RESPONSE TO PORNOGRAPHY REVIEW CALL FOR EVIDENCE

About the Online Safety Act Network

The Online Safety Act Network brings together over 60 civil society organisations, campaigners and advocates with an interest in the implementation of the Online Safety Act. It is run by Maeve Walsh , with Professor Lorna Woods (University of Essex) as an adviser and continues the work carried out at Carnegie UK during the passage of the Online Safety Bill. This includes collaboration with a number of organisations with an interest in Violence Against Women and Girls, with whom we published a draft code of practice in 2022. More details about the work of the OSA Network are here.

Summary

We welcome the Government's commitment to the Pornography Review and to the approach of the Call for Evidence, particularly its focus on the regulatory, legislative and enforcement context. We focus most of our response to the Call on those issues. Our experience in shaping and tracking the progress of the Online Safety Act (OSA), from initial policy development through to Royal Assent, informs this response. While we know that there is a line drawn between the scope of the OSA and the interests of this Review, we would recommend that it is not taken as read that the OSA will deliver the step change envisaged in the online environment – at least not in the short-to-medium term and we would encourage Baroness Bertin and the review team to consider where gaps remain.

While the OSA contains a number of different categories of content and service, leading to a fragmented picture in terms of the regulation of pornography, this story of fragmentation is seen also when looking at the regulation of content more generally. In seeking to rationalise this area we suggest that the review is mindful of a number of key distinctions:

- The different sorts of laws that can be used as mechanisms of control: criminal; regulatory; and civil – as well as the different degree of intrusion that these techniques imply;
- Different mechanisms of control – prohibition on content; restrictions on access (age- or place-based);
- A distinction between private possession (linking to private life) and distribution for business purposes (commercialisation in its many forms, which links to speech in public); and
- The difference between online and offline, and the extent to which this is still a valid distinction to make.

Key points: Boundary with other regulatory and legislative regimes

Online Safety Act

The Call for Evidence provides a useful overview of the current landscape (pp13-25) and the confusing and muddled boundaries that lead to differences in definitions and consequential differences in criminal and regulatory enforcement. It is important to recognise that the significance of imposing criminal liability (in this context aimed at the users of online services), which imposes penalties on the individual – whether this be the mere fact of a criminal record or the possibility of loss of liberty through imprisonment. This is very different from regulatory action when it is the activity which is the focus, even though regulatory action may lead to brand embarrassment. Beyond the difficulties of using the criminal law as a benchmark for regulatory action, it is important to recognise this difference in terms of the significance/intensity of state intrusion. Moreover, it is also important to emphasise that in the offline (including broadcasting and video on demand) context, although criminal content would not be permitted there has never been any suggestion that regulation (with its lower level of intrusion) should be limited to circumstances in which content is bad enough to be criminalised. In this context, the binary phrase that "what's illegal offline should be illegal online" is unhelpful as it suggests that there is only one type of law, rather than recognising the existence of regulatory and civil regimes in addition to the criminal law.

We note that in the Review's press notice, it says that the Pornography Review: "builds on the government's work to take the long-term decisions for a better future for our children and grandchildren through the Online Safety Act, by stopping children from accessing pornography online by requiring services to establish the age of their users, including through age verification and age estimation tools." The OSA, as a vehicle to tackle pornography, is problematic in a number of respects.

We would refer the Review to our recent submissions to Ofcom which point to a number of potential shortcomings in the enforcement approach being taken which will directly impact on the effectiveness of the Act in protecting both against illegal content and children's access to commercial porn. We highlight a few of these concerns here.

Approach to illegal harms

Our response to the illegal harms consultation set out a number of our concerns about Ofcom's approach, which are relevant here due to the inclusion of the extreme pornography criminal offence as a priority offence (see OSA Schedule 7) as well as the new offences of non-consensual intimate image abuse. Primary priority content that is harmful to children (OSA section 61) includes pornography.

We are of the view that Ofcom's approach to enforcement – which takes a narrow approach, mainly focused on takedown – is not going to bring about the step change in the online environment that the Government envisaged at the time of the passage of the Act, and that is reinforced in the way the documents relating to the Pornography Review refer to it. We would draw the attention of the Review particularly to our analysis on the illegal content judgements guidance.

Our response was supplemented by a transcript of a roundtable attended by a number of experts from the Violence Against Women and Girls sector which sets out some of the wider context for more effective action by Ofcom in enforcing the illegal content duties. We would also refer the Review to the

recent comment by the UN Special Rapporteur on Violence Against Women and Girls at the end of a visit to the UK:

> "While the enactment of the Online Safety Act is a welcome development, gaps remain, specifically around the issues of violence within the pornography industry, the influence of pornography on individual and societal attitudes towards VAWG and the impact of legal pornography on perpetration of child sexual abuse, both online and offline. We need to move away from companies self-regulating towards a legally enforced duty of care on tech companies across the distribution chain to ensure that they have adequate infrastructure to prevent tech abuse and to support survivors." (UNSR Summary of Preliminary Findings after visit to UK – 21 February 2024)

We went on to say in our response that: "Until the Government conceded on Baroness Morgan's amendment in the latter stages of the Bill's Parliamentary passage, the Government promised that the new offences would go a long way to improving protections for women and girls and that a separate code of practice was unnecessary. The opposite is true – and Ofcom's guidance on VAWG, which was the Government's concession, will not be consulted on for at least another year."

Moreover, we agree with the points made by Professor Clare McGlynn in her submission to the Pornography Review that the OSA has "resulted in 8 categories of pornographic content each with their own regulation regime: this is a confusing and complex regulatory regime in itself, but even more so as the boundaries between the categories are not clear."

These multiple categories are compounded by the reliance on criminal offences in the Act and the imperative this sets for regulated services (and indeed the regulator) to rely on criminal thresholds for action (takedown of content) and enforcement (focused on the user's behaviour) rather than the development of an effective regulatory regime that is focused on reducing harm through effective risk-based systems and processes. It also pre-supposes that the criminal law provides a complete catalogue of problematic behaviours and content online, even before we consider the development of technologies. While the new offences in Part 10 cover deepfakes, it is less clear that priority offences relevant to pornography would all translate well to virtual environments, for example.

We note also that the OSA does not cover pornography short of the criminal threshold (even where the threshold is not satisfied for rather technical reasons) in relation to adults, meaning that there are no controls required. The list of content areas for user empowerment tools does not mention pornography, yet surely it would have been appropriate to give people the ability to control whether they see "NSFW" content that goes to the heart of private life. In this context we not that significant amounts of porn are found on mainstream social media platforms (e.g. X) and that user tools to indicate that the user does not want to see certain content at the moment send rather weak signals to recommender systems. While some protection may be provided by terms of service, it is important to note that services have no obligation to takes steps against pornography and that it is only Cat 1 services which are required to enforce their terms of service generally.

Approach to OSA part 5 duties on commercial pornography providers

Our recent response to Ofcom's consultation on the guidance for pornography providers relating to their duties under Part 5 of the OSA focuses on the likely effectiveness in reducing the access children have to commercial pornography sites. In it, we set out a number of concerns about the differing approaches to age verification taken between the OSA, Video-Sharing Platforms regime (which is repealed by the OSA and whose regulated services are now in a transition phase) and the On-Demand Programme Services regime.

Part 5 and Part 3 both deal with the issue of non-criminal pornography through controlling access for children. The position as regards adults is not dealt with, save to the extent that the content does not trigger the criminal law (which we have noted is problematic as currently interpreted). Part 5 provides even weaker protection vis a vis adults. There are no content rules (and this is a contrast to the position under the VSP and VOD rules) - the position is worrying given the amount of non-consensual material that has been found on mainstream sites.

The wider legislative context

As has already been noted, the OSA is not a mechanism addressing all aspects of pornography. Even for its main focus of user-to-user content it has gaps. Part 5 seems to be a replay of the Digital Economy Act 2017, Part 3 - which seemed a response to the gaps in the video-on-demand regime. While the regime did contain content rules that would tackle pornographic material – and was specifically linked to the BBFC classifications – it was geographically limited. The rules regulating video-on-demand (VOD) in the UK derive from the Audiovisual Media Services Directive (AVMSD) as amended in the mid noughties. Originally, powers to regulate these services were delegated to ATVOD, but retracted in-house by Ofcom in 2015.

One of the early problems relating to the implementation of the VOD rules concerned jurisdiction and the tension was created by the pornography providers. Because the VOD rules came from the AVMSD there was a one-stop shop principle for VOD services based in the EU: the country of establishment regulated them. This rule did not apply to providers established in third countries (e.g. Canada). Nonetheless, the British legislature decided just to empower Ofcom to regulate companies established in the UK, and the resulting rules did not cover incoming services from non-EU states. Pornography providers came within the substantive VOD rules but objected to being regulated (although they would be subject to constraints off-line). The result was that the providers relocated from the UK to other places (e.g. Canada) and then transmitted back to the UK from there. Even for services within jurisdiction, Ofcom has not seemed to enforce the rules with any particular degree of enthusiasm – perhaps because of political signals at the time the regime was set up. Note that some content providers using platforms such as YouTube could be service providers within the VOD regime in their own right.

The VOD rules are the subject of review, with the Media Bill currently under scrutiny in Parliament. It is not a completely fresh start but rather adapts the existing broadcasting and VOD regimes. Clauses 37 to 40, together with schedules 5 to 8, extend the jurisdiction of the VOD rules to some non-UK based service providers and would provide Ofcom with new regulatory powers to draft and enforce a VoD code

applying to them as well as to some but not all UK based ODPS. UK ODPS seem still to be subject to s 368E- 368H which outline content standards for both editorial and commercial content.

Services which satisfy these requirements each constitute a "non-UK on-demand programme service". Specific obligations apply to "Tier 1 Services". The details of these obligations are found in Sch 5-7 Media Bill. Note, Pt 5 Online Safety Act will not apply to a service which is an ODPS, but that refers to the current language in s 368A (s 80(6) OSA) and would not seem to extend to any non-UK services. Tier 1 services, in addition to the base obligations already in the Communications Act, will need to comply with a code to attain "standards objectives". In addition to ensuring that under-18s are protected (which seems to some degree to overlap with the already existing VOD rules), the providers will need to ensure

> "that generally accepted standards are applied to the contents of those services so as to provide adequate protection for members of the public from the inclusion of offensive and harmful material".

As part of its new obligations, Ofcom will be required to carry out a review of "audience protection measures" (which were required by previous regimes), and which include

(a) age rating or other classification systems;

(b) content warnings;

(c) parental controls; and

(d) age assurance measures.

See Cl 23 Media Bill inserting a new s 368OB in the CA03.

These amendments seem still to leave non-Tier 1 non-UK services outside the regulatory regime – though presumably the protection provided by Part 5 OSA is viewed as dealing with that category of services. We have noted the weakness in that regime as regards adults and illegal content.

Online Safety Act Network

March 2024

Contact: maeve@onlinesafetyact.net