Consultation response form

Please complete this form in full and return to IHconsultation@ofcom.org.uk

Consultation title	Protecting people from illegal harms online
Full name	Victims' Commissioner for England and Wales
Contact phone number	
Representing (delete as appropriate)	Organisation
Organisation name	Office of the Victims' Commissioner for England and Wales
Email address	victims.commissioner@victimscommissioner.org.uk

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how Ofcom handles your personal information and your corresponding rights, see Ofcom's General Privacy Statement.

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? Delete as appropriate.	Nothing
Your response: Please indicate how much of your response you want to keep confidential. Delete as appropriate.	None
For confidential responses, can Ofcom publish a reference to the contents of your response?	Yes

Your response

Question (Volume 2)	Your response
Question 6.1: Do you have any comments on Ofcom’s assessment of the causes and impacts of online harms? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer. **Question 6.2:** Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.	**General feedback on Volume 2:** I have written to Minister Frazer to set out concerns about the approach that has been taken to this consultation. I will reiterate here some of my concerns which apply specifically to Volume 2. Throughout the guidance, the online space is viewed in isolation. The online space interacts with offline space; this can be seen in how societal attitudes impact the online space and, in recent times, the degree to which the online world can shape offline attitudes. Harms are viewed in isolation in the online space without much appreciation of the links to offline harms being perpetrated against the same victim. Yet moderators are asked to consider individual incidents without considering how online incidents of abuse can be part of an offence such as coercive control which is a pattern of behaviour offence and will include offline abuses too. The guidance casts tech companies as good faith actors, making the incorrect assumption that the online world is inherently neutral or safe. This starting point and that perspective is unhelpful, and I would suggest that the onus should be on platforms themselves to provide the evidence that their business models are safe and that they have inclusive policies. There is an over-emphasis on freedom of expression, which is not adequately balanced with the rights of individuals (or society) not to be harmed. This could result in greater weight being given to upholding freedom of expression rather than to the rights of the individual who is being harmed. Freedom of expression in this consultation seems to be mostly concerned with and explored in the context of the ‘abusive’ user and not on the on-going freedom of expression of the ‘victim’ or witnesses to the abuse. There is inconsistent treatment of evidence-bases across different offences, with far greater ‘pragmatism’ and leeway given in relation to some offences such as foreign interference, weapons, drug offences, compared to violence against women offences. Lastly, the harms as categorised by Ofcom into separate chapters means the co-occurrence of and links between harms are not well explored. This is a problem because victims often experience multiple harms/ abuses online. This will be discussed further below.

Question (Volume 2)	Your response
	6E. Harassment, stalking, threats and abuse offences • Paragraph 6E.11 states that "Stalking and harassment online can differ from offline contexts, relying on specific technological affordances and dynamics". Whilst this is true, it is critical that they are not viewed as independent offences. 45% of stalking victims are stalked by an ex-partner and the vast majority of stalking victims know their stalker personally – most victims therefore have an 'offline' link to their stalker, making it impossible to separate the psychological impact of online abuse from the fear of offline consequences. There is also no recognition given to physical and sexual abuse when discussing impacts on victims, despite research indicating that half of perpetrators who make threats of physical and sexual violence will follow through with these threats.[1] • The guidance should also make clearer the established link between domestic abuse and stalking and harassment, to emphasise that these online offences rarely occur in a vacuum, and should highlight the specific risks faced by victims of domestic stalking. • It is also crucial to note that a reliance on reactive actions against harm, such as blocking and removal of accounts, can have the opposite intended effect – a removal of the ability to cause online harm can lead to perpetrators seeking out methods to escalate the abuse and move to offline targeting. The focus on blocking and takedowns is also problematic as it places the onus on the victim to instigate action against the perpetrator, rather than encouraging safety by design. There is no real attention given to the idea of prevention in this guidance. There is discussion of the fact that perpetrators of abuse and harassment frequently create fake user profiles to harass their victims, but nothing suggesting that tech companies should be working to prevent this being so easy. We know that many tech companies have vast resource and choosing not to improve safety by design to prevent fake profiles being created for this purpose is a choice; this must be addressed. • This exemplifies wider concerns I have about the Register of Risks. Firstly, there is a risk that only including these 15 broad groups of illegal harms leads to harms not included being overlooked. This is particularly serious when one considers some of the harms which have not been included in the Register, such as honour-based abuse and female genital mutilation. Secondly, by identifying these groups and treating them as separate within the Register, this creates a perception that these harms are siloed and

[1] Violence in stalking situations (researchgate.net)

Question (Volume 2)	Your response
	fails to raise awareness of the fact that many victims will experience multiple harms, often simultaneously. Research by this office in 2022 found that victims of online abuse frequently experienced multiple types of abuse, with the average number of harms experienced being 4.2 per person. This average was even higher for victims of cyberstalking, at 6.9 per person.[2] • Similarly, I would welcome consideration of the relationship between risks of increased stalking, harassment and abuse and wider contextual factors including the rise in 'incel' content and misogynistic influencers which have been shown by numerous research publications to have a direct impact on the normalisation of misogynistic abuse online. Greater recognition must be given in the 'recommender systems' section of the guidance to the role played by algorithms and search functions which direct harmful traffic and result in further harmful content being recommended. • It is right to highlight that women are far more likely to be at risk of serious harm as a result of these behaviours. Our research showed that, in 12 of the 21 categories of online abuse investigated, women reported higher levels of victimisation. Abuses such as intimate image abuse, cyber stalking and cyber flashing were significantly more likely to be experienced by women.[3] • There are some intermittent references in this chapter to intersecting risk factors such as age and race. However, I am concerned that the links between these risk factors are not explored in the depth they warrant. It is well documented, for example, that female politicians from BME and marginalised backgrounds receive disproportionate amounts of harassment and hateful messages on social media platforms such as X and Instagram, compared to their white counterparts.[4] It is crucial to recognise that gender and race are factors which compound this abuse, and must not be treated in isolation. • Finally, I wish to highlight the problems associated with introducing strictly defined 'illegal harms' to deal with crimes such as stalking and harassment, where the offence is derived from course of conduct. There is a risk that patterns of behaviour are not picked up due to individual posts or messages not flagging as illegal. Tech companies should be encouraged to adapt their policies to ensure patterns are recognised.

[2] The Impact of Online Abuse: Hearing the Victims' Voice - Victims Commissioner

[3] Ibid

[4] Black and Asian women MPs abused more online | Amnesty International UK

Question (Volume 2)	Your response
	6F. Hate offences • Many of the issues identified in the previous chapter also relate to hate offences. In particular, I would urge this chapter to focus more on algorithms and search functions which direct harmful traffic and result in further harmful content being recommended. • Again, it is extremely concerning that the subsection on 'Services enabling online community building' within 'Risk factor: Service types' simply accepts as a given that services can be used by users to build online communities which facilitates the spread of hateful content among like-minded users. The guidance recognises the serious impact this can have by referring to a study which examines the role of the internet in facilitating violent extremism, but proposes nothing suggesting that tech companies should take it upon themselves to prevent this from being possible in the first place. • A similar point can be made regarding subsection 'Advertising-based revenue model' within 'Risk factors: Business models and commercial profile'. Ofcom should be much bolder in restricting sites' abilities to use hateful content to drive user engagement and derive profits through advertising as a result. **6G. Controlling or Coercive Behaviour (CCB)** • As already discussed in reference to 'Stalking, harassment, and threatening behaviour', this chapter requires more recognition and analysis of the fact that controlling and coercive behaviour often takes place online and offline. • Location tracking and the use of children to track/monitor/control victims needs to be highlighted as there is copious evidence of this. This is double pronged in terms of the impact and harm on children and the victim. • Online theft of documents, paperwork etc. by perpetrator(s) as a form of CCB has not been addressed here. This would be useful in creating a more well-rounded and holistic picture of the harm - particularly digital passport information and immigration documents for migrant victims.[5] **6L. Extreme pornography offence** • I am aware that Professor Clare McGlynn has submitted evidence to this consultation. I would like to directly reference and echo some of her submission on extreme pornography:

[5] Insights on the impact of coercive control on children and young people (nspcc.org.uk)

Question (Volume 2)	Your response
	• There is no consideration of the wider impacts of extreme pornography on society or the more up-to-date research on the impact of pornography through it's 'sexual scripts'. This research focuses on pornography broader than 'extreme pornography', however it is still relevant and useful for its discussion of harm which goes beyond the specifics of the very particular 'extreme pornography' offence. • The guidance rightly notes that 'direct effects' evidence will always be inconclusive, due to insurmountable ethical barriers. However, it is wrong to say that regulation should only be shaped by 'direct effects' evidence. This approach ignores the wealth of research on how pornography influences 'sexual scripts'[6] and the impact of pornography on attitudes and harmful sexual practices. The government's own research that 'there is substantial evidence of an association between the use of pornography and harmful sexual attitudes and behaviours towards women'.[7] • Further, the focus on 'no conclusive evidence' is in direct contrast to the approach of the draft guidance in relation to other harms where there is reference to harms despite there being a 'lack of direct insight'. In relation to other offences, the broader context of why an offence was introduced is taken into account in establishing the nature of the harms, explaining the need to take such harms seriously and therefore the need for action from internet service providers. Similar statements could and should be made in relation to extreme pornography, explaining that provisions on pornographic images of rape (non-consensual penetration) were introduced due to the harmful nature to society of its widespread impacts and that these images normalise sexual violence against women. • When considering a civil regime which is requiring service providers to design systems to reduce harms, instead of trying to prove the unprovable (with 'direct effects'), the onus should be on those objecting to regulation to demonstrate there is no effect of extreme pornography. Our attitudes and behaviour are shaped by our social environment which includes pornography. It is, therefore, reasonable to expect it to be one contributing factor to a culture which normalises and minimises sexual violence.

[6] Bridging the Theoretical Gap: Using Sexual Script Theory to Explain the Relationship Between Pornography Use and Sexual Coercion - PubMed (nih.gov)

[7] The relationship between pornography use and harmful sexual attitudes and behaviours (publishing.service.gov.uk)

Question (Volume 2)	Your response
	6M. Intimate Image Abuse • This chapter fails to recognise the severity of the threat posed by deepfakes, despite the sharing of these images being an offence under the Online Safety Act, and does not give sufficient recognition to the differences between deepfakes and 'traditional' intimate image abuse. • The risks posed by deepfakes need to have a much more prominent place in the guidance. The importance of this cannot be overstated, as sharing of deepfakes is fundamentally different to traditional intimate image abuse – the existence of nudify apps and other open-source software mean that people are at risk of deepfakes of themselves being created and shared if they do so much as little as upload a photo of their face. Discussion of deepfakes in this chapter is severely limited and inclusion of references to deepfakes as a form of intimate image abuse comes across as 'box-ticking'. • Domestic abuse should also be given greater prominence as a risk factor for becoming a victim of intimate image abuse. My predecessor's report on online abuse found that 44% of people experiencing intimate image abuse were victimised by a partner or ex-partner. The vast majority of women who experienced threats of intimate image abuse from their partners or ex-partners also experienced other forms of abuse demonstrating that, as with all forms of domestic abuse, threats rarely occur in isolation.[8] • I am aware that the Domestic Abuse Commissioner has called for extending the recommendation of hash-matching to intimate image abuse, and I am supportive of this. • It is also crucial to recognise cultural nuances that affect the impact and harm experienced by users. Whilst I am glad that there is some recognition given to the fact that the impact of intimate image abuse can vary substantially based on an individual's personal circumstances and the cultural or social context, I am worried that this approach only considers the different impacts of the same type of images, rather than giving consideration to the fact that 'intimate images' will have different meanings in different cultural contexts. I would welcome more flexibility around the understanding of 'intimate images' being a broader concept in some religious communities and amongst some minority ethnic communities. It is important that the guidance reflect the need for nuance and flexibility around this, and prioritises the harm experienced by the victim above generic assessments of perceived harm.

[8] The Naked Threat (refuge.org.uk)

Question (Volume 2)	Your response
	6O. Fraud and Financial Services offences • It would be useful for this chapter to discuss how users' personal characteristics affect their levels of risks for different types of harms experienced. There is some discussion of how some victims are more likely to fall victim to a romance scam, because of their personal risk factors, but little recognition is given to the nuance of the harm that can be experienced in these cases. Short-term emotional and long-term psychological harm can be just as impactful as financial loss, and should be discussed as part of this guidance. **6S. Cyberflashing offence** • The guidance rightly notes that cyberflashing is most prevalent amongst young people. However, it is important to note that whilst around half of women aged 18-25 reported having been cyberflashed, this figure is much higher for girls aged under 18, at 74%.[9] This finding is echoed by the report of the schools' regulator in England, Ofsted, which found that the vast majority of girls (9 in 10) said that being sent sexual images, being coerced into sharing images, or having their images re-shared was common.[10] This suggests that age is a risk factor; yet this is given very little discussion in the guidance. • High rates of cyberflashing victimisation amongst under-18s should also be considered in the context of the normalisation of misogynistic abuse online, as discussed in response to the chapter on 'Stalking, harassment and threatening behaviour'. • The guidance should include reference to the act of cyberflashing by 'AirDrop' images in public. This method of cyberflashing is unique as the victim is not likely to know who has sent them the image and there is no built-in feature to allow for tracking and viewing AirDrop transfer history. As images can only be airdropped between phones within 30 feet of each other, the act of being cyberflashed via AirDrop is particularly intimidating for its victims as it creates a very real, proximal threat. There needs to be separate reference to this unique threat, and more onus placed on tech companies with AirDrop-like features to instil safety by design.

[9] Teen Girls' Experiences Negotiating the Ubiquitous Dick Pic: Sexual Double Standards and the Normalization of Image Based Sexual Harassment - UCL Discovery

[10] Review of sexual abuse in schools and colleges - GOV.UK (www.gov.uk)

Question (Volume 4 and 5)	Your response
General feedback on Volumes 4 and 5	I have some overarching concerns about the apparent assumptions that underpin the guidance: **Mitigating risk of illegal harms** There is an undue focus on retrospective measures such as takedown and blocking which emphasises action by the person who is on the receiving end of the abuse and does not consider safety by design or the ways in which companies facilitate abuse as per the intention of the Act. Ofcom should consider targeting design choices which intentionally perpetuate misogynistic/ harmful behaviours. For example, by algorithms which drive traffic to harmful content. Despite the legislation being predicated on the consensus among civil society and parliamentarians that self-regulation and the voluntary initiative of tech companies will not prevent harms or make the internet safer, as explored at length in the online harms white paper and asserted by parliamentarians during the passage of the Bill, Ofcom have made an assumption that tech companies will comply with and adopt best practice approaches. Fundamentally, because these companies are commercial enterprises, profit and the bottom line are usually their main motivating factors, this rarely translates to making extra effort to keep people safe. There is considerable evidence to suggest that companies do not even adhere to their own terms and conditions. In the research conducted by my office (cited above) 43% of respondents reported the abuse they experienced to the internet companies. There were even higher levels of dissatisfaction expressed with the internet companies than with the police, with 65% of respondents indicating they were dissatisfied or very dissatisfied with the response they received from them. The majority of those who reported wanted the companies to prevent the abuse. Other research such as that undertaken by Refuge last year demonstrates similar findings. This suggests that platforms are not adhering to their own processes and so a new approach to compliance is required. OFCOM has relied too heavily on existing best practice which as demonstrated above is a low bar. As this guidance development is an iterative process, starting with such a low bar also risks further dilution. This is likely exacerbated by the inaccessibility of the consultation, as outlined in my letter.

Question (Volume 4 and 5)	Your response
	Explicitly because civil society organisations are less able to respond to this and ongoing consultations whereas tech companies whose motivations are more likely to be the bottom line rather than human rights or safety will have the resource to provide robust responses, it is hard to envisage anything other than further dilution. The assertion that company size should dictate the onerousness of measures they must undertake to address harms, risks missing those companies who may have lower traffic but cause very high harm. **Approaches to assessing illegal content** The interpretation of 'reasonable grounds to infer' criminal activity has taken place is restrictive in nature and there is a reliance on the very high criminal burden of proof even though this is guidance is a civil regime and does not functionally serve the investigation or prosecution of crime. Additionally, this approach misses the contextual harm and systems approach needed to target perpetrators and tackle harms. The intention of the act was to police a civil regime as well as a criminal one. For example, as Prof. Clare McGlynn outlines in her response, this focus on criminal thresholds means there is an unjustified introduction of a new, high threshold for when acts of strangulation and choking should be considered 'life-threatening' and therefore constituting extreme pornography. This misses the fact that medical consensus is that any act of strangulation can be life-threatening and there is no 'safe' way to undertake it. It is not possible to predict what reaction individuals will have or what type of act will be 'safe'. The guidance should be based on its' status as a civil regime, aimed at designing a system to reduce and prevent harm. If that were the case then on the balance of probabilities, it would be reasonable to infer that depictions of strangulation (not needing to be 'extreme') may constitute extreme pornography and therefore steps should be taken to reduce their prevalence. As outlined elsewhere in this response in human rights terms the focus of the guidance centres around users and companies and so there is little to no focus on collateral human rights such as the collateral impacts on women's human rights.

Please complete this form in full and return to IHconsultation@ofcom.org.uk.