The Safety Net – Pornography providers

Age Assurance under Part 5 OSA

Aside from its core provisions addressing illegal harms and protection of children, the Online Safety Act ('OSA') contains a short, standalone section (Part 5) specifically addressing online pornography services. As of 17 January 2025, Part 5 is fully in force, following commencement by the Government.

Who is in scope of Part 5?

The OSA defines pornographic content as 'content of such a nature that it is reasonable to assume that it was produced solely or principally for the purpose of sexual arousal.' For the purposes of Part 5, this does not include pornographic content that consists only of text, text accompanied by an emoji or text accompanied by a non-pornographic GIF.

Perhaps somewhat confusingly, Part 5 only applies to a service if the pornographic content available on the service is published or displayed by or on behalf of the *provider of the service*. Services that allow users to post and share their own pornographic content will be treated as user-to-user services under the broader provisions of the OSA (see our articles on the illegal harms and child safety requirements, which apply to user-to-user services). It should also be noted that services incorporating generative AI tools which enable users to generate pornographic content for their own consumption (as opposed to them sharing this with other users), even if unintentionally, will be covered by Part 5.

Of course there may be hybrid pornography services that publish provider content, as well as user generated content, which will therefore be subject to both the obligations on user-to-user services and the Part 5 obligations.

To add some further confusion, Part 5 only applies to services with links to the UK, but presents a more limited 'links to the UK test' than the equivalent test under the broader provisions of the OSA (see our article on the scope of the OSA). In order for Part 5 to apply, the test requires that either:

- a service has a significant number of UK users; or
- the UK forms one of the target markets for the service, or the only target market.

Ofcom's guidance on Part 5, which was published on 16 January 2025, states that whether a service has a significant number of UK users should be understood as meaning that the number of UK users on the service is material in the context of the service, rather than the absolute number of UK users of the service necessarily being a large or substantial number. This means that smaller services cannot avoid the OSA simply by virtue of their smaller user bases, and will be in scope if a significant proportion of its users are in the UK.

The OSA provides some exemptions from Part 5, which include on-demand programme services (essentially streaming services and TV 'catch-up' services) and results displayed on search services.

What are the requirements under Part 5?

The obligations under Part 5 are fairly limited and are divided into:

- age assurance duties; and
- record-keeping duties.

Age Assurance

Age assurance is the key duty on providers of online pornographic services under Part 5 and requires that providers implement age verification and/or age estimation tools in order to ensure that children are *not normally able to encounter* pornographic content on the service. To meet the standard required by the OSA, these tools must be *highly effective at correctly determining whether or not a particular user is a child*. "Child", for the purposes of Part 5 (and the OSA more generally), means anyone under the age of 18. Ofcom confirmed in a statement on 16 January 2025 that it expects providers of Part 5 pornography services to implement highly effective age assurance as of 17th January 2025.

Ofcom's guidance sets out some further expectations around the implementation of age assurance, including that:

- providers should take steps against enabling or encouraging children to use tools that can circumvent age assurance measures, such as VPNs; and
- age assurance measures must be implemented at the 'point of entry' to a service, so that no pornographic content may be viewed before age checks have been cleared.

Ofcom also sets out four key criteria for age assurance, all of which should be met if providers are to ensure that an age assurance solution is 'highly effective' as required by the OSA:

1. **Technically Accurate** - the solution should be sufficiently capable of correctly determining the age of users under 'test lab' conditions.
2. **Robust** - the solution should be sufficiently capable of correctly determining the age of users in 'unexpected or real-world' conditions.
3. **Reliable** - the solution should be consistent and produce similar results from similar inputs.
4. **Fair** - the solution should avoid bias or discriminatory outcomes.

Ofcom recognises that some solutions may perform better under some of these criteria than others. It emphasises that providers must ensure that the solution they select sufficiently fulfils all of the criteria when taken as a whole, but acknowledges that a degree of 'trading-off' may be appropriate.

Ofcom has favoured taking this 'principles-based' approach over providing a more concrete, metrics-based threshold for demonstrating that an age assurance measure is effective. Notably, the consultation responses to the draft guidance showed that many providers pushed for the latter in order to gain greater certainty.

Further principles set out in Ofcom's guidance include ensuring that age assurance solutions are accessible and easy to use by all users and are interoperable with all common and standard technological systems.

Ofcom has been careful not to confirm that any particular age assurance methods meet the 'highly effective' standard under the OSA, but has provided some examples, within its guidance, of methods that may meet this standard, including:

- Photo-ID matching;
- Facial age estimation;
- Credit card checks;

- Digital ID wallets; and
- Open Banking (essentially confirming with a user's bank that they are over 18).

Ofcom has also provided examples of methods that are not capable of being highly effective, including self-declaration of age, contractual restrictions on child users and debit card checks.

It is also worth noting that Ofcom expects providers to regularly review the age assurance solutions that they are using and to determine whether newer technologies may be more effective. It is therefore not simply a case of meeting the necessary requirements when a solution is first implemented, but rather there is an ongoing duty to keep this under review.

Record-Keeping

The OSA requires providers of Part 5 services to keep a record of the age verification and/or estimation methods used, how they are used and how the provider has taken account of user privacy rights when deciding on the method to use. Providers are also required to make a summary of this record publicly available.

Ofcom's guidance builds on this duty, making it clear that the record must be easy to understand, easy to locate, durable and kept up to date. The record should be made or updated as soon as possible after a new age assurance method is deployed, and, where possible, should be in English (or either English or Welsh for providers based in Wales). The record should also include details of how the four criteria in Ofcom's guidance are met and should provide details of any third parties involved in providing the relevant age assurance solution.

Ofcom also elaborates on the importance of respecting user privacy and data protection rights when implementing age assurance tools and recommends that providers familiarise themselves with data protection legislation and ICO guidance on age assurance.

Last updated: 22 January 2025