulatory regimes in the UK and the EU imposes additional obligations on the largest platforms: services deemed "high risk and high reach" under the OSB will have additional duties, such as having to provide users with empowerment tools and the option to verify their identity. Under the DSA, "very large online platforms" having 45 million users or more in the EU will have additional obligations. For smaller platforms, duties are less onerous; in line with this, the OSB applies a concept of proportionality in which measures required to be taken to comply with obligations will be proportionate to the risk level, size and capacity of the service provider.

Key obligations imposed

The duties relate mainly to illegal content and content harmful to children, and involve conducting risk assessments, having appropriate systems and processes in place, taking action in relation to illegal or harmful content, keeping records and reporting to the regulator. Importantly, these will need to be undertaken extensively and properly, and there is a duty to publish risk assessments or transparency reports under both regimes. Regulatory oversight will be applied to ensure the services discharge their duties in accordance with guidelines and policies to be developed in due course by the national regulators (in the UK and in EU member states).

With respect to illegal content posted on platforms under the OSB, service providers will need to carry out an assessment to understand the risks of such content being presented on their platform. A large focus of the OSB is on child sexual exploitation and terrorism content, but the duties relate to any criminal offence where the victim is an individual (with a few exceptions). Platforms must take proportionate measures to mitigate and manage the risk of such content, and must have systems in place to minimize the exposure of users to illegal content, allow users to report the content and have

processes ensuring it is swiftly taken down. There is also a duty to report UK-linked child sexual offences to the National Crime Agency.

Under the DSA, all online platforms are obligated to remove content that is illegal in any EU Member State, suspend accounts that disseminate such illegal content, and report criminal offences. Very large online platforms need to produce an annual risk assessment and independent audit, have risk mitigation measures in place, and appoint a compliance officer for illegal content obligations.

Platforms that are likely to be accessed by children have additional obligations that extend beyond strictly illegal content, and each service provider must assess whether the platform is likely to be accessed by children. Under the OSB, platforms likely to be accessed by children need to carry out a children's risk assessment for harmful content. Obvious examples are pornographic and violent content, but this could also extend to things like cyber bullying, self-harm promotion, or content about eating disorders, as well as anything that risks causing a child psychological or physical harm. The platform must implement proportionate measures to mitigate and manage the risk of harm to children to prevent them from encountering the harmful content. These include having proper age assurance mechanisms in place. Related to this, there is a specific provision requiring services that publish pornographic content to prevent children from accessing it, again, likely through age verification measures.

In the case of the DSA, platforms "accessible to minors" must have appropriate measures in place to ensure that minors have a high level of privacy, safety and security. Specific obligations are not listed in the same way as they are in the UK Bill, so operators of services will need to assess and limit the risks their platforms pose to children. Best practices for doing this are expected to be developed over time by regulators and quite likely by the industry itself.

As originally proposed, the OSB outlined duties in relation to the management and mitigation of legal but harmful content to adults. The UK government recently announced that those duties have been dropped from the bill following political controversy not only over the fact that it is a heavy obligation to monitor legal but harmful content, but also over freedom of expression concerns. By comparison, under the DSA, there is no general duty on platforms to mitigate against harmful content to adults which is not unlawful. However, very large online platforms will have a risk assessment duty requiring them at least once a year to identify, analyze and assess "systemic risks" coming from their service regarding not only the dissemination of illegal content, but also serious harm to physical and mental wellbeing and to society in general.

Consequences

The OSB will be overseen by the UK's communications regulator, OFCOM, which will have a range of powers to address non-compliance, including applying to the courts for an order that a business be blocked for use in the UK in cases where urgent action is required. Such an order is temporary but can be made permanent, and can require internet service providers, search engines and app stores to block the platform or take it

down. In addition, fines of up to the greater of £18 million or 10% of the business's annual revenue can be imposed. OFCOM will also have rights of entry and inspection and can request information at any time; a failure to comply with such a request, or the deliberate withholding or destroying of information, can result in the imprisonment of a senior manager.

Under the DSA, each EU Member State will designate a competent authority to ensure compliance. The national regulators will be empowered to interview operators, carry out inspections, access data, request documents and information, and carry out searches and seizures. Again, in urgent situations, restriction of access can be ordered. The regulator can order a cessation of DSA infringements, and impose fines of up to 6% of annual turnover.

How to prepare

Preparation for compliance with the new regulatory regimes is essential for all affected digital platforms. The DSA will come into force on 17 February 2023, with most providers needing to publish an initial statement of usage by that date but otherwise having a one-year general grace period to comply with their remaining obligations. However, those that the regulator designates as “very large online platforms” will only have four months from such designation to comply. The OSB is likely to pass in April 2023; if it is delayed further than this, under Parliament rules, the bill will need to be dropped entirely and the legislation process will have to be restarted, which is something the Government will want to avoid.

To help service providers comply with the OSB, OFCOM will publish Codes of Practice within three months of the Bill becoming law that can be taken as authority for compliance purposes. In practice, compliance with the regimes will likely involve developing and/or operating automated tools and algorithms, specialty compliance staff, secondary manual review systems, age assurance processes, user control mechanisms, policies, transparency, audits and record keeping. In the meantime, it is prudent for digital service providers to assess whether the OSB and DSA apply to their business, to prepare to implement such systems and processes, and to assess and adapt their existing systems and policies relating to user-generated content for risk.