The Safety Net – Enforcement

Nowhere to hide? Ofcom's powers and obligations under the OSA

The OSA contains complex and far-reaching obligations in relation to a variety of online platforms. While on one hand, the OSA attempts to maintains a proportionate and risk-based approach to enforcement, it does contain some incredibly wide-ranging and probing investigatory and enforcement powers. That's where Ofcom, the regulator responsible for overseeing and enforcing the regime, comes in. This article explores what powers it holds and how it intends to use them.

Risk based approach

Ofcom has been clear that it does not intend to be overly intrusive with its enforcement efforts under the OSA. Instead, it will work with companies as far as possible, including through a stipulated supervisory regime (several larger online platforms are already engaging with Ofcom in this regard, with some having received fines under the existing VSP regime), and will take "targeted" and "proportionate" measures against non-compliant companies, in-line with a risk-based approach. This will be welcome news for industry, with Ofcom also clarifying that it will only make use of its most far-reaching powers under the OSA in relation to the most egregious online harms or where particular groups e.g., children, are particularly at risk. It also mirrors the approach under other similar technology laws, including the GDPR. Having said this, as Ofcom has not regulated specifically on online safety before, there is limited precedent in terms of the enforcement approach that the regulator may take and therefore a good deal of uncertainty remains.

Resources

Ofcom has outlined in its roadmap that it will have several means of driving improvements in online safety. The first of these is to provide resources to help companies understand and manage risk. These resources will include: commissioning research into specific online safety topics e.g., children's mental health online; analysing the cause and impacts of online harms; providing guidance (on a range of topics from protecting women and girls to freedom of expression); and drafting codes of practice, which will explain what services can do to mitigate against certain online harms. Importantly, the codes of practice will operate as a "safe-harbour" whereby if an organisation can demonstrate compliance with the relevant code of practice, it will be presumed to be compliant with the OSA, as well. Many of these resources have been published in draft form, with the first illegal harms guidance and codes now published in final form.

Aside from this, Ofcom will be required to set up advisory committees to deal with issues relating to media literacy, disinformation and misinformation. It must also publish an annual report.

Regulatory supervision

Interestingly, the OSA provides Ofcom with certain powers that appear to replicate those held by Ofcom's colleagues in the Digital Regulation Cooperation Forum or DRCF under relevant legislation (including the Financial Conduct Authority or FCA). For example, Ofcom will engage with the "largest and riskiest services" via what it calls "continuous regulatory supervision" - this mirrors certain powers held by the FCA. This approach centres on maintaining pro-active communication with online platforms to improve online safety measures on a rolling basis. SMEs may also benefit from this kind of supervision.

Enforcement process and notices

While Ofcom's preference is to encourage voluntary compliance with the OSA through providing resources and supervision, if necessary, it will launch investigatory and enforcement actions.

Ofcom has published, in its guidance on enforcement, how the enforcement process will work from start to finish. Ofcom will undertake an initial assessment where infringements of the OSA are alleged. If these

allegations appear to have some merit, a formal investigation may be launched. If the case is not closed post investigation, then a provisional notice of contravention will be issued, at which point the parties may provide representations and take actions to address Ofcom's concerns. Ofcom will consider these representations (and may even publish a further provisional notice allowing for additional representations by the parties) before publishing a so-called "confirmation decision". This decision can include a penalty or any other enforcement steps – discussed further below.

Importantly, Ofcom announced, on 3 March 2025, its enforcement programme to assess industry compliance with the first set of illegal harms duties under the OSA. See our Illegal Harms explainer article for more information. As part of this, Ofcom issued notices to certain online providers – including large platforms and smaller sites that may present particular risks to users, requiring them to submit their illegal harms risk assessments by **31 March 2025**, stating that they would risk enforcement action if they failed to do so.

Investigation powers – in more depth

The OSA contains an entire chapter of provisions setting out Ofcom's information gathering powers when investigating a potential infringement under the OSA. These include a general power to ask companies to provide "any information" that it requires for the purpose of exercising, or deciding whether to exercise, any of its online safety functions. Specific information notices may also be issued to companies under defined circumstances – including those that allow Ofcom to request information relating to a deceased child's social media account if requested to do so by a coroner investigating the child's death.

Further, Ofcom may commission reports by "skilled persons" to shed light on failures or possible failures of companies to comply with a requirement under the OSA – this is also a concept employed by other DRCF regulators including the FCA. Ofcom also has general powers in the context of investigations to enter, inspect and audit business premises – including under certain circumstances – with just a notice (i.e., no warrant is required). The regulator may also require interviews with the services provider's staff.

Enforcement powers – in more depth

Fines

Where Ofcom identifies compliance failures, it can impose fines of up to £18 million or 10% of qualifying worldwide revenue (whichever is greater). Ofcom is currently consulting on fees and penalties, with regulations governing the calculation of qualifying worldwide revenue coming into force throughout 2025 (please see our article on this consultation here) It will be interesting to see how often, and in which scenarios, Ofcom is willing to impose the highest fines - especially given its emphasis on proportionality.

Business disruption measures

In the most serious cases of non-compliance, Ofcom will be able to exercise some highly invasive powers, including the ability to seek a court order imposing business disruption measures, which may require third parties (e.g., payment or advertising providers) to withdraw from, or limit access to, the breaching services in the UK. Practically, it is not entirely clear at this time when Ofcom would consider a breach of the OSA to be so egregious that such invasive powers would be used – especially given (at least theoretically) the measures can be imposed without confirmation that a provisional or confirmation notice was not complied with. Interim measures will also be possible in relation to both service restriction and access orders.

Requirements to use certain technologies

Another significant provision of the OSA is that Ofcom will be able, under certain circumstances, to issue notices which require companies to utilise certain accredited technologies to identify and/or remove illegal content relating to terrorism and child abuse related content. These powers have been the subject of much debate, as some commentators have interpreted the provisions to mean that online platforms will have to *pro-actively* scan content, including potentially by decrypting content. Interestingly, the UK government

has confirmed that such technologies do not currently exist and so these provisions will only apply when such technologies become available, opening the door for tech companies to try to develop such technical capabilities.

Criminal liability and senior management liability

Regulated service providers may commit a criminal offence if they fail to comply with certain provisions of the OSA, including if they do not meet the requirements of an information notice or if they fail without reasonable excuse to take compliance against certain illegal content e.g., failing to take child safety measures against child sexual abuse content. In such cases, directors and other senior managers of the provider may also be criminally liable for the failures. Senior management should also note that information notices will be able to publicly name them.

Appeals and super-complaints

In-scope service providers will be pleased to learn that all of Ofcom's decisions will be subject to appeal. However, this may be a difficult process to pursue given that an appeal may only be brought with permission of the Upper Tribunal, which will only decide the appeal on the same principles as would be applied for judicial review. This is a notoriously high standard to meet for appellants.

Certain designated entities (these are yet to be determined) will also be able to make a "super-complaint" where a feature of a service presents a "material risk" of causing significant harm to users, may adversely affect freedom of expression, or may otherwise have a "significant adverse impact" on users or members of the public. Ofcom will publish further guidance on the procedure for making a super-complaint.

Transparency measures

Ofcom will have significant powers to require certain services to be more transparent about their online safety measures, including powers to evaluate the impact of these measures, and their implications for user rights and freedoms.

Ofcom will be required to issue every in-scope service provider with a notice to provide a transparency report about their service. This will be used by Ofcom to draft its own transparency reports summarising patterns and trends in terms of how organisations are furthering online safety and also highlighting any good practice measures companies are taking.

When will enforcement action bite?

Ofcom states in its consultation on enforcement, that while it will operate with "a bias against intervention", it will take action promptly when necessary. In terms of next steps, the first codes of practice on illegal harms are now in force (as of December 2024) and companies have until 16 March 2025 to conduct the relevant illegal harms risk assessments. Equally, as of January 2025, obligations on providers of pornography services to implement highly effective age assurance are now in force and all in-scope service providers are required to carry out child access assessments by 16 April 2025. After this, we may start to see some initial engagement from Ofcom, including making requests for specific information or copies of risk assessments from companies. It remains to be seen how heavy handed Ofcom's "risk-based" approach will be in practice.

Last updated: 5 March 2025