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

Your response

Question	Your response
Question 1: Do you have any comments on our proposed approach to 'content and activity' which 'disproportionately affects women and girls'?	Confidential? – Y / N
	We are concerned that stalking is not adequately covered by the four focus areas identified by the draft guidance (i.e. online misogyny, pile ons and online harassment, online domestic abuse, image-based sexual abuse). Indeed, only around half of all callers to the National Stalking Helpline are stalked by a current or ex-intimate partner (National Stalking Helpline data for the year ending March 2024). Stalking is a unique and highly complex crime which cannot be subsumed within online domestic abuse. The Trust defines stalking as a pattern of fixated and obsessive behaviour which is repeated, persistent, intrusive and causes fear of violence or engenders alarm and distress in the victim. Stalking can include many types of unwanted behaviour such as regularly sending flowers or gifts, repeated or malicious communication, damaging property and physical or sexual assault. These behaviours therefore do not always present as harmful and might not have misogynistic undertones. Additionally, stalking is usually perpetrated by one individual towards another, meaning that stalking behaviours are not covered within "pile-ons and harassment" which was described in the guidance as "cases where groups of coordinated perpetrators target a specific woman or girl, or groups of women and girls" (Draft guidance, 1.10). Although we acknowledge that stalking is a priority illegal harm under the illegal harms code, the guidance is an opportunity to instruct providers on how to go above and beyond when responding to certain forms of online harms. Whilst there are pertinent suggestions and examples of how providers might do this for stalking throughout the guidance (i.e. case studies 13, 17, 20, 23), the focus areas mean that stalking as a specific form of harm is often subsumed within, or confused with, other forms of online harms such as domestic abuse, harassment or coercive

Question	Your response
	control. For example, in 2.29 the guidance provides an overview of coercive control. The example used of a perpetrator posting a picture of a door as a way to intimidate and distress someone could also be considered stalking were it to occur as part of a course of conduct of stalking behaviours. We would therefore want the guidance to explore best practice specifically for stalking in more depth and ensure that stalking behaviours are not confused with other crimes. Whilst we understand that the guidance does apply to all services, we are worried by the statement made in 1.24 of the accompanying consultation document which states Ofcom's focus will be "on those services with the highest reach or highest risk for online gender-based harms." Small platforms can be sites of extreme harm for women and girls as highlighted in our response to the Illegal Harms Code consultation. In our experience, smaller sites can be where some of the most significant harm and extreme content is situated for women and girls. Stalking specifically often occurs across multiple platforms regardless of their size.
Question 2: Do you have any comments on the nine proposed actions? Please provide evidence to support your answer.	Confidential? – Y / N
	Action 1: Ensure governance and accountability processes address online gender-based harms We concur with the guidance that "effective governance and accountability processes provide the foundation for service providers to identify, manage, and review risks to their users". However, we are concerned about the reliance on "senior leaders setting it as a priority" (see 3.8, draft guidance). There is a need to ensure that accountability processes are enforced externally rather than being defined internally by platforms themselves. Internal decisions can easily be subject to change or reversed altogether, as highlighted by the recent rollback of Meta's policies around 'hateful conduct' (The Guardian, 2025). These concerns were echoed during the passage of the Act when there was widespread acknowledgement that business initiatives had not gone far enough, and "without the right incentives, tech companies will not do what is needed to protect their users."

Question	Your response
	Action 2: Conduct risk assessments that focus on harms to women and girls As pointed out in the draft guidance, gendered harms do "get broadly overlooked" and intimate partner violence online has been missed due to assumptions that strangers pose the most risk to women and girls online (see 3.14, draft guidance). We would add that stalking behaviours, whether by an ex-intimate partner or not, are also missed since they might at first glance appear innocuous. It is the pattern of behaviour which causes alarm and distress in the victim, and which is a crime. Therefore, it is important to embed understanding that someone might not be explicitly threatened online but could still be experiencing online harms such as stalking. **Action 3: Be transparent about women and girls' online safety** We acknowledge that only a small number of categorised services are subject to transparency notices by Ofcom. However, without clear visibility and oversight around the scale of gendered online harms experienced by users on platforms it will be impossible to build up a picture of where and how harms occur. Indeed, our report *Unmasking Stalking: A Changing Landscape* found that there was a significant rise in online stalking behaviours, aligning with evidence documented by the National Stalking Helpline of an increase in cyberstalking during the same period. Being able to track the increase in cyberstalking behaviours would enable platforms and specialist stalking services to respond to emerging harms and new behaviours within the context of stalking. In the context of stalking, transparency reporting and information sharing between platforms themselves could help both sites and victims to build up a picture of offending across sites and profiles. Stalking is a course of conduct crime which requires an evidence base of repeated, fixated and obsessive behaviours to demonstrate it as a crime. Data sharing and transparency across and between sites would enable better evidence gathering, enabling the victim to demonstrate a course of conduct of stalking and platforms to more efficiently respond to it. For example, the Trust has long called for all dating platforms to monitor if a user's profile has been previously removed on their platform or other similar platforms following abusive behaviour (see case study 1). *Case study 1: Jason Lawrence is a serial rapist who targeted women he met through online dating platforms Match.com and*

Question	Your response
	Dating Direct between 2009 and 2014. Despite four victims having reported his behaviour to Match.com, his profile was not removed, and he went on to rape and assault multiple other victims. **Action 4: Conduct abusability evaluations and product testing** We welcome this action and see it as a critical way of ensuring that products are approached through a 'safety-by-design' lens. We also agree that "those conducting the tests should be familiar with the specific nuances and dynamics of online gender-based harms" (see 4.17, draft guidance). We would amend the wording from "particularly valuable" to "imperative" that platforms "partner with subject matter experts who have experience of supporting survivors and victims when conducting such exercises" (see 4.17, draft guidance). In 4.15, the guidance must include stalking when it states that "Perpetrators of online gender-based harms can be very innovative in co-opting technologies to facilitate pre-existing patterns of harassment, coercion and control" (draft guidance). **Action 5: Set safer defaults** We concur that setting default safety measures are "particularly important for harms like stalking" (see 4.25, draft guidance). It is crucial that users are clearly informed when these default measures are changed. **Action 6: Reduce the circulation of content depicting, promoting or encouraging online gender-based harms** Platforms should not only remove content "swiftly" when it is illegal but also when reports are made. We elaborate further on this in answer to question 3 (see 4.33, draft guidance). Additionally, we are concerned that not all content that would form part of a course of conduct of stalking would necessarily fit in or be captured here since it might not be explicitly depicting, promoting or encouraging online gender-based harms. Indeed, the online harm that comes from stalking is not necessarily about the content but primarily the repetition and the fixated and unwanted nature of the contact.. By virtue of being unwanted and repeated, these can have a huge impact on the mental health of those who are targeted. It is critical that at a minimum all posts that are evidence in stalking cases where the perpetrator was convicted be removed. **Action 7: Give users better control over their experiences**

Question	Your response
	Users should be given better control over their experiences, but platforms must be proactive in responding to reports of and addressing the proliferation of online harms across their platforms to ensure that the burden does not fall on users to protect themselves across sites. For example, X recently changed its rules to allow profiles that an individual has blocked to still see what that individual is posting in its public posts. In the context of stalking, this means that a victim might post sensitive information believing that a perpetrator who has been blocked is unable to see this. **Action 8: Enable users who experience online gender-based harms to make reports** Platforms must not only enable and encourage users to make reports in a simple and clear manner when harmful behaviours occur but should also signpost to specialist services for additional support. For example, if a user makes a report of stalking behaviours, the platform must provide them with information regarding specialist stalking services like the National Stalking Helpline. We also want the guidance to make clear that not only are more transparent reporting mechanisms crucial, it is imperative that platforms also feedback to users and/or Ofcom on what has been done following a report. **Action 9: Take appropriate action when online gender-based harms occur** This is key in responding to online harms. In the context of stalking, we know that it can be incredibly difficult for victims to get platforms to take down offending posts even when the perpetrator has been convicted of a stalking offence. Platforms must be swift and efficient in removing content, particularly when the person posting the content has been convicted of a crime such as stalking and those posts were used as evidence in court. We would also argue that anyone convicted of stalking must be banned across the whole platform and prevented from creating new accounts. **Our overarching concern with all of these action points is their enforceability**. **The guidance**, and much of this content, **remains optional for platforms** as they are not integrated and set within legally-binding codes of practice. We are sceptical that platforms will take these extra steps without an enforcement mechanism backing them, particularly in light of recent political developments in the United States and comments made by Mark Zuckerberg and Elon Musk (see here and here). Furthermore, **stalking is**

Question	Your response
	designated as a priority illegal harm under the illegal harm codes and as such, we insist that the examples of good practice pertaining to stalking set out in the VAWG guidance should feature in the illegal harms code and be legally binding.
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.	Confidential? – Y / N
	Chapter 3: Taking Responsibility **Action 1:** We are concerned in 3.13 (a) that setting policies defining and prohibiting "forms of gendered harm such as stalking, harassment and intimate image abuse" is listed as a **good practice step** for services to take. **This should be a foundational step** in tackling these forms of harms on platforms. We agree with 3.13 (c) which stipulates that platforms should be consulting with subject matter experts, particularly those with experience of supporting survivors of gender-based harms. We would want this reflected in 3.13 (d), so that training staff involved in setting policies is done in consultation with and alongside specialist organisations such as specialist stalking services. In Case Study 2, we want it made clear that setting a policy, in this case a sexualised harassment policy, is the first step in tackling those behaviours. It is imperative that the policy is enforced and that actions are taken against users who breach these policies. **Action 2:** We welcome the emphasis on the need to consult victim-survivors as well as the specialist services that they support. In Case Study 5, dating platforms are highlighted as sites where users are at particular risk of abuse, including stalking. Stalking is a course of conduct crime, and we know that for many users the

Question	Your response
	stalking behaviours will not be confined to one site or platform. Dating platforms are often the initial meeting site but perpetrators might start stalking their victims across various other platforms after this. This should be reflected in the case study to prompt platforms to think about how they could safeguard victims when the majority of behaviours are being experienced on other sites. Platforms should work alongside each other and specialist stalking services to design policies and reporting mechanisms that address these concerns. **Action 3:** Transparency requirements should apply to all platforms. We believe that transparency could also mean sharing of information between platforms, such as flagging repeat offenders to other sites or monitoring patterns of concerning behaviours across multiple platforms in order to build up a picture of offending when it comes to course of conduct crimes like stalking. For example, if multiple sites flag a person for harassing posts this could indicate stalking. **<u>Chapter 4: Preventing Harm</u>** **Action 4:** Any abuseability testing should take into account how the platform interacts with, and how users might be present across, different platforms. For example, many platforms have a 'people you might know' feature which points users towards profiles they might have connections to on other platforms. It is crucial that, if a stalker connects with a victim on one platform, they are not pointed to the victim's profile on other sites as well. **Action 5:** We are concerned that most of the foundational steps regarding default settings only apply to children. These should apply to all users across all sites. For example, as per the example given under action 4, "Child users are not presented with prompts to expand their network of friends or be included in network expansion prompts presented to other users" should apply to all users online. We agree with 4.29 (a and b) which stipulate a number of interactions defaults and privacy defaults. It should be clearly stipulated that users' profiles should be set to private by default and that having a public profile should be an opt-in choice. We also agree with 4.29 (e) around users being able to see users and IP addresses currently connected to an account. This should

Question	Your response
	however **not be a good practice step and should be a foundational part** of any platform design. Similarly, removing geolocation information by default should also be a foundational step. The harms this may cause are evidenced in case study 9 of the guidance and we are concerned that this is set out as a good practice step rather than an obligatory one. **Action 6:** We are concerned that many of the good practice steps set out under action 6 would be largely ineffective in the case of stalking. For example, nudging (4.40 (a)) is a useful tool when addressing explicitly harmful content. However, stalking behaviours can appear innocuous when assessing content in isolation. The prompt around content being harmful would therefore not appear when a user is posting a seemingly harmless photo or post yet the outcome would still cause the victim significant distress and alarm. There is an important need to accompany features such as blocking (see 4.41) with relevant information related to course of conduct crimes, including signposting to specialist support services such as the National Stalking Helpline. Whilst blocking might provide some respite for users experiencing stalking or harassment, blocking or disabling comments may mean that the escalation of communication is not picked up and the subsequent risk is missed. On certain apps, such as Snapchat, blocking a user results in the activity and messages is deleted, thus destroying evidence of stalking behaviours. It is therefore important that users have access to specialist independent support on stalking or harassment no matter what course of action they choose to pursue. Similarly, implementing a time out feature (4.41 (b)) wouldn't necessarily be effective in tackling stalking either. Stalking is characterised by the obsessive, unwanted and repeated nature of the behaviours, meaning that a perpetrator's account being frozen is unlikely to deter them and might mean they create a new profile or stalk the victim on a new site. This feature must therefore be backed up with a feature that prevents the creation of new accounts to avoid perpetrators from circumventing protection mechanisms. This type of feature is laid out in 4.42 (e) but the guidance could better illustrate the need for these features to be interlocking so that they work effectively in tandem. Automated content moderation (see 4.43 (b), draft guidance) wouldn't always be effective against stalking as the content itself

Question	Your response
	might not appear harmful out of context. It would need to pick up repetitive behaviours which are unwanted by the victim. In case study 13, users should also be signposted to specialist services alongside receiving "a supportive message with information about how to report and block users on the service". **<u>Chapter 5: Supporting women and girls</u>** **Action 8:** Any exit button must not only take the user out of the reporting system but also to a safe page. We are particularly supportive of 5.20 (e) and the accompanying case study 23, as reporting behaviours on other platforms is crucial in building up a picture of offending when it comes to stalking. Case study 20 is not only pertinent to harassment but also to stalking and we would want this highlighted. Whilst we agree that users should be able to report offences occurring on other platforms, it is important that users can also inform platforms of behaviours occurring offline too. Many stalking cases will include a proximal element as well as an online element. By failing to make this link, there is no reference to the links between online and physical violence (see case study 2). This is despite stalking being positioned at stage 5 of 8 stages on Professor Jane Monkton Smith's homicide timeline. We are therefore concerned that tech platforms will not understand stalking as high risk, despite the increased risk of escalation that stalking poses (see case study 3). *Case study 2: Caroline Hallam met Matthew Ghent through Match.com. They dated for 6 months during which he was very controlling. He began to stalk her when the relationship ended, bombarding her with 70 emails and phone calls, trying to deposit money into her PayPal account, booking a holiday for them even though they had broken up, turning up at her work place… Ghent was able to report Hallam to Match.com and get her profile blocked, despite having been convicted and sentenced for stalking her.* [redacted]

Question	Your response
	[redacted] **Action 9:** We are concerned that platforms are reluctant or slow to take down offending posts, particularly in the context of stalking where individual posts might not be perceived as harmful but are illegal when considered within the context of a course of conduct of stalking. We know of victims whose perpetrator has been convicted of stalking or served with a protective order, yet platforms continue to refuse to remove the offending posts. This perpetuates the alarm and distress these posts can cause victims. This is why it is imperative that the steps laid out in the guidance are not seen as good practice but are foundational steps in ensuring the safety of women and girls online. Regardless, the guidance must emphasise that if a perpetrator has been convicted of an offence where some of the behaviours took place online, the platforms must immediately remove those posts. As highlighted in our answer to question 2, a key issue with much of the guidance is that it remains optional. As demonstrated by Meta's rollback of its hateful conduct policies, it is clear that these changes are not something technology companies and online platforms will opt into willingly. **This guidance, including the changes pointed out above, should be more than good practice. This should be the foundational approach towards tackling violence against women and girls online.**
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	Confidential? – Y / N

Question	Your response
other ways we could encourage providers to take up the 'good practice' recommendations?	
	We welcome the proposal to publish an assessment of how platforms are addressing women and girls' safety in the wake of the publication of this guidance. It is crucial that any assessment does not give too much weight to reporting as an indicator of harm online. We know that the majority of survivors do not report, and this should not be the primary basis for the measure of safety for a given platform. A systems-based approach is needed to root out harmful practice and patterns of behaviour and not rely on reporting of behaviours by the victim. We remain concerned that the regime remains focused on processes that companies need to follow in a tick-box exercise in order to comply, particularly as many of the steps that go above and beyond are listed as good practice. The decision to format the guidance by separating out the good practice examples from the foundational steps further emphasises the 'optional' nature of the good practice. This is incredibly dangerous as we do not believe tech companies will implement these good practice steps unless forced to do so, as demonstrated by concerns raised during the passage of the Act itself when there was widespread acknowledgement that "without the right incentives, tech companies will not do what is needed to protect their users." However, the steps outlined in the good practice examples are closer to what we called for in the Illegal Harms Code consultation and represent, to us, the bare minimum that providers should be doing to ensure the safety of users, particularly women and girls, online. We also believed that the use of the term 'foundational steps' is misleading and should be changed to 'minimum steps'. Foundational could be interpreted as aspirational for tech platforms whereas minimum clearly communicates that these steps represent a baseline that platforms must meet to be compliant with their duties. We are troubled that Ofcom has stated that the guidance is not mandatory for providers to follow. We concur with the Online Safety Act Network's explanation that although the guidance might not have a particular legal effect, this does not mean that they are totally ignorable. Ofcom does have enforceable obliga-

Question	Your response
	tions relating to the requirement to carry out a 'suitable and sufficient' risk assessment in relation to illegal content risks (of which stalking is one). As outlined above, Ofcom has enforceable duties regarding the carrying out of 'suitable and sufficient' risk assessments. Its risk assessment guidance sets out the qualitative standards expected in platform's risk assessments. Although technically a best practice tool, Ofcom treats this guidance as more than optional, as it forms the basis for evaluating whether a risk assessment meets the required standards. A similar approach could be adopted with regards to the stalking elements of the Guidance on Women and Girls. Stalking is a priority illegal harm under Ofcom's codes and as such the best practice laid out in this guidance could be understood as forming part of a 'suitable and sufficient' risk assessment. The Online Safety Act was enacted to address all forms of online harm, including VAWG. Accordingly, Ofcom should interpret the *Guidance on Women and Girls* in the same way it is interpreting its risk assessment guidance. As argued by Professor Lorna Woods, the *Guidance on Women and Girls* discusses risks which might disproportionately impact women and girls and could therefore contribute to defining what constitutes a 'suitable and sufficient' risk assessment, much like the existing risk assessment guidance.
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.	Confidential? – Y / N
	The impact assessment highlights the relative lack of power this guidance will have in pushing online platforms to change the ways they deal with VAWG online. Indeed, the accompanying consultation document to the guidance states: "Overall, we do not think the draft Guidance will impose any significant burdens on service providers. This is because the draft Guidance does not mandate any new requirements." The best practice highlighted throughout the guidance should be the bare minimum when it comes to tackling VAWG online.

Question	Your response
	We are also concerned by the focus on cost which seems to be understood by Ofcom as costs to service providers. This understanding does not take into account the costs to society, with VAWG estimated to cost the UK an estimated £40 billion each year.[1] We therefore believe that the guidance should impose a more stringent duty on platforms to prevent harm occurring their platforms rather than relying on service providers to implement best practice voluntarily and respond to harm when it has already occurred. 1. Scottish Government. 2023. "Violence Against Women and Girls – Independent Strategic Review of Funding and Commissioning of Services: report." Available at: https://www.gov.scot/publications/violence-against-women-girls-independent-strategic-review-funding-commissioning-services-report/pages/12/.
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 and treating Welsh no less favourably than English.	Confidential? – Y / N

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