Open Rights Group oppose the new amendment proposing blocking of pornographic websites failing to age-verify their users:

- **Administrative, not court ordered blocking**

Website blocking will be carried out on purely administrative grounds. If the amendment does not specify *"appropriate"* means of website identification, the age-verification regulator will block **legal erotic and pornographic content** without due **legal process** (such as obtaining a court order).

The web blocking amendment says the age-verification regulator is the responsible body for identifying "*the non-complying person"* and allows them to do so *"in such manner as the age verification regulator considers appropriate".*

Unlike a court order process, administrative web blocking does not automatically provide a route of appeal. The Bill only provides information about the arrangements for appeals, not a specific route. Thus we assume that Judicial Review would be the normal route to challenge a block. This seems excessive. A simple and inexpensive route of external appeal, to the courts, should be included.

- **Blocking in bulk**

The process appears to be designed to allow the regulator block websites in volume. This is likely to lead to overblocking and administrative errors if this approach is taken.

Nevertheless, Parliament has been led to believe that blocking is required to prevent children from finding or 'stumbling upon' pornography. To reach this goal, vast numbers of sites would need to be assessed and then blocked. This is not realistic.

- **Technical methods of blocking**

No method of blocking is perfect. Usually, the UK ISPs block websites through the domain name system (DNS) requests. Requests from people's computers to access domain names (e.g. porn website address) are blocked and redirected to other websites (usually to a webpage belonging to the ISP). New encrypted mechanisms for resolving addresses (which are likely to start to be adopted in the next two years) will make it less easy for ISPs to identify and block requests for erotica and porn websites using filters or pattern matching. In the longer term, this method of ISP blocking is likely to be ineffective.

Using other ways of web blocking, such as IP address blocking, would cause overblocking of websites which share an IP address with a blocked website. Any website, whether it offers adult content or not, can have the same IP address as an adult website. If ISPs were to block them they would cause unintended damage to third parties.

Blocking on the ISP level will demand large investments in projects with short-term results.

- **Costs coverage and scope**

Wide-scale blocking of websites will impose costs from the technical deployment and maintenance of censorship systems. The proposal makes no mention of who will be financially

responsible for administering website blocking. Previously, businesses have been provided with means to cover implementation[1] of other legislative requirements.

It is not reasonable to impose the costs of this policy on ISPs. The costs would in some circumstances be prohibitive, as not all ISPs have the means to implement blocking especially at scale.

The amendment allows age-verification regulator to issue a compliance notice for website blocking to any ISP without regard to their size or ability to implement blocking. This would have a detrimental effect on smaller ISPs. For this reason smaller ISPs have been exempt from copyright related court orders for website blocking.

- **Scale of blocking**

The amendment requirements to set standards for the administration of the blocking of non-complying websites. It is not clear:

- how they will know that websites continue to be non-compliant,
- whether ISP blocking will be targeting only websites in English language,
- how websites in other languages will be assessed without significantly increasing the costs,
- whether unauthorised (unsafe but effective) AV methods on porn and erotica websites will be considered non-compliant[2] and blocked.

- **Cybersecurity risks**

The proposal may create an unsafe environment filled with criminals operating scam porn sites to gather credit card details.

The regulator has the power to issue guidance on requirements of arrangements for age verification. If credit cards become the default arrangement for age verification and, at the same time, a credible and permissible ask in the minds of UK citizens, then there will be a serious risk of criminals setting up sites in the UK. People will simply be invited to supply their credit cards to "age verify" on scam sites. This kind of fraud could be applied to any kind of site claiming to require users to prove their age.

This is exacerbated by website blocking as it may be hard for the regulator to object to credit cards as a means of verification. It would seem excessive to block websites using credit cards as verification, for instance.

- **Net neutrality, Human rights & EU law**

These proposals are likely to be in breach of the EU regulation on net neutrality and the Open Internet principle. The Article 3[3] of the net neutrality regulation does not allow blocking or throttling or discrimination of online content, applications and services.

---

[1] The Home Office allocated £174.2 million over ten years from its budget to cover costs for ISPs retention of Internet connection records required in the Investigatory Powers Bill.

2 https://www.openrightsgroup.org/blog/2016/website-blocking-will-open-up-age-verification-to-credit-card-fraud

3 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.310.01.0001.01.ENG&toc=OJ:L:2015:310:TOC

Any UK regulation that calls for ISP website blocking has to comply with the EU net neutrality regulation. The EU law has to abide by *"the requirements of the Charter of Fundamental Rights of the European Union ('the Charter') in relation to limitations on the exercise of fundamental rights and freedoms"*. Under the net neutrality regulation, the only reason to restrict the fundamental rights is if it is proportionate, appropriate and necessary within a democratic society. It is unclear that administrative procedures that affect both users' and sites' free expression would meet the standards required by the Charter or the ECHR to justify censoring in a democratic society.

There is also no requirement for a proportionality assessment prior to blocking in the amendment.

The amendment would therefore expose the DEBill to a potential judicial challenge at the CJEU and ECtHR.