WARNING: This consultation response contains language and/or material that may be distressing

domestic abuse commissioner

Victims Commissioner

22nd May 2025

Sent via email to: Ofcom Consultation Team (OS-Section54@ofcom.org.uk)
Copied to: Melanie Dawes, Ofcom Chief Executive Officer

Ofcom Consultation: A Safer Life for Women and Girls Online — Practical Guidance for Tech Companies

We are writing jointly in response to Ofcom's consultation on the draft guidance *"A Safer Life for Women and Girls Online."* As statutory consultees, established via the Online Safety Act 2023, we welcome the opportunity to contribute to this important piece of work.

As Commissioners responsible for improving the response to domestic abuse and victims of crime across England and Wales, we have long observed the increasing prevalence and severity of tech-facilitated abuse and online harms disproportionately targeting women and girls. The online environment has become a key extension of abuse, coercive control, stalking, and harassment, and as such, online safety is inseparable from women's and girls' physical safety and right to live free from violence and fear.

We commend Ofcom for having a prioritised focus on the issue of online gender-based violence and abuse. We also strongly support the emphasis in this guidance on governance, accountability and risk assessments (Actions 1 and 2). However, internal mechanisms alone will be insufficient. To achieve best practice and accountability, in any field, it is imperative that we refer to the relevant specialist sector.

Whilst we welcome the reference to collaboration with experts in relation to abusability and product testing (Actions 4, 5), to inform safer default settings, collaboration must be a standing expectation across the board. We therefore recommend that Ofcom require – explicitly within the guidance 'foundational steps' – tech companies to collaborate with and resource independent specialist services in the domestic abuse and violence against women and girls (VAWG) sectors. This expertise is essential to the development of effective, survivor-informed policies, procedures and support, and robust scrutiny.

We also have concerns about the efficacy and ambition of the guidance as currently drafted and wish to highlight these in this correspondence, alongside opportunities we believe would strengthen the guidance. These concerns and recommendations are set out under the themes of:

1. Enforceability and framing
2. Categories of harm
3. Support for victims
4. Transparency and data-sharing
5. Prioritising safety over profit

We will turn to each of these themes in turn, and would welcome the opportunity to discuss them further with relevant leaders at Ofcom.

Enforceability and Framing

We take into account the need to categorise harms and that, as misogyny is not a criminal offence, many of the harms we are concerned about sit in the 'harmful but legal' category. Unfortunately, this process of categorisation means that many of the actions which address these harms are set out as 'good practice steps', which tech companies are not mandated to follow. We are therefore deeply concerned as to their enforceability. Throughout this letter we will reference a number of measures currently included in the 'good practice steps', which we believe should be strengthened to 'foundational steps'.

Further, while the 'foundational steps' in the guidance are rooted in the 'Codes of Practice', which tech companies have a duty to implement, the wording used and framing of the guidance nonetheless could potentially give the impression that following these steps is voluntary.

We are aware that the specialist VAWG sector is calling for this guidance on protecting women and girls to be upgraded to a statutory Code of Practice to ensure enforceability, and for the 'foundational steps' to be renamed 'minimum steps', to emphasise that these are the industry standards that tech companies must follow. We support these recommendations. The guidance must make clear that tech companies have a duty to implement these 'minimum steps', or face enforcement action from Ofcom. It must emphasise throughout the responsibilities and duty of care already imposed on tech companies within the existing Illegal Harms and Children's Codes of Practice.

Proactivity

We welcome the 'good practice steps' that place the onus on the tech company to take action, rather than relying on victims to keep themselves safe. These include encouraging tech companies to engage with subject matter experts and victim-survivors to inform their work on online safety (Actions 4 and 5), as well as promoting the use of hash-matching to detect intimate image abuse (Action 6). However, as 'good practice steps', there is no requirement placed on tech companies to follow these recommendations. We believe that these should be made 'minimum (foundational) steps' to better guarantee their implementation.

The active nature of perpetration

While the guidance rightly acknowledges the significant risk of online abuse to women and girls, we are concerned by the use of passive and ambiguous language throughout. References to women "experiencing" harm risk obscuring the active nature of perpetration.

We urge Ofcom to adopt language that more clearly reflects the agency of perpetrators and the coercive, aggressive nature of online harm. For example, "women and girls subjected to abuse" rather than "experiencing harm."

The right to digital safety and participation

It is vital that the guidance goes further in recognising how the right to freedom of expression can be intentionally misused and weaponised against women and girls. While protections for freedom of speech are crucial, the guidance must be clear that the right to express oneself online does not extend to the right to harass, intimidate, or threaten others—nor should it come at the expense of women's and girls' safety or freedom from abuse.

We urge Ofcom to make explicit that safeguarding rights and ensuring digital participation for women and girls includes protecting those who speak out about sex-based rights and experiences of abuse. These voices are often silenced under the

guise of “harmful content,” and the guidance must actively prevent such misapplication.

Intersectionality

It is critical that the guidance consistently applies an intersectional lens. Women and girls from minoritised communities often face heightened risk, greater barriers to accessing support, and are disproportionately impacted by both online and offline forms of abuse. Every effort must be made to ensure that tech companies design their risk mitigation and prevention approach with the most vulnerable victims and survivors in mind.

Case Study 15: *Automated detection of misogynoir content and results* powerfully highlights how misogynoir can be detected and removed. For the guidance to sufficiently recognise and emphasise the intersectional nature of VAWG and the experiences of marginalised groups, this must be made a ‘minimum (foundational) step’.

We strongly recommend further engagement with ‘by and for’ specialist organisations to refine this lens, in a way which best values their time and expertise and reflects the resource and capacity constraints they face.

Categories of harm

We are pleased to see domestic abuse included among the four key categories of online gender-based harm, as well as an improved understanding of the complexity of domestic abuse and the co-occurring nature of online and offline domestic abuse. However, to effectively represent the harm being caused online to women and girls the four harms included in the guidance require further consideration and expansion.

Interconnection of online and offline harms

We are disappointed to see that so much of the guidance pertaining to the need to consider online and offline harm holistically sits solely in the ‘good practice steps'. It is imperative that tech companies understand that a single incident online could very likely be part of a wider course of conduct. Isolated ‘legal’ behaviour(s) online can and do often constitute illegal behaviour(s) when considered within the wider context of offline harm. There needs to be clarity as to the expectation on tech companies in these instances and the quality of support available to victims and survivors. This should span across both ‘minimum (foundational) steps’ and ‘good practice steps’.

Cyberstalking

Further, in the context of the online and offline co-occurrence of harm, the omission of cyberstalking as a standalone category is deeply concerning. We feel this is a

critical gap in the guidance. We are pleased to see reference to online harassment in the context of domestic abuse, but cyberstalking can occur independently of domestic abuse and is frequently experienced as part of a broader pattern of control and surveillance in the offline space. The impact can be devastating, leading to psychological trauma, social withdrawal, and is linked to risk of physical harm. Its increasing prevalence, especially among young women and girls, must be reflected in the guidance, as too should the lack of reporting by those most at risk of harm.

The Suzy Lamplugh Trust has reported that 100% of calls to the National Stalking helpline involve an online element[1]. There are concerns across the specialist VAWG sector that the lack of specific reference to cyberstalking in the guidance deprioritises this harm type and will further hinder reporting and positive outcomes for victims and survivors. Cyberstalking, like all forms of stalking, is a course of conduct offence, however incidents of abuse are frequently viewed in isolation which risks mis-categorisation, mis-recording, minimisation and ultimately inaction. To ensure tech companies appropriately discharge their duty to prevent illegal harms we would like to see cyberstalking included as a standalone category.

Emerging spaces and harms

Online VAWG is an evolving issue, and while we recognise that many harms take place on social media and user to user-based platforms, the guidance misses other important and emerging online spaces. For example, there is no exploration of perpetration of VAWG in online gaming and the metaverse.

Recent cases of virtual or meta-rape demonstrate why these spaces and the companies who 'provide' them must be included in the guidance. This is an emerging area, so encouraging good practice and safety by design principles now could help prevent future harms.

Online misogyny

It is crucial that the guidance recognises how behaviours that are not explicitly illegal contribute to both a conducive context for illegal harms and the broader normalisation of violence against women and girls. To strengthen this guidance, rape culture and its impact online and offline must be explored.

The increasing problem of boys and young men becoming radicalised into extreme misogyny online, often by misogynistic influencers[2], has recently been the focus of much public discourse following the Netflix show 'Adolescence'. The guidance must build on this public awareness and concern and go further in exploring the

[1] Ofcom consultation 2024- Suzy Lamplugh Trust
[2] Influencers radicalising boys in 'terrifying' way, say police - BBC News

consequences of online misogyny and emphasising the importance of early interventions to prevent illegal harm.

Explicitly, as tech companies have a duty to prevent illegal harms, highlighting the potential for escalation (for example from a threat of sexual violence online) may encourage tech services to implement 'good practice steps' to prevent illegal harms – and the risk of Ofcom enforcement action should they fail.

Girls' experiences

The guidance should also take the opportunity to go beyond the existing Children's Codes, by setting out the specific experiences of girls online, and how these differ to those of women. It is essential that tech companies understand how girls are targeted online and the specific harms that they are disproportionately subjected to. For example, the Internet Watch Foundation found that 97% of 278,492 reports containing CSA imagery showed the sexual abuse of girls only[3]. They also report that the majority of 'self -generated' CSA images are of girls.

We support NSPCC calls for Child Sexual Abuse and Exploitation to be included as specific harms in this guidance to ensure online platforms design and deliver appropriate risk mitigation and harm prevention strategies.

Support for victims

We are clear that tech services must do more to support victim-survivors and recognise their needs both online and offline. This includes engaging with criminal justice agencies and the specialist VAWG sector.

Reporting and advice

Action 3 outlines 'good practice steps' to encourage tech companies to create appropriate reporting processes. These include supporting victims to build a case, rather than each incident reported being recorded as a single act. As a 'minimum (foundational) step', it should be mandated that all behaviours that could be part of a wider course of conduct are recorded comprehensively. This must be done in a way that ensures the best outcome for victims and survivors; linking incidents where applicable from the point of reporting.

In addition, the information and advice tailored to victims after a report must consider the case-specifics. For example, in some cases where both online and offline harm is occurring, simply blocking the offender could lead to harmful offline behaviour, and the loss of evidence. As a 'minimum (foundational) step', tech companies must engage with the specialist VAWG sector to ensure they obtain expert advice on how

[3] IWF 2024 Annual Data & Insights Report

best to support victims. Any engagement with the specialist sector should include consideration of the very real resourcing issues they face, and measures which would support them to engage in a way which best values their time and expertise.

Criminal proceedings

As the guidance applies to criminal offences, there must be further consideration as to how tech companies can support victims of crime looking to progress criminal cases, as well as ensuring their access to rights under the Victims' Code. This includes the right to be referred to specialist support services. Consideration must be given, however, to the additional demand this may place on these services, and the resourcing necessary to meet this demand.

In a survey completed by the Open University, 56% of victims reported their concerns to the online platform, but only 4% to the police[4]. Informing victims of their option to report a crime committed against them online, or offline should be a 'minimum (foundational) step' included in this guidance. This would ensure that online platforms help victims of abuse to recognise the illegality of the harm committed against them and could help encourage victims to report such crimes to the authorities. This would allow for prevalence to be better understood, emerging trends to be identified, and action to be taken by Police as appropriate.

Victims seeking to collect evidence of the online harm they have been subjected to often report encountering barriers when requesting a data trail from online platforms. It is vital that victims have access to this data, and tech services should be obligated to provide it on request. However, consideration must also be given to the policy surrounding this process to ensure there are adequate safeguards to prevent perpetrators mis-using the process to obtain information about, or perpetrate further abuse on, their victims. We recommend that online platforms consult with subject matter experts when designing this policy.

With this in mind, we would like to see further exploration of the role tech companies should play in the sharing of information and evidence to policing, particularly with regards to sharing information relating to an act perceived as legal in isolation, but illegal when considered as part of a wider course of conduct.

Furthermore, when abuse is occurring across different platforms, data sharing between tech companies can also help to build a complete picture of abuse and/or perpetration which could help reduce or prevent harm both to individuals, in individual cases and more widely by understanding pattens of perpetration.

Transparency and data-sharing

[4] O. Jurasz, 'Online violence against women: A Four Nations study' (The Open University, 2024) p.74

Data-sharing is paramount to the prevention of online harm and the safety of all users, particularly children, marginalised and vulnerable people, women and girls. We welcome the inclusion of transparency measures (Action 3) and recommend that gender-based harms be established as a standing metric in all Transparency Notices for categorised services.

The prevalence of harm women and girls are subject to online and offline concurrently, and the pervasive use of tech in our day-to-day lives means there is no platform, service or device that does not have the potential to facilitate gender-based harm if misused or abused. There is therefore no tech company that could evidence a lack of risk or justifiable ground to be excluded from reporting against this issue.

We would further recommend Ofcom work with the specialist VAWG sector to inform a framework of indicators to determine a baseline requirement in Transparency Notices. This should include the option to add to data requirements on a 'notice by notice' basis, allowing for deep dives into specific themes, where and when required and appropriate. We would also encourage Ofcom to require all data be disaggregated by gender and age to ensure clarity on the specific impact on girls, as well as women.

We would also welcome guidance to encourage tech companies to engage with national and local strategic need assessment processes, and wider information sharing processes to inform prevalence data, cost analysis, and service design.

Risk mitigation

It is essential that data-sharing and reporting mechanisms are trauma-informed and prioritise survivor safety. Particularly in cases of domestic abuse and stalking, reporting abuse may significantly escalate the risk of harm to a victim or associated person.

The guidance currently advises tech companies to 'exercise caution' in the process of data-sharing, to reduce the risk of identifying a victim or pro-social bystander. We would like to see the advice to 'exercise caution' in all references to data-sharing and reporting, in both 'minimum (foundational) steps' and 'good practice steps'.

We would also be reassured to see a recommendation to all tech companies to co-develop a risk mitigation plan specifically relating to reporting and data-sharing. This would help to reduce the margin for error in this very fragile space. We would again encourage that this be co-developed with the specialist sector.

Prioritising safety over profit

A clear driver of online gender-based harm is misogyny and gender inequality, which are, unfortunately, too often amplified by parts of the media, influential content creators and commercial brands. The guidance currently offers limited recognition of

how commercial incentives—such as algorithmic content promotion and monetised misogyny—perpetuate harmful narratives and facilitate abuse, and how this may further undermine any steps to create safety that are not mandated. To prevent profit being prioritised over safety and to ensure 'safety by design' is embedded from the outset, tech companies must be encouraged to consider how business models can inadvertently contribute to gender-based harms, and how this can be mitigated against.

Conclusions

We thank Ofcom for the opportunity to contribute to this important consultation. The draft guidance, while a positive step, remains non-binding in many critical areas. We are concerned that without clear statutory mandates or regulatory consequences, the 'good practice steps' will not be implemented by tech providers at the scale or pace required.

It is also clear to us that if the specialist VAWG sector is not engaged in the development and delivery of all aspects of the guidance, then it is at risk of becoming tokenistic at best, and obsolete at worst.

We have made various recommendations to engage the specialist VAWG sector throughout our response, but we must also reiterate the concern of funding and resource across this sector. It must be resourced to do this work, in a way that is sustainable and proportionate to risk and need. There is a clear objective to increase reporting of online gender-based harm throughout this guidance, which is likely to increase demand for support. As such, it would be irresponsible not to consider the uplift required in capacity to meet this need and demand.

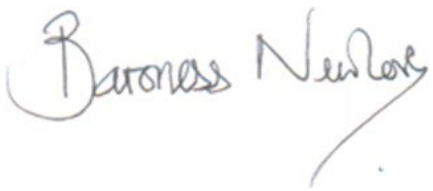
Whilst we acknowledge that questions of resourcing extend beyond the remit of this guidance and consultation, we would like to make clear nonetheless that we support calls from the specialist VAWG sector[5] to government to ringfence tax collected from tech companies to fund preventative online gender-based violence work.

There is much progress to build on, and we look forward to continued engagement with Ofcom. We are committed to supporting the implementation of strong, survivor-centred regulation and would welcome a meeting to discuss our recommendations in more detail.

Yours sincerely,

[5] General Election 2024: VAWG sector's manifesto calls on political parties to end violence against women and girls for good | End Violence Against Women

Dame Nicole Jacobs
Domestic Abuse Commissioner for England and Wales



Baroness Newlove LLD (hc) DCL
Victims' Commissioner for England and Wales