



Your response

Question	Your response
<p>Question 1: Do you have any comments on our proposed approach to 'content and activity' which 'disproportionately affects women and girls'?</p>	<p>Confidential? – N</p> <p>Although we understand that the guidance applies to all services, we are concerned by the statement made in section 1.24 of the accompanying documentation. It states that Ofcom's focus will be "on those services with the highest reach or highest risk for online-gender based harms." Smaller platforms can be sites of high risk and harm for women and girls, even when they are not directly accessing them. Our research indicates that smaller online forums and seemingly innocuous discussion threads contain harmful content and facilitate community discussions of how to enact online domestic abuse, such as co-opting smart home devices for surveillance and control. Therefore, we feel it is important these sites are addressed too to ensure accountability and reduce opportunities for harm.</p>
<p>Question 2: Do you have any comments on the nine proposed actions? Please provide evidence to support your answer.</p>	<p>Confidential? – N</p> <p>Action 2: Conduct risk assessments that focus on harms to women and girls</p> <p>We concur with section 2.50 that gendered harms do "get broadly overlooked" and that the potential risks of online domestic abuse have been missed due to assumptions that strangers pose the most risk to women and girls online.</p> <p>We encourage risk assessments to also consider that someone might not be explicitly threatened online but could still be experiencing online domestic abuse. Some abusive behaviours of current and ex-intimate partners are also missed as they might appear innocuous at first glance (e.g., location sharing). It is the pattern and escalation of behaviour that should also be considered in the risk assessments.</p>

Question	Your response
	<p>Action 3: Be transparent about women and girls' online safety</p> <p>The ability to monitor behaviours related to online domestic abuse is key for informing research, platform, and support service responses to emerging harms, increases in behaviours, or new behaviours (such as the abuse facilitated by smart home devices) within the context of online domestic abuse. Our concern is that there are only a small number of categorised services that are subject to transparency notices by Ofcom. Without a clear picture of the nature and scale of gendered online harms, it will be impossible to accurately understand how, why, and when harms are occurring.</p> <p>Action 4: Conduct abusability evaluations and product testing</p> <p>We agree with the inclusion of abusability evaluations in the list of actions and believe it is a key step to understanding how perpetrators can co-opt technologies to facilitate coercion and control. Therefore, we also agree that “those conducting the tests should be familiar with the specific nuances and dynamic of online gender-based harms” (4.17, draft guidance).</p> <p>We feel it is especially important to embed lived experience and subject matter expertise into the abusability evaluations to ensure that points of compromise reflect the nuances of domestic abuse and perpetrator tactics. Therefore, we suggest that the guidance should be amended here from “particularly valuable” to “imperative” (4.17, draft guidance).</p> <p>Action 5: Set safer defaults</p> <p>We welcome this action and agree that “safer defaults can also embed better consent practices in service design” (4.23, draft guidance). Regular reminders of who has access to the device/account and to what data would also be useful for promoting consensual use and limiting opportunities for smart home devices to be used maliciously.</p> <p>Action 6: Reduce the circulation of content depicting, promoting or encouraging online gender-based harms</p>

Question	Your response
	<p>We agree with considerations of how to reduce the “safety work burden on those having to report individual pieces of content” (4.32, draft guidance).</p> <p>However, we are concerned that not all content related to tactics of online domestic abuse will be captured as it might not explicitly depict or encourage gender-based harms. In our experience, the online harm that is related to domestic abuse is not always about the content itself but about the repetition of behaviours or unwanted contact. For example, seemingly innocuous behaviours can be about establishing a sense of omnipresence by the perpetrator (tracking location, access to accounts, sending repeated messages). Identifying the coercive and controlling elements of these behaviours can be challenging so these nuances need to be embedded in guidance to reduce the circulation of harmful content.</p> <p>Action 7: Give users better control over their experiences</p> <p>While we agree with this action for user autonomy, we are concerned this may burden users with the responsibility to keep themselves safe online and across different platforms. Users should be given better control over their experiences, but providers must be proactive in addressing online harms on their platforms and in responding to reports of abuse.</p> <p>X recently changed its blocking feature¹ to allow profiles to access content of an individual that had blocked them. This is particularly problematic in the context of online domestic abuse, as this may exacerbate the reach of a perpetrator’s control and provide them access to potentially sensitive information about the target.</p> <p>1. https://www.bbc.co.uk/news/business-66550959</p> <p>Action 8: Enable users who experience online gender-based harms to make reports</p> <p>A wider network approach to reporting online gender-based harms is needed. For example, when a user makes a report about online domestic abuse, the platform should signpost them to specialist support services (e.g., Refuge) for additional support. In addition, it is crucial</p>

Question	Your response
	<p>that platforms also follow up with users and/or Ofcom outlining what actions (or not) have been taken following a report. This would ensure the reporting process is more transparent and provides users with key support information.</p> <p>Action 9: Take appropriate action when online gender-based harms occur</p> <p>Case study 24 outlines the key challenges with taking appropriate action in the context of online domestic abuse. We agree that domestic abuse training, which focuses on the nuances of abusive dynamics, is needed to better identify instances of this harm and respond to user accounts sensitively. However, how companies could be encouraged to work with frontline services to provide this training to content and search moderators is unclear in the foundational steps (5.24, draft guidance).</p> <p>Overall, our concern is the enforceability of the action points and how this will tackle online gender-based harms. Given the voluntary nature of the guidance, many of the key points raised are optional as they are not integrated into codes of practice. In light of recent political developments and the commentary of Elon Musk² and Mark Zuckerberg³, we are not confident that platforms will engage with additional steps unless they are more enforceable.</p> <p>Technology abuse was recognised as a national threat and strategic priority for police in 2023⁴ with clear expectations around implementation. Controlling and coercive behaviour and harassment, stalking, threats, and abuse are considered illegal harms under the illegal harm codes and as such, we believe that the examples of good practice pertaining to these behaviours (which relate to online domestic abuse) in the VAWG guidance should feature in the illegal harms code and be legally binding.</p> <p>2. https://www.telegraph.co.uk/business/2025/02/16/tech-quit-britain-online-safety-act-warn-musk-google/#:~:text=Uber%20also%20criticised%20the%20plan,regime%20would%20capture%20their%20worldwide</p>

Question	Your response
	<p>3. https://www.theguardian.com/technology/2025/jan/11/tech-giants-told-uk-online-safety-laws-not-up-for-negotiation#:~:text=While%20he%20did%20not%20single,number%20of%20laws%20institutionalising%20censorship</p> <p>4. https://www.vkpp.org.uk/assets/VAWG-STRA-PUBLIC-OFFICIAL.pdf</p>
<p>Question 3: Do you have any comments about the effectiveness, applicability or risks of the good practice steps or associated case studies we have highlighted in Chapter 3, 4 and 5? Are there any additional examples of good practices we should consider? Please provide evidence to support your comment.</p>	<p>Confidential? – N</p> <p>Action 1: Setting policies defining and preventing “forms of gendered harm such as stalking, harassment, and intimate image abuse” is listed as a good practice step. However, we feel this should be a foundational step to ensure platforms tackle these harms on platforms (see 3.13). We feel domestic abuse or coercive control should also be listed here.</p> <p>We agree the forums, such as those sharing explanations of how to monitor your partner, should be a foundational step to tackling harm, as our research suggests these can be sites of significant risk for women and girls.</p> <p>We agree with 3.13 (c) which states that platforms should engage subject matter experts with experience of supporting survivors of gender-based harms. This should also be considered in 3.13 (d) to ensure staff training, particularly for those involved in setting policies, is designed or delivered alongside specialist organisations or experts.</p> <p>Action 2: We agree that platforms should engage with targets of abuse and the specialist services that support them. Consideration of cross-platform collaboration could be key for addressing perpetrators who use different platforms to harass their target and designing safeguards.</p> <p>Action 3: All platforms should be required to be transparent. This could be particularly impactful in cases of online domestic abuse where coercive and controlling behaviours are</p>

Question	Your response
	<p>proliferated across different platforms or devices. Therefore, sharing of information between platforms could build a picture of offending when it comes to course of conduct crimes like harassment or coercive control. If multiple sites flag or report a user for abusive posts, this could indicate patterns of controlling behaviour.</p> <p>Action 4:</p> <p>We concur that for abusability testing to be effective and reflective of the nuances of online domestic abuse and other forms of gender-based violence, those conducting the tests should be familiar with the dynamics of gender-based violence. We feel it is imperative that subject matter experts are consulted on these tests.</p> <p>Action 5:</p> <p>While we agree it is important for children to be protected under the foundational steps for default settings, we are concerned that other users are overlooked. For example, 4.26 i and iii should be expectations for all users. Protecting the location information and visibility of accounts is important in the context of domestic abuse as it can limit the reach of perpetrators particularly if a partner is trying to escape.</p> <p>In addition, removing geolocation information by default should be a foundational step. The consequences of geolocation information are highlighted in case study 9, so we feel this step should be more enforceable.</p> <p>Action 6:</p> <p>Several of the good practice steps are not appropriate for tackling cases of online domestic abuse. In 4.40 (a), nudging may be a key tool for addressing content that is explicitly harmful. Behaviours relating to domestic abuse are rarely conducted in isolation so the assessment of single pieces of content may not provide the full picture of harm. Instead, some content (messages or photos outside the home for example) may not seem harmful on their own, but could cause the target significant distress and harm and be part of wider pattern of coercion and control. Similarly, the section on automated content moderation outlined in 4.43 (b) would need to identify</p>

Question	Your response
	<p>repetitive and non-consensual behaviours as some content in isolation may not seem harmful without context.</p> <p>Action 7: While 5.15 (f) is a key step, we feel it should be considered foundational to signpost all users to supportive information which addresses specific harms, such as domestic abuse. It could be integrated alongside 5.14 (f) which only applies to children.</p> <p>Action 8: In line with our previous comments, any exit button should take a user to a safe page to prevent the risk of escalating harm.</p> <p>Action 9: Particularly in situations where an offender has been convicted or served with a protective order, we are concerned that platforms respond inadequately to requests to remove posts. This can cause further harm to a victim and allows the abuse to continue. Therefore, we feel steps set out in the guidance need to go beyond good practice and are foundational steps in promoting the safety of women and girls online.</p>
<p>Question 4: Do you have any feedback on our approach to encouraging providers to follow this guidance, including our proposal to publishing an assessment of how providers are addressing women and girls' safety? Do you have any examples or suggestions of other ways we could encourage providers to take up the 'good practice' recommendations?</p>	<p>Confidential? – N</p> <p>We suggest that some terminology (e.g., 'foundational') could be changed to reflect the minimum standard that platforms must meet to be compliant with their duties in protecting against VAWG online.</p> <p>We are concerned that the guidance is not mandatory for providers and are sceptical that companies would implement steps without incentives or enforceability. We agree with the Online Safety Act Network's commentary that although the guidance might not have a legal effect, it should not mean that the actions can be totally ignored by providers⁵. Ofcom does have enforceable obligations relating to carrying out a 'suitable and sufficient' risk assessment in relation to illegal content risks (of which controlling and coercive behaviour is one).</p>

Question	Your response
	<p>We agree that publishing data on how providers enforce their policy and the effectiveness of safety features allows for a clear assessment of what works. We are encouraged that transparency reporting could equip stakeholders with knowledge about the safety practices of providers. However, this requirement (3.25, draft guidance) needs to expand beyond categorised services to ensure we have a clearer picture of responses to online VAWG and ensure all platforms are accountable for upholding the safety of their users.</p> <p>5. https://www.onlinesafetyact.net/analysis/ofcom-s-draft-guidance-on-protecting-women-and-girls/</p>
<p>Question 5: Do you have any comments on our impact assessment, rights assessment, or equality impact assessment? Please provide any information or evidence in support of your views.</p>	<p>Confidential? – N</p> <p>We welcome the best practice highlighted throughout the guidance but feel this should be the minimum standard for mitigating online harms experienced by women and girls. The draft guidance states that “it does not mandate any new requirements”, which suggests it will have limited power in getting online platforms to improve the ways in which they respond to VAWG.</p> <p>Rather than relying on service providers to voluntarily follow best practice and respond to harm retrospectively, we believe that the guidance should impose more responsibility on platforms to proactively prevent and address abuse occurring on their platform.</p>
<p>Question 6: Do you agree that our draft Guidance is likely to have positive effects on opportunities to use Welsh and treating Welsh no less favourably than English? If you disagree, please explain why, including how you consider the draft Guidance could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh</p>	<p>Confidential? – Y / N</p>

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

Question	Your response
and treating Welsh no less favourably than English.	

Please complete this form in full and return to OS-Section54@ofcom.org.uk.