

LITIGATION & DISPUTE
RESOLUTION

The Online Safety Act in Focus: *Key challenges, implementation, and navigating Ofcom's approach*

On 26 October 2023, the UK's Online Safety Act received Royal Assent. In the first of our 'Online Safety Act in Focus' series, we outline some of the challenges arising from the Act for online platforms, search engines and tech companies. We also provide an overview of Ofcom's approach to implementing the Act, the regulator's prospective consultation launch in November and how in-scope services can best prepare for the new regulatory regime coming into force.

11 MIN READ

On 26 October 2023, the [Online Safety Bill](#) received Royal Assent and entered UK law as the [Online Safety Act 2023](#) (**'the Act'**). The accompanying government press release declared that the statute heralded *'a new era of internet safety and choice'*, while Technology Secretary Michelle Donelan repeated the familiar government mantra that the Act *'will make the UK the safest place to be online in the world.'*

It remains to be seen whether this ambitious claim is borne out in the years to come. In the short-term, however, what is immediately apparent is that the UK may have become the most complex place in the world for online platforms and search engines to operate user-to-user services. This is largely due to the history of and context for the Act. It has been characterised by contention and controversy throughout its legislative journey which was set in motion by the government's [Internet Safety Strategy Green Paper](#) in October

2017 and [Online Harms White Paper](#) in April 2019.

In its [White Paper](#) response of December 2020, the government claimed that it was *'unashamedly pro-tech'*, and *'committed to using digital technologies and services to power economic growth ... and ensure a more inclusive, competitive and innovative digital economy for the future'*. The government went on to say that it would take action to *'unlock innovation across digital markets, while also ensuring ... a thriving democracy, where pluralism and freedom of expression are protected.'*

Six years, four Prime Ministers, eight Department for Digital, Culture, Media and Sport Secretaries of State, and 135 amendment papers on from the inception of the Internet Safety Strategy later, the Act arguably presents more challenges than opportunities for online platforms and search engines.

At a glance: what the Online Safety Act means for online platforms

The Act establishes a complex regulatory landscape for online platforms and search engines that operate in the UK and imposes wide-ranging obligations and significant consequences where in-scope businesses fail to comply. One challenge facing in-scope companies and service providers is the sheer extent of the regulatory regime. The original draft Bill, first circulated in May 2021, comprised 141 clauses and five schedules across 145 pages. By the time it was returned to the House of Lords for final amendments in July 2023, the Act had evolved into 242 clauses and 17 schedules across some 288 pages.

While we will unfold the detail of the Act's provisions in the course of our 'Online Safety Act in Focus' series, the key obligations are set out below.



General
(sections 9-10)

Remove illegal content – platforms have an obligation to do so quickly (or to prevent it from appearing in the first place). This includes terrorist content (Schedule 5), child sexual abuse material (Schedule 6), revenge pornography, threats to kill, and other priority offences (Schedule 7).



Children
(sections 11-13)

Prevent children from accessing harmful and age-inappropriate content – this includes pornographic content, content encouraging suicide or self-harm, and content that depicts serious violence.

Enforce age limits and age-checking measures.

Ensure the risks and dangers posed to children on social media platforms are made clear by the platform, including by publishing detailed risk assessments.

Provide parents and children with clear and accessible ways to report problems when they do arise.



Adult
(sections 14-16)

Social media platforms have a legal responsibility to enforce the promises they make to users when they sign up, through terms and conditions. This includes a duty to make provisions in the terms of service specifying how individuals are to be protected from illegal content.

Offer users the option to filter out harmful content that they do not wish to see online. This includes suicide, deliberate self-injury, and racial, religious, sexual, ableist, or gender-related abuse.

Penalties for non-compliance with the Act include fines up to £18m or 10% of a platform's global annual revenue (whichever is greater). Additionally, executives could attract criminal liability and receive a two-year jail sentence if they ignore Ofcom's enforcement notices, while senior employees could face prison if they knowingly impede Ofcom's investigations. The regulator also has the power to block websites and apps in the UK in extreme cases.

Ongoing uncertainty: waiting for Ofcom

The future outworking of many of the provisions of the Act remains uncertain. One criticism which has been levelled at Parliament in this regard is that it has placed the onus to supply the detail of a number of key regulatory provisions squarely on the shoulders of Ofcom, an organisation that has traditionally been a broadcast regulator.

Beyond this, many aspects of the Act ultimately remain ambiguous and raise concerns over privacy and/ or security, freedom of expression and platform innovation. Questions have also been raised over how future-proof the legislation may be, while divergence from other regimes such as the EU's Digital Services Act and the shift from more traditional liability shields for platforms to positive obligations on platforms has caused concern.

The following issues stand out:

- **Systems vs content moderation:** The government has frequently claimed that

the Act is 'systems-focused'. In late 2021, for instance, the Department for Digital, Culture, Media and Sport stated that *'the regulatory framework set out in the draft Bill is entirely centred on systems and processes, rather than individual pieces of content, putting these at the heart of companies' responsibilities.'* However, as the Act has progressed through Parliament it has become clear that its obligations effectively amount to content moderation. In fact, content moderation is an explicitly mandated measure under the illegal content safety duty in section 10, and the children's safety duty in section 12. Meanwhile, the Impact Assessment for the Act has estimated that consequent *'potential additional content moderation'* costs incurred by companies will fall somewhere between £1.3bn and £2.5bn, and that the mandated risk assessments will *'result in some platforms requiring additional content moderation .. with the largest, highest risk platforms expected to do more.'* Beyond this, provisions such as section 10(2) have raised concerns that the Act requires proactive monitoring on the

part of platforms, and even prior restraint of publication of certain kinds of content.

- **Private messaging & encryption:** In the case of private messaging, and by extension encrypted messaging apps, the 2019 White Paper took care to distinguish between public and private communications for the purposes of online harms, noting that respondents to its consultation *'opposed the inclusion of private communication services'* within the scope of prospective regulation. However, this has not survived the legislative process. Concerns have been raised over provisions in the Act that could require platforms to use certain technologies to identify terrorist or child sexual abuse content in private messages. While the government appeared to climb down on this at the eleventh hour, the issue remains open, and hints at a lack of understanding on the part of lawmakers as to what encrypted messaging apps have in common with social media platforms.
- **Risk assessments:** The Act compels platforms to compile illegal content risk assessments and children's risk assessments. This represents a potentially onerous burden; the risk assessments must be kept continuously updated and must be carried out again when making a *'significant change'* to *'any aspect of a service's design or operation'*. For platforms that are regularly updating their services, processes, and technology, the ambiguity inherent in this provision is problematic, while the continuous nature of the obligation could deter platform innovation.
- **Freedom of expression:** The significant consequences for non-compliance with the Act – sizeable fines and even criminal liability for executives – arguably incentivise an over-zealous approach to content moderation and removal. Effectively making platforms and services the arbiters of speech could have serious implications for Article 10 ECHR rights.

In this way, then, Royal Assent for the Act effectively marks only one more instalment in an ongoing journey toward a fully realised regulatory regime. While the Act aims to address legitimate areas of concern, the detail and workability of its envisaged regulatory burden on online platforms will only begin to become clear under the auspices of Ofcom in the coming months. Ultimately, while the general duties have been laid out, compliance with Ofcom's Codes and guidance will represent compliance with the law. Some 20 years on from the [Communications Act 2003](#), under which the internet was excluded from Ofcom's remit, the regulator has been charged with a momentous task.

Decoding Ofcom's approach to implementing the Act

For the 100,000 platforms set to fall within the scope of the Act, this is something of a double-edged sword. While the National Audit Office [anticipates](#) that the Act will not be fully operational until at least 2025, the coming months will likely determine its impact on online platforms and search engines. To ensure that future Codes of Practice effectively accommodate freedom of expression, privacy, clarity and flexibility,

Ofcom will launch its first consultation on illegal content in the coming days.

For platforms, this represents an opportunity. Although service providers need not follow Ofcom's recommendations under its Codes of Practice, the regulator has [stipulated](#) that doing so means that they '*will be deemed to have complied with the relevant legal duties*'. In practice, therefore, forthcoming guidance will effectively become the de-facto guide for platforms of all categories for compliance with the new statutory regime. Ahead of Ofcom's launch of its first consultation on 9 November 2023, we preview the regulator's approach to consultation, Codes of Practice and enforcement under the Act.

When will consultations begin?

Ofcom will implement the Act in three phases:

- i. illegal harms
- ii. child safety duties and pornography
- iii. duties on categorised services, including transparency.

Consultations during Winter 2023 are expected to focus on illegal harms, risk assessments, and enforcement guidance.

Consultation on phase (ii) will begin in December 2023, with a view to the publication of proposals in Spring 2024. By Spring 2025, Ofcom expects to publish draft guidance on online safety for women and girls, completing its work under phase (ii).

Finally, phase (iii) will address 'categorised services', or those who meet (as yet undefined) criteria relating to user numbers or risk profile. Ofcom anticipates publishing a register of categorised services by the end of 2024 to enable the final publication of its Codes of Practice and full guidance before 2026.

Who can respond to consultations?

Ofcom has [committed](#) to consulting '*fully and transparently*' on its plans under the Online Safety Act, '*giving companies sufficient time to comment*', and ensuring feedback is adequately considered. We expect these consultations will be invitational. Under clause 41(6), Ofcom has wide discretion to determine who best represents digital service providers, UK users, children, and affected parties for the purposes of any given consultation.

How will the new statutory regime be enforced?

As the UK's broadcasting, telecommunications, and postal regulator, Ofcom is responsible for enforcing compliance with the new regime. Notwithstanding its express preference 'to work with services to encourage voluntary compliance', the Act affords the regulator sweeping new powers to tackle contraventions of the Act and failures of compliance with its notices and Codes.

Discretionary powers open to Ofcom under the Act include:

- **Notices of Contravention (clauses 131-139):** Issued where there are 'reasonable grounds for believing' a provider has failed, or is failing, to comply with the Act. These notices will set out the breaches alleged and the proposed penalty. Should platforms persist in non-compliance, Ofcom may issue a subsequent confirmation notice requiring the provider to take steps, pay a penalty, or use proactive technology to address its contravention.

- **Penalty Notices (clauses 140-143):** As noted above, failure to comply with the Act may result in fines of up to £18m or 10% of global revenue (whichever is greater).
- **Business Disruption Measures (clauses 145-147):** Ofcom has a 'backstop power' to seek a Court order imposing requirements on a regulated platform or, in the most serious cases, requiring ISPs to block access to non-compliant platforms.

How Ofcom chooses to use these new powers is yet to be determined. In practice, however, three factors should give platforms cause for relative optimism.

Firstly, any fines issued for non-compliance must be appropriate and proportionate to the breaches identified. In addition, Ofcom must consider a range of factors when determining penalties, including platforms' own evidence, the effect of any failures and steps taken by the platform to resume compliance.

In addition, despite the oft-trumpeted figures of £18m and 10% of global revenue, Ofcom's new enforcement powers are

comparable to those conferred on the Information Commissioner's Office under the [Data Protection Act 2018](#). Just as requiring the ICO to investigate every complaint received 'would become extreme and take the system to breaking point if not beyond', so Ofcom will likely adopt a targeted enforcement approach.

Finally, a number of recent ICO penalty notices have been reduced significantly on appeal. In May 2022, for instance, a [decision](#) that saw a £1,350,000 fine levied against Easylife Limited was reduced to just £250,000, in part because Easylife 'stopped the unlawful processing which formed the basis of the ICO's concerns.' In light of the government's [renewed focus](#) on 'driving innovation and growth across digital markets', Ofcom too will likely face pressure to act pragmatically when issuing financial penalties under the Act.

Outlook

Realising the Online Safety Act's policy objectives remains both practically complex and commercially fraught. It remains to be seen how far a number of the Act's provisions are actually workable and enforceable in practice. Only time will tell how Ofcom will shape the contours of the UK's purported '*new era of internet safety and choice*.'

In this respect, platforms' engagement with Ofcom in the coming months could prove decisive in shaping the Act's scope, interpretation and commercial impact. User-to-user services have the opportunity to provide robust responses to the forthcoming consultations, including in relation to content review and risk assessment requirements. This could not only reduce the likelihood of future regulatory enforcement action against platforms but may also assist preparations for formal information requests made under the Act.

Although the Act will come into force gradually, forward-planning platforms that can show that senior managers are considering the Act's obligations, conducting relevant risk assessments, updating terms of service, and compiling compliance plans will be in a strong position to deal with questions or information notices from Ofcom.

Future instalments of our '*Online Safety Act in Focus*' series will examine the Act's obligation on platforms to proactively monitor for illegal content, divergence from Article 15 of the E-Commerce Directive, the future of encrypted messaging services under the Act and detailed breakdowns of Ofcom's forthcoming consultations, guidance, and Codes as they are published.

If you would like to discuss the issues raised by this article further, please contact **Ciaran O'Shiel**, **Ronan Marlow**, or any member of the **IP, Media, and Technology Disputes Team** in ALG's Belfast office.

Key contacts



Ciaran O'Shiel
Partner
+44 28 9072 7448
coshiel@algoodbody.com



Ronan Marlow
Senior Associate
+44 28 9072 7549
rmarlow@algoodbody.com



Caroline Price
Solicitor
+44 28 9072 7442
cprice@algoodbody.com



Niamh Flanagan
Solicitor
+44 28 9072 7702
nflanagan@algoodbody.com

Resources



[The Online Safety Act 2023](#)

[READ MORE](#)



[The Online Safety Bill](#)

[READ MORE](#)



[Ofcom's approach to implementing the Online Safety Act](#)

[READ MORE](#)



[Ofcom's roadmap to regulation](#)

[READ MORE](#)



[The EU's Digital Services Act](#)

[READ MORE](#)