LEWIS SILKIN

The Online Safety Act

Inside

The Online Safety Act introduces a new regulatory regime to address illegal and harmful content online. We are seeing more and more scrutiny in this area, with Australia, Ireland and the EU already passing new legislation, including the EU's Digital Services Act.

Under the Online Safety Act, companies in scope will have to put in place systems and processes to improve user safety. Ofcom will be the appointed regulator in the UK to enforce the Act. The focus of the Act is not on Ofcom moderating individual pieces of content, but on tech companies pro-actively assessing risks of harm to their users and putting in place systems and processes to keep them safer online. The Act extends and applies to the whole of the UK, except for some of the criminal offences which apply differently within the home nations.

What companies are in scope?

The Act imposes legal requirements on:

- providers of internet services which allow users to encounter content generated, uploaded or shared by other users;
- providers of search engines which enable users to search multiple websites and databases; and
- providers of internet services which publish or display pornographic content (meaning pornographic content published by a provider).

As well as UK service providers, the Act applies to providers of regulated services based outside the UK where they fall within scope of the Act, for example, because such services target the UK, or they have a significant number of UK users.

Companies in scope will either be categorised either as "Category 1" services or "Category 2" services where Category 1 services will include the largest platforms with the most users and will be subject to more onerous obligations.

Does the Act affect my business?

Its scope goes well beyond the obvious 'Big Tech' social media platforms and search engines, and it is likely to encompass thousands of smaller platforms, including websites, platforms, and online forums where information can be shared, where advertising is served, or where users might interact with other users.

What does the legislation require?

Platforms will be required to:

- remove illegal content quickly or prevent it from appearing in the first place. This includes content under offences designated as priority offences in the Act, such as immigration and modern slavery;
- prevent children from accessing harmful and age-inappropriate content (such as, pornographic content, online abuse, cyberbullying or online harassment, or content which promotes or glorifies suicide, self-harm or eating disorders);
- enforce age limits and implement age-checking measures;
- ensure the risks and dangers posed to children on the largest social media platforms are more transparent, including by publishing risk assessments; and
- provide parents and children with clear and accessible ways to report problems online when they do arise.

In relation to adult protections, Category 1 services will be required to facilitate a so-called "triple shield". Platforms will need to remove all illegal content, remove content that is banned by their own terms and conditions, and empower adult internet users with tools so that they can tailor the type of content they see and can avoid potentially harmful content if they do not want to see it on their feeds. Children will be automatically prevented from seeing this content without having to change any settings.

Category 1 services will also be required to prevent paid-for fraudulent adverts appearing on their services. They will also have a duty to protect journalistic content, news publisher content and content of democratic importance.

Criminal offences

The Act also creates new offences, such as:

- The false communications offence, aimed at protecting individuals from any communications where the sender intended to cause harm by sending something knowingly false.
- The threatening communications offence, to capture communications which convey a threat of serious harm, such as grievous bodily harm or rape.
- Flashing offence, aimed at stopping epilepsy trolling.
- Criminalising assisting or encouraging self-harm online.

What happens if companies do not comply?

Ofcom will:

- be able to require companies not meeting their obligations to put things right, impose fines of up to £18 million or 10% of global annual turnover (whichever is higher) or apply to court for business disruption measures (including blocking non-compliant services);
- be able to bring criminal sanctions against senior managers who fail to ensure their company complies with Ofcom's information requests, or who deliberately destroy or withhold information, or against executives whose companies do not comply with child protection rules under the Act;
- have a range of powers to gather the information it needs to support its oversight and enforcement activity;
- be able to make companies change their behaviour, by taking measures to improve compliance, including to use proactive technologies to identify illegal content and ensure children aren't encountering harmful material; and
- help companies to comply with the new laws by publishing codes of practice, setting out the steps companies should take to comply with their new duties. Companies will either need to follow these steps or show that their approach is equally effective (the government says that it expects Ofcom to work collaboratively with companies to help them understand their new obligations and what steps they need to take to protect their users from harm).

How should my organisation prepare for the new regime coming into force?

Organisations should carefully consider if they come within the scope of the Act, bearing in mind its wide scope of application. Indeed, most companies that provide online content are likely to be caught by its provisions. If that's the case, here are some practical steps your organisation should take:

- carry out a risk assessment of your operations and websites, and review complaints procedures and terms of service;
- set up and consider improvements to your systems for monitoring all content, and how to balance freedom of expression with the need to protect users from harm;
- consider internal systems for spotting and reporting potential harm to children to the National Crime Agency;
- assess if you might be classified as a Category 1 service and therefore be required to comply with the extra obligations imposed; and
- keep an eye on Ofcom's activities, as it prepares to regulate the Act and consults on various aspects.

The Act received Royal Assent in October 2023 and Ofcom has now published a timeline of the actions it intends to take to prepare for regulation. The Act will not take effect until the Secretary of State has made secondary legislation to implement the Act, and Ofcom has published the relevant codes of practice.

For more information please contact:

Geraint Lloyd-Taylor
Partner

+44 (0)20 7074 8450
geraint.lloyd-taylor@lewissilkin.com

LEWIS SILKIN

Arbor, 255 Blackfriars Road,
London, SE1 9AXT
+44 (0)20 7074 8000
www.lewissilkin.com