Ofcom Consultation on Illegal Harms Updates for New Priority Offences

Dated April 24th

By email to NewPriorityOffences@Ofcom.org.uk

For any questions or further communication please contact [redacted]

EVAW

The End Violence Against Women Coalition (EVAW) is a leading coalition of more than 170 specialist women's support services, researchers, survivors, campaigners, NGOs and other experts working to end violence against women and girls in all its forms. Established in 2005, we campaign for every level of government to adopt better, more joined up approaches to ending and preventing violence against women and girls, and we challenge the wider cultural attitudes that tolerate and condone this abuse. The EVAW Coalition is a company limited by guarantee (no. 7317881) and a registered charity (no. 1161132).

EVAW has carried out extensive policy and campaigning work on online violence against women and girls (VAWG), with a specific focus on image-based sexual abuse as it pertains to criminal legislation and regulation. For the purposes of this consultation, we will speak specifically to the proposals relating to cyberflashing. As a result of our limited capacity we have chosen to respond to this consultation as briefly and succinctly as possible below.

Introduction

The consultation document quotes a 2021 Law Commission report stating that: *"Survivors and victims of cyberflashing describe feelings of shame, embarrassment and vulnerability following the experience."* We would suggest that there is more to say on the harms and nature of cyberflashing, and note that the source for this overview is 5 years old and therefore quite dated given the fast paced nature and exponential rise in forms of image-based sexual abuse we have seen in recent years. We would perhaps suggest that such a summary and citation could be perceived as reflective of Ofcom's minimal approach.

Risk Assessments

We agree that providers must now separately risk assess for the illegal harm of cyberflashing, and assigning risk levels.

Risk Profiles

We identify that livestreaming should be identified as a specific risk factor for cyberflashing. We also stress the need for dating sites to be specifically named in the risk profiles, notwithstanding the intention for the risk profiles to provide a simplified overview. As Ofcom themselves

acknowledges, there is strong evidence that dating sites have a higher risk of cyberflashing, and as such should be explicitly listed. Given this acknowledgement, and the Illegal contents judgement guidance (ICJG) describing cyberflashing as a 'commonly accepted' practice, we are concerned by the apparent contradiction this omission creates.

We recommend that Ofcom considers further services and actions as additions in line with the intimate image abuse and extreme pornography offences. This should include discussion forums and chat rooms, reposting or forwarding content. See table below from the Draft Risk Assessment Guidance and Risk Profiles:

12.	Extreme pornography	1a. Social media services, 1d. Adult services, 5e. Posting images or videos and 7a. User-generated content searching.
13.	Intimate image abuse	1a. Social media services, 1d. Adult services, 1e. Discussion forums and chat rooms, 1g. File-storage and file-sharing services, 4b. User groups, 4b. Group messaging, 5b. Direct messaging, 5e. Posting images or videos and 5g. Re-posting or forwarding content.

Generative AI

It is also our view that generative AI should be included as a risk factor in the risk profiles, notwithstanding the stated need for a comprehensive update. Generative AI poses a specific and particular risk in relation to online VAWG, and must be featured and understood as a risk profile.

There is a need for greater leadership from both Ofcom and the government in acknowledging, responding to and taking steps to prevent AI-facilitated and AI-driven online VAWG. We strongly support Ofcom's reference to undertaking a comprehensive review, and recommend that this proceeds with urgency.

Register of Risks

Ofcom refers to a small amount of new evidence on cyberflashing. It would be helpful if this data was included here.

We also seek to better understand how Ofcom will be maintaining its knowledge and data relating to cyberflashing, particularly in regards to the rates of reports, convictions and prosecutions from the police and Crown Prosecution Service (CPS). We suggest that there are insufficient mechanisms or forums for information exchange and learning between Ofcom, the police and CPS in this regard..

We also stress that there is inadequate data and understanding of cyberflashing more broadly - outside of those limited offences which reach criminal justice agencies - and the risks and context associated. This is in part because there is no mechanism by which individual members

of the public are able to report their experiences of cyberflashing (and other online harms) to Ofcom - this should be acknowledged more fully and highlights a role for an online commission. Please see our IBSA policy paper for further context.

Illegal Content Judgments Guidance

We are confused and opposed to the designation of cyberflashing as "commonly accepted" practice on gay dating sites in the draft ICJG, and the exception granted. We echo the position of Professor Clare McGlynn on this issue and have attached her briefing on this, also available here.

"There is no such defence or exception in the cyberflashing criminal offence. Indeed, sending unsolicited dick pics is against the terms of service of most dating sites. It is not at all clear why Ofcom continues to provide this exemption to the law and excuse for services not to act.

….

Why is Ofcom giving carte blanche to sites to decide for themselves if there is a 'commonly accepted culture' on their service of sending unsolicited dick pics, meaning they don't have to take proactive action, when this is exactly the type of conduct that the law was introduced to prohibit?

Why is Ofcom allowing a situation to continue whereby Terms of Service prohibit this conduct, but this is not enforced?"

We seek clarity on the above questions proposed by Professor McGlynn and stress the need for cyberflashing, a criminal offence, to be treated as such.

Proposals: Codes

We agree that the measure relating to blocking and muting (ICU J1) should also apply to relevant services at risk of cyberflashing. However, this measure can only be deployed once the harm has been done and the image or video received. We strongly recommend that Ofcom considers additional measures such as blurring or blocking an image before it is received. Additionally, the use of nudges or 'counterspeech' to the individual attempting to send the image or video.

We stress again here the need for dating services to be explicitly named and included in the risk profiles.

WARNING! EXPLICITLY GRAPHIC TEXT IN THE NEXT PARAGRAPH

We also propose that more consideration and research is required in relation to recommender systems for cyberflashing. Our position is that specific algorithms which drive and recommend content that relate to indecent exposure, flashing, unwanted and non-consensual sexual contact and content where such behaviours are presented as humour (see for example a widely shared

video that where a young man cut a hole in his ‘bum bag’ so that when searched at a festival by a female security guard she was confronted by his penis) contribute to cyberflashing activity, and as such should be included as a measure.

Impacts on Service Providers

We express some concern at the repeated statement that the impacts on service providers from Ofcom’s proposals will be limited. This feels minimising of the work that could and should be carried out in line with the proposals, and meaningful prevention and intervention.

Ofcom states that it is unlikely for any new services in scope which is surprising given the knowledge and evidence Ofcom have regarding dating services as a locus for cyberflashing. This suggests an overly narrow approach to the proposed code.

We echo and endorse the proposal from the Online Safety Act Network that extreme pornography should be added as a cross-reference for the risk factors recommended, in recognition of the motive requirement of sexual gratification.

Conclusion

Overall, we are unsettled by Ofcom’s stated position that the impact of these codes will be limited. There is a clear discrepancy here with the government’s own more ambitious claims on this issue which imply more significant changes to the online ecosystem, not apparent in these proposals.

ENDS