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

Ofcom VAWG Guidance Consultation Transcript

Maeve Walsh, OSA Network:

Thank you to everyone for joining the call today. I'll start with a few pieces of housekeeping and then some opening remarks on the context for this discussion before we get into the detail.

This meeting is an opportunity for the expertise and insight across the VAWG sector to be consolidated and presented to Ofcom as evidence in their consultation on their guidance on protecting and women and girls online. I'm delighted to be chairing the discussion today and will do my best to ensure that everyone has a chance to contribute and that also we keep to time. The transcript of this discussion will then be tidied up after the call and, when finalised, will be submitted to Ofcom before their consultation closes in a few weeks time. We are also likely to produce a summary on the key themes for publication as well.

We have a number of key themes already identified and I'll be bringing in individual organisations to kick off the discussion on each of those themes, with space then for others to add their views. If we don't get the chance to cover all the angles on a particular theme, or there is more that you would like to have said or extra evidence that could be added to the final transcript after the meeting, then there will be an opportunity to do that. The key objective here is to make sure that we can provide Ofcom with the fullest picture on the sector's views and concerns.

The reason we are so keen to facilitate this engagement is because of the long-running interest and involvement of many of the organisations on this call in this particular topic. A number of organisations and experts on this call collaborated, way back in 2022, on the development of a code of practice on online VAWG - namely, NSPCC, 5 Rights, EVAW, Refuge, Glitch and Professor Lorna Woods and Professor Clare McGlynn. I was involved in my previous role as an associate at Carnegie UK and the OSA Network traces its roots back to the coalition building done during that period.

That code of practice (which is linked here) was a key component in the successful campaign to amend the Online Safety Bill, as it was then, to ensure there were greater protections for women and girls to address the disproportionate levels of harm and abuse they experience online. Ofcom's guidance would not be in existence were it not for that campaign and the code itself remains - in my humble opinion - an exemplary piece of work and set a template for Ofcom to follow, which I'm sure we'll return to in the discussion.

The collaboration and engagement during that code development has continued during Ofcom's implementation of the Act to date and it's important to put on record upfront that the guidance, welcome as it is, is only one part of the tools in the regulator's toolbox for reducing the risk of harm to women and girls online. Both the illegal harms codes of practice and the children's codes of practice are fundamental underpinnings for those protections. Unfortunately, they are nowhere near as strong as they should be - and that is something that the guidance, which sits

on top of them and which is not enforceable - cannot fix. So, before we look at the detail in the guidance, we would refer Ofcom back to the responses that we have previously submitted to their consultations on the illegal harms codes and the children's codes (which are linked here and here)) as many of the weaknesses which we flagged to them during those consultations remain.

So without further ado, I'm delighted to hand over to Rebecca Hitchen from the End Violence Against Women Coalition to start off our discussion today.

Rebecca Hitchen, EVAW:

Many thanks, Maeve, and thank you for your support in chairing and the support from the Online Safety Act Network in general, it's been hugely valuable for the sector. You mentioned some of the work that we've been involved in and we'd helped convene. It started off with the Principles for online safety in 2021 and that was the basis as well for a lot of the points that came through in the fuller proposal for a VAWG Code of Practice in 2022. We've done petitions alongside Glitch and also helped convene a joint oral submission like this for the Illegal Harms consultation, and, like you've said, a lot of the themes remain the same.

I do also want to flag that while the VAWG response that we have pulled together has been really powerful and excellent, it's important to note that a lot of frontline services, and a lot of other VAWG organisations, aren't able to engage in this level of quite deep complex policy work to the extent that they would like or offer support to survivors of online abuse due to chronic underfunding of the violence against women and girls sector, and that chronic and long term underfunding is particularly faced by 'by and for' services for black and minoritised women and girls, and those who support disabled women and girls. I think it's just really important to say that this is ever present for organisations doing this work and so hopefully in creating this submission, we can then summarise it so that other organisations are able to put their name to it because the level of input that's needed that has been needed across the passage of the Bill and in the work with Ofcom has been considerable.

So, to the guidance. We're going to use this session to talk about some of the areas which we feel need to be made stronger and some of the areas which are missing. Among them, and indeed the key one that Ofcom will be aware of, is the lack of enforceability. But I did also want to begin by talking and referencing a lot of the positive measures that we've seen in the guidance. I'll do a quick list now, but I know we may return to these in the discussion.

- Inclusion of intersectional data and racially disaggregated data as part of good practice in transparency
- Recommendation for external oversight
- Acknowledgement that survivors needs must be understood through co production
- Hashing technology to be used by platforms to address intimate image abuse

- Recommendation for platforms to give staff guidance on online misogyny, including gender-sensitive AI training and algorithm training
- Strike based system to address repeat perpetrators
- Tech platforms to partner with subject matter experts to evaluate their products usability in relation to VAWG
- Pornography removed from children's feeds

But these remain quite a low bar. We've had a number of concerns about the fact that this is guidance rather than a Code of Practice. One of the things which we have hoped for in this guidance was the fact that there could be more freedom with it being guidance rather than Code of Practice which could afford ambition and greater scope, but that doesn't really seem to be the case in this document. I know that we will go on to later the issue around take up the issue around how to measure the impact of this guidance and for us the key and central issue around the lack of enforceability.

Maeve Walsh, OSA Network:

Great. Thank you, Rebecca, for that.
Really important framing there and it is important to acknowledge some of the positives in the guidance and indeed where some of those have actually been included as a result of our pre-engagement with Ofcom which I think does deserve acknowledgement. We're going to start off with one of the big issues relating to this whole area and Ofcom's wider approach to the implementation of the Act, which is safety by design, so I wonder if we might be able to bring in Professor Lorna Woods from the University of Essex and the expert advisor to the Online Safety Act Network to kick off that part of the discussion.

Lorna Woods, University of Essex:

Thank you, Maeve.
Talking about safety by design links to a fundamental idea in the Online Safety Act, section 1(3), which says that services should be "safe by design". As Ofcom recognises in its document, the idea of safety by design doesn't have a single or agreed meaning, and so Ofcom takes a particular approach and that is what we might call looking at the temporal scope of safety by design.

If I can summarise, it requires thinking about safety by design right from the initial product specification and design of a product or a feature, through to its deployment through to its maintenance on to the end when it is going to be retired. And this is good start and I think we acknowledge that is one aspect of safety by design, but, as I think is implicit in the consultation, it is not the only aspect to safety by design. So I'd like to flag up two other aspects to safety by design which could be taken into account and which would support Ofcom in achieving that ambition that services should be safe by design.

The first aspect of this is the sort of features that are taken into account, the technical scope rather than the temporal scope. This is just to reiterate that when we are thinking about how services are designed, we shouldn't just be looking at the end of the communication chain - takedown measures and the like - but we should be looking all the way through and ensuring

that from account creation and the incentives for content creation to the distribution and through to the way that users engage with services and content. Safety should be part of each of those stages, and although there is some recognition at some of these points, more could be done, particularly at the early point of the distribution chain, and I suspect when we get onto more detailed discussion that some of those points will come through.

Perhaps the more significant aspect is the question of priorities. What do we expect a designer or a product manager to be doing when they consider safety by design at the beginning, at the middle and at the end. What are their priorities? And I think we can take a look at the UN guidelines on business and human rights, as well as other disciplines, for views of what safety by design implies. They say that there is a three-stage hierarchy here and that the priority should be to design out the risks, and that product safety should be a central function of the product. So the idea is you design risks out or you design them down, and only then do you start to look at how you mitigate/manage the risks and then the final stage is remediation for those risks that cannot be taken out and cannot be managed.
But it is important that the priority should be reduce or eliminate before we get to mechanisms to manage and to remediate. So that is a general framing that is in the guidance, but I think it would strengthen it.

Maeve Walsh, OSA Network:

Thank you, Lorna, that's really helpful, and obviously we've engaged quite a bit with Ofcom across their teams on the principles of safety by design and how we feel that both the Codes and this work could maybe have gone further too, so it's important to refer further back to that work as well. (Prof Woods' work on Safety By Design can be found here.)
I think [redacted] did you want to come in now from the End Violence Against Women Coalition (EVAW) perspective.

[redacted], EVAW:

Yes, thank you Maeve.

I think whilst Rebecca's already noted some of the positive safety by design measures that this guidance takes to address VAWG, we're concerned that the measures that will have the most impact are framed within the good practice section of the guidance, which relies on the goodwill of platform to implement, and, we'll be talking more about enforcement issues later on, but the foundational steps set out in the guidance are those which platforms need to take in order to comply with the Illegal Harms Code and the Children's Code, and illegally required platforms through this new regulatory system.

But we think the framing of these steps as foundational could be interpreted as aspirational for tech platforms, with a lack of emphasis on their new duties within that regulatory framework. Instead we want foundational sets to be changed to minimum steps, which would clearly communicate that these steps represent a baseline standard that platforms must meet to be compliant with their duties as set out within those two codes. I think this distinction is really crucial to avoid any misinterpretation by platforms that these measures are in any way optional

or flexible under the current framework. Minimum steps would also better reflect that platforms must go further to properly ensure women and girls safety is prioritised.

I'd also point out that whilst the guidance provides some detailed case studies relating to intimate image abuse and stalking which outline some positive steps, however their place within that good practice section, given that both stalking and intimate image abuse are listed as priority offences, should instead be placed in the minimum steps section to reflect the duties that platform have to protect their users from those offences.
Thanks Maeve.

Maeve Walsh, OSA Network:

Great. Thank you, [redacted].
I think now we might go to 5 Rights' [redacted], if you want to come in on some of your particular safety by design concerns.

[redacted], 5 Rights:

Thank you, Maeve, and thank you for the invite to speak.

You know for the reasons that Lorna so brilliantly outlined, it's worth understating how important adopting a safety by design approach is at keeping women and girls, and particularly children safe in the online world and I think it's welcome that the guidance itself seems to reflect some of those principles more deeply than the Codes of Practice.

It's not worth understating the fact that it is critical that tech companies are doing the due diligence involved in safety by design and actually tackling that harm upstream before it's manifesting, and then before the lives and well-being of children, and in particular girls, are put at risk. So on that basis, I just wanted to quickly set out one of the gaps that we've noticed at 5 Rights regarding the guidance specifically around business models within that risk assessment framework.

I think whilst the guidance, regarding the risk assessment, does broadly address some more gendered approach to risk assessment in what is asking companies to do, it's important that the full scope of those risks are explored and in particular from the business model 5 Rights has done a lot of work previously, notably our pathways research interviewing service designers, and there is a critical sort of interlink between the business models that drive those services and the design features and functionalities that are deployed specifically to achieve three things within the tech sector business model about maximizing reach, time and activity and engagement on the service. Designers were telling us that these would often take precedence over the well-being of children, and, more generally, help shape the behaviour of people, including children, on that service.

So I think one gap that the guidance has is the actual risk assessment itself doesn't consider how the business model in itself can be harmful, and I think it's worth stating that this is relating not only just to third party advertising but also how it's guiding specific design choices that could disproportionately impact girls. I think it's also worth stating that this also goes beyond the high

risk of harm from some of the things that are addressed in the guidance, but also to more nuanced harms, for example, the way that the business model could drive the implementation of things like beauty filters and beautification filters which encourage changes in perceptions in body image and reinforce narrow beauty ideals more broadly. I think it's worth saying that this is well evidenced, and we have testimonies from Facebook whistleblowers, notably Frances Haugen, and more recently Sarah Wynn Williams, which revealed how the advertising models are coming back to the business model which targets children when most vulnerable. An example that Sarah Wynn Williams gave was that after a girl had deleted a selfie was a good time for advertising in the business model to recommend beauty products on the basis that they may not have been feeling good about their appearance. So I think it's worth saying on that basis, if this guide is to be truly transformational, as it can be for changing these experiences online, Ofcom should provide a further recommendation for services or more explicit consideration to business model risks within the guidance specifically to women and girls and go beyond just that advertising structure, but also about the design features and functionalities that are not acting in the best interest of children and women and girls.

Specifically on top of this, I think one other gap within the guidance relates more to resourcing throughout the guidance. Ofcom first set out the expectations of what they want from services of specific sizes, natures and risks they may need to take on, and I think that it's important for encouraging initial uptake of this guidance, particularly as the group has already raised, that it is enforceable, so there needs to be sort of an incentive to uptake it. However, the guidance also needs to recognise that some services, if they really want to tackle these harms, will need to build that resource up in order to create that industry-wide step change for women and girls, and require allocations of a greater resource to do this. One of the examples within the governance actions is about establishing oversight mechanisms for trust and safety decisions, but one of the potential outcomes of these trust and safety mechanisms is that it's determined that there's not enough resource for the trust and safety team responsible for monitoring the specific harms and actioning those harms before they arise. Specific to women and girls, and 5 Rights recently published a report around trust and safety team specifically that emphasizes the importance that these teams are resource, and it's not just about the sort of material budgeting and human resource, but also about access as well between teams within a service. So, for example, making sure that the trust and safety team has adequate access to designers so they could talk about these decisions that are being taken in ways that they can be mitigated as well.

It's important that at this time where there's a big industry wide shift away from trust and safety specifically, I think that the guidance would really benefit from a recognition that to innovate in the name of protecting women and girls that a service may need to dedicate more of their resource and should dedicate more of their resource for that purpose.
Thank you.

Maeve Walsh, OSA Network:

Thanks, [redacted]. I think that's a really good point in terms of the general drift away from resourcing on this and for an ambitious guidance, or a guidance that is intended to push and stretch companies, then that's a really good point to include.

Can I come to NSPCC now, [redacted] I think you wanted to contribute some comments on this section.

[redacted], NSPCC:

Yes. Thanks Maeve.
Really agree with the comments we've heard so far this morning and particularly want to draw out the fact that wherever we're discussing safety by design, it's really important this is nuanced by consideration of an age appropriate design as well, and that we need to be appropriately nuancing the guidance to recognise experiences of girls specifically. I think the need for this can really be seen, particularly in action 5 and action 7, where the guidance is using language such as 'aiming for better and increased controls over settings' which really risks suggesting that for all users regardless of age more choices, more empowerment to alter settings away from those default high settings for children is appropriate, which we know that it isn't for children of all ages.

We recommend that the guidance goes on to explore a more age-appropriate approach and to consider examples like whether the safest settings and defaults should be unalterable for the youngest children. This isn't completely radical and new. This is something that's already been considered by platforms and as a stated aim of things like an Instagram Teen accounts, although there are some questions about whether this is being delivered. I'd also say similarly, as well as considering non alterable safety settings, it's really important to think about which features are appropriate for children and young people. There are some examples where things like quick ads, live streaming etc. incentivise behaviours which might not be developmentally appropriate or safe for some of those youngest users of services, so it's really critical that Ofcom support services to do more thorough analysis of whether each of these features they're offering is appropriate, and for whom.

A key point that research by 5 Rights and the NSPCC both highlight is that crucial to delivering these greater protections and safer designs for children is the ability to know which users are children of which ages. So robust age assurance is going to be an absolute key part of delivering safety by design that's more age appropriate for children. We think this is a massive oversight currently in the guidance and will be really keen to see the guidance echoing calls which are already made in the recently published Children's Code which recommends services look more at their use of age assurance because, as I said, it will be absolutely crucial for delivering safer products for children, and so it must be a key part of any discussion on delivering safety by design.

Thank you.

Maeve Walsh, OSA Network:

Thanks [redacted] and I think we're going to come back in, possibly in the enforcement section, to how the guidance links to the codes, and whether there is much more that Ofcom could be doing both to ensure that the guidance is properly stretching in a way that some of the codes measures aren't, but also that it sits very firmly within the risk assessment and that kind of broader regulatory approach from companies too. So I think that that's really helpful from a

design and age appropriate design perspective, and I know that Glitch also had some contributions they wanted to make on safety by design, but unfortunately we don't have someone on the call at present, so hopefully we'll be able to get their contributions added into the transcript after the meeting and we'll move on now to the topic of prevention, which links in a lot of ways to safety by design, but more broadly in terms of the sort of the tools and the types of support that might be useful for preventative measures. So if I come back to EVAW, Rebecca is going to come in here on media literacy.

Rebecca Hitchen, EVAW:

Yes, I won't go into too much detail on this because there's so much to go through, but we definitely welcome the systemic understanding of violence against women and girls prevention which is laid out in chapter four of the guidance, and it's good to see the focus on media literacy and education. There are definitely some positive measures highlighted, but the guidance then defers to the strategy set out in the media literacy guidance that Ofcom has recently published. We have definitely campaigned a lot for media literacy, it's something that we talk about in pretty much every conversation we have with the Department for Education, and we're also feeding into the development of the violence against women and girls strategy at the moment, but the concern is that there isn't enough dedicated resource or concern around media literacy.

The media literacy strategy that Ofcom has created is quite vague and unclear, the impact isn't measurable, and the overall strategy isn't really robust enough to do the challenging work that is needed when it comes to media literacy. It's a really fundamental part of tackling all forms of online harm, as well as violence against women and girls, and would have an impact on Ofcom's enforcement work if prevention strategies were properly implemented with and by tech companies, as well as by civil society and Ofcom. So we're really disappointed by the absence of detail that there is around the media literacy strategy and what will be delivered, a lack of clarity, and, like I said, the measures of success I think given that there was a focus on evaluation within the strategy, we would have expected more attention to how the implementation strategy itself will be measured and evaluated and a need, as with everything, for whenever you're sort of trying to implement any sort of training, the need for clear and dedicated resource attached to that. That's something that we haven't seen with the Department for Education and we haven't seen enough of it when it's come to Relationships and Sex Education and that has resulted in teachers not feeling confident enough to be able to approach certain issues like this that mainly relate to violence against women and girls because they can be quite sensitive and can be seen and felt as to be quite difficult. So, whereas I'm talking a fair amount about what happens in the classrooms and what happens there with children and young people, there is the glaring issue that media literacy needs to be for all society, and that's recognised in the media literacy strategy but there isn't enough clarity as to what that would actually translate to in practice.

Maeve Walsh, OSA Network:

Thanks, Rebecca. I suppose there's also a bigger strategic point here too, isn't there, in the context of the government's cross government work on their violence against women and girls target, Ofcom's role within the online space, but also then how well both support and should also stretch other parts of government, like the Department for Education or DCMS, as well as in the delivery of their wider objectives. So I think again it may be a little bit of a missed opportunity there in the sense of pushing that ambition further forward. And again, I think we probably will have some contributions from Glitch on the topic of media literacy at a later stage too.

Rebecca Hitchen, EVAW:

Absolutely.

Maeve Walsh, OSA Network:

I wonder now if we can come to [redacted] from Zero Tolerance to talk about your perspective on the prevention aspect here.

[redacted], Zero Tolerance:

Thanks.

So for those who don't know, Zero Tolerance is Scotland's expert organization on primary prevention, and so our focus is on tackling the root cause of violence against women and girls, which is gender inequality. It's our experience as an organisation that non violence against women sector stakeholders often confuse the terms prevention, early intervention and crisis intervention, and when they're taking action they can often come at the intervention level rather than at the primary prevention level.

Looking at Section 4 of Ofcom's draft, we can see that it's framed as harm prevention. But we're concerned that this is going to create confusion as tech companies attempt to implement this, because what the content of the chapter, or the section, actually focuses on is harm reduction. It's about deterring perpetrators from perpetrating violence when they're already at the point of wanting to do something, consciously or subconsciously. Primary prevention is about addressing attitudes and culture across society, so that fundamentally violence against women and girls is unimaginable, and deterring people at the point of perpetration almost becomes unnecessary because we've changed society so much.

So instead, Zero Tolerance would strongly recommend renaming this section of the guidance to harm reduction, because it's focused on reducing harm to women by men who are consciously or unconsciously already seeking to perpetrate violence against women and girls. We're happy to provide more support to Ofcom with clarifying definitions outside of this meeting. If that's helpful, please just get in touch.

Despite this chapter being focused around harm reduction, there is a really important role for tech companies to play in primary prevention, activity and stopping violence against women and girls across society. For tech companies, primary prevention activity would involve deprioritising sexist content, promoting gender transformative content in their algorithms, removing gender

normative language from dating services, and supporting women to have an equal voice on platforms, for example. It's about building gender equality into the subtle, everyday norms of platform and removing the conducive context in which violence against women and girls take place.

Zero Tolerance would really like to see more of this in the guidance. If the guidance is to aim for best practice, then primary prevention should certainly be part of that and we're really happy to support Ofcom with developing that as the work continues.

Maeve Walsh, OSA Network:

Great, thank you so much for that, [redacted] that's really helpful, and also for the offer to provide more of that detail for Ofcom to improve that section and hopefully change that section where necessary. I note that [redacted] from Glitch is with us now.
I don't know whether you're ready to speak or not, but if you wanted to contribute on media literacy, please go ahead.

[redacted] **Glitch:**

Hi everyone. Yes.
We put in a response to Ofcom's media strategy consultation alongside EVAW, and what we'd really like to see is the strategy and the guidance speak to each other.
We felt that the strategy was lacking in terms of ambition and overall vision for understanding the importance of media literacy for online safety, and the guidance doesn't really speak to that.

So what we'd really like to see is the media literacy strategy as part of the guidance showing Ofcom having a really proactive roleincluding resource from Ofcom being put behind the strategy because currently there doesn't seem to be any resource put behind it, and actually as part of the work around violence against women and girls, media literacy should be at the heart of that. Ofcom's own role should be in tandem with incentives for tech companies to take a proactive role in media literacy campaigns, upskilling and resources also. Media literacy work should be primarily linked to improving understanding how platform design decisions can contribute to harm and/or safety, to support users to make decisions that support their safety.

Maeve Walsh, OSA Network:

Great. Thanks so much for that, [redacted]
That's really helpful and definitely supplements what Rebecca said earlier as well.
OK, so I think we'll move on from prevention to look at gaps in the guidance and a lot of these are quite specific to some of the concerns of organisations on the call. So I will go first to NSPCC on the perspective of children and young people, [redacted] would you like to come back in on that?

[redacted] **NSPCC:**

So this is probably the key area for development that we wish to highlight at the NSPCC as currently there's a really stark gap around the experiences of children and girls. One of the strengths of the guidance is that it provides an opportunity to go beyond the codes and to be more ambitious as other people have referenced. So the logic that child sexual exploitation and

abuse has already been addressed in the code simply doesn't stand because this guidance is actually a unique opportunity to create some more ambition around protecting girls online from gender based harm.

We think that introducing child sexual exploitation and abuse as a fifth harm category will be essential for bringing out key recommendations and nuance throughout the guidance about the specific experiences of girls. For example, an important gap in the guidance relates to the detection of new child sexual abuse material. A distinct focus on child sexual exploitation and abuse would ensure that important issues are fore-fronted, such as the need to recommend proactive detection of unknown, new CSAM, which is not currently recommended in the Illegal Harms Codes. It is illogical for the Guidance to include hash matching for NCII but not new CSAM, despite both measures being absent from current Codes.

We also know that girls can and do have very different experiences to women. They're targeted in specific ways and have different experiences of using support tools like reporting. For example, from Childline, we hear a lot that with intimate image abuse girls believe, or are led to believe, that they might be prosecuted for self-generated intimate images. By applying a specific lens of age to online experiences of gender-based harm, really important recommendations start to come to the fore around the need for age-appropriate signposting and support for girls.

Also there are some really important examples in the guidance where Ofcom have overlooked the views and experiences of girls' and the language used reflects this. By focusing only on the women who experience domestic abuse, the guidance is misleading and helps to perpetuate this misconception that girls don't experience domestic abuse directly. Although we know that the legal definition is people who are 16 years and above. By overlooking the important fact that girls also experience domestic abuse and intimate image abuse, the Guidance fails to challenge misconceptions and overlooks important recommendations for services such as the need for specific training for moderators on abusive relationships in young people and the need for age-appropriate language and signposting support to girls who experience technology facilitated domestic abuse.

Then finally, I'd like to highlight that the guidance's current focus on social media among user-to-user services means that the risks and the recommendations specific to gaming are currently overlooked. NSPCC research on targeting girls online highlights that there are some really important specific routes for grooming which occur specifically on gaming sites such as the use of gift cards to establish unequal power dynamics between adults and children. It's important that examples like these are drawn out and that services are made aware of them so that appropriate recommendations can be extended.

So, to summarise, to properly address the experiences of girls online, we recommend that Ofcom uses child sexual exploitation and abuse as one of those harm categories for the guidance and adopts a more age sensitive analysis throughout, expands their focus to include gaming, and, crucially, actually engages with girls themselves to reflect on this guidance and say how much this reflects their experiences and where can we go further to make sure they're protected. Thanks.

Maeve Walsh, OSA Network:

Thanks, [redacted]
That was a really clear contribution there.
I should say as we're going through all of these sections, if there's anybody who does also want to add in anything or respond to anything that any of the other participants have said, please do just stick your hand up and I'll bring you in.
OK, we'll move now to [redacted] again from Glitch if you wanted to come in on your concerns about some of the gaps.

[redacted] **Glitch:**

I wanted to address the intersectionality framework used in the guidance. We were really pleased to see that applied through with a case study on automated detection of misogynoir and mentioned in relation to decision making in governance. We weren't sure, given the use of language, if the mention around governance and decision making was referring to intersectionality itself as a framework, or intersectionality as a word in a different sense so it would be good to have that clarified - we would support the former. Overall, the guidance should more clearly articulate how the intersectionality framework should be applied to practice i.e. Ofcom should put forward recommendations in the guidance that push providers to take context into account during content moderation, risk assessments, governance and decision making approaches. This would better ensure the guidance actually addresses harms against Black women and girls and other groups with multiple characteristics under the Equality Act 2010.

In case study 15 on automated detection of misogynoir content, we were again very pleased to see Ofcom thinking about this, but we wanted the case study to go a bit further. We think there's a gap there in terms of recommendations of how service providers could use a tool so they talk about the difficulty of defining misogynoir, but they don't actually go far enough to say this is how you could do it. First, the guidance must clearly recommend companies develop policies on misogyny and misogynoir to support the reduction of harmful content towards women and girls. Ofcom must also call on companies to change policies that allow misogynistic and misogynoiristic content (such as Meta's recent changes). Also, Ofcom should recommend alternative content moderation approaches such as instead of commonly used single binary classifiers to label content as harmful or not, content moderation can be designed as a cascade of binary multi-layer questions about the content, and its context. We will submit additional evidence on training models to look for misogynoir content..

Academics from the Open University have put together a paper on misogynoir, which is referenced in the guidance, and actually that paper does show that forms of misogynoir are much broader and more nuanced and complex than the more kind of extreme, stereotypical hate speech, and I think the same applies to misogyny and the way that misogyny is spoken about in the guidance in terms of the more extreme end being the most important for radicalisation, which is not necessarily the case. Actually, normalisation of harm is really key. Glitch will also be sharing a taxonomy for coding misogynoir directly with Ofcom, which we hope can support practical detection of misogynoir in many more forms.

Equally as important as detecting misogynoir, Black women and girls must have their speech and online experiences protected from inappropriate content moderation, particularly when engaging in counter-speech, intra-community dialogue or when sharing their own experiences in relation to discrimination, violence and harm. This is currently a gap in Ofcom's guidance.

Maeve Walsh, OSA Network:

Great. Thanks [redacted]
Thanks for flagging those additional submissions too. I'm going to come back to Suzy Lamplugh Trust now to speak about a few gaps and then on to Refuge after that.
[redacted] would you like to come in on stalking and course of conduct crimes.

[redacted], Suzy Lamplugh Trust:

As a specialist stalking service, our overarching concern with the guidance is that stalking and other course of conduct crimes are not adequately covered by the full focus areas that structure the guidance itself. Stalking is a unique and highly complex crime, and is completely distinct from other forms of harmful behaviours like online domestic abuse. It can include many types of unwanted behaviours, and these behaviours don't always present as harmful and might not always have misogynistic undertones. Stalking is usually perpetrated by one individual towards another, meaning that stalking behaviours would also not be covered within the pile-on and harassment focus area, which was described in the guidance as cases where groups of coordinated perpetrators target a specific woman or girl or groups of women or girls.

In the case of stalking, it's the course of conduct that's a crime, not necessarily the incident itself, and we're worried that the guidance doesn't underline this strongly enough despite evidence that tech platforms don't have a solid understanding of this.For example, we know of victims whose perpetrators have been convicted of stalking or are served with a protective order linked to stalking behaviours, yet platforms still refuse to remove the offending posts as they do not meet a threshold of harm despite these having been used as evidence at the trial itself.

The guidance is also an opportunity to instruct providers on how to go above and beyond when responding to certain forms of online harms, which we feel it doesn't do with regards to stalking. There are pertinent suggestions and examples of how providers might address stalking throughout the guidance, namely case studies 13/17/20 and 23, but the focus areas mean that stalking as a specific form of harm is often subsumed within or confused with other forms of online harms like domestic abuse, harassment, or coercive control.

We'd also like to emphasise what [redacted] mentioned earlier. These case studies could and should have formed part of the foundational minimum steps in tackling stalking, as it has been identified as a priority illegal harm. Addressing course of conduct crimes such as stalking also means building up a picture of where and how harms occur. Transparency around the scale of gender online harms experienced by users on platforms is therefore key, and we would argue that transparency reporting and information sharing between platforms could help both sites and victims to build up a picture offending across sites and profiles, enabling victims to demonstrate a course of conduct of stalking and platforms to more efficiently respond.

For example, if multiple different platforms are flagging a person for harassing posts towards one specific individual, this could indicate a pattern of stalking. Users should not only be able to report offences that are occurring on other platforms, it's also important that users are able to inform platforms of behaviours that are occurring offline as a result of the online behaviours. Too many stalking cases will include a proximal element as well as an online element and the escalation of one type of behaviour can indicate not only an increase in risk to the victim, but if online harms are allowed to proliferate this could exacerbate offline behaviours as well. By failing to make this link the guidance fails in informing platforms of the connection between online and physical violence, and the increase in risk to victims this indicates, particularly with regards to course of conduct crimes like stalking.

Maeve Walsh, OSA Network:

Thanks so much for that, that was really clear and some really strong examples where that can be strengthened. It's back to that issue again, isn't it, about where the guidance sits in relation to the codes and how the two should be reinforcing each other and a lot of the material in in the codes too. So we'll come to [redacted] now from Refuge, if that's OK.

[redacted], Refuge:

Thanks Maeve.
We completely endorse and agree with what colleagues from the Suzy Lamplugh Trust just shared. Following on from that, at Refuge we have a specialist tech facilitated abuse team and we've gone through the guidance with those experts on our team, as well as the Survivor Panel, and an issue they raised in terms of gaps is that whilst they really welcome parts of the guidance that talk about action against perpetrators, particularly repeat perpetrators, a really common challenge that they're having that isn't addressed in the guidance is that when an account is taken down or blocked or stopped for a period, perpetrators commonly just set up another one instantly under a different name, sometimes under the same name.

What survivors really want to see in this guidance is that tech companies are strongly encouraged to stop that happening. So when multiple accounts are set up from the same IP address, and the IP address has had some suspicious activity, they should be stopped from creating those accounts. I think there's a lot more that tech companies can be asked to do, particularly in the context of this guidance, and, as other colleagues have said, can be ambitious to use the information that companies have about their account holders to block and prevent further harm in terms of stopping the creation of accounts from the same IP addresses of those that have been blocked or stopped. So there's an addition we'd like to see there.

Maeve Walsh, OSA Network:

Great. Thank you, [redacted]. Really important as well to emphasise the expertise that you and Refuge bring to this assessment so that's really helpful. We're going to come on to some of the gaps around the treatment of pornography now.

If I can bring in [redacted] from CEASE first, that would be great.

[redacted] CEASE:

Thanks, Maeve. I think one of the things that we noticed in terms of the gaps is that while they do acknowledge pornography is a priority harm to children, there's a heavy focus on child protection rather than addressing the border or the role of pornography in shaping harmful norms with women and girls. What we wanted to highlight is the need to focus more on porn and also incest porn as well as a driver, for example, as a significant subcategory contributing to the normalisation of sexual violence, but there's no dedicated section that focuses on just porn as a cultural driver of violence against women and girls. I think they briefly mentioned it in terms of the fact that 12% of titles focus on this, but that's about it.

Alongside the focus on child protection, there's also little explicit mention on how inadequate age verification, and the lack of removal of harms from pornographic content, effects adults and also children in general, when it comes to escalating VAWG, so we'd like to see more of that. The other part that I also wanted to focus on in terms of the gaps was the absence of dedicated section on nudification apps. There is a broad area that's addressed in terms of deepfakes, but we'd like to see more in terms of how the nudification apps function, their accessibility, especially via search engines and mainstream platforms like apps, and also the effective disruption methods that will be applied.

The other thing we wanted to raise was just in terms of the lack of consideration of the risks that these pose. So, for example, when it comes to incest porn and nudification apps, how algorithms and all social media platforms are promoting this need to be considered, but this is not addressed within the document itself. Overall, I think mainly focusing on porn as a cultural driver overall, not just in relation to children, but also thinking more about the risk factors relating to nudification apps and incest porn.

Maeve Walsh, OSA Network:

Great. Thank you so much for that.
Professor Clare McGlynn, I think you were going to follow up then on some of the issues around the gaps relating to pornography.

Professor Clare McGlynn, University of Durham:

Yes, thank you.
I'd like to follow up on CEASE's comments and endorse them as well.
CEASE has made a number of comments as well about how the guidance does reflect some elements of pornography's role in promoting and sustaining misogynistic attitudes, so welcoming some of the elements of the guidance in relation to pornography. They also recommend that we do take some further steps, particularly in relation to recognising its wider role in sustaining and normalising a culture around sexual violence legitimates many forms of violence against women and girls.

Just a few points specifically. It's vital to emphasise that the role that pornography plays is not just on mainstream pornography sites, but across many social media sites. X actually has far more unregulated forms of pornography available now, compared to some of the mainstream pornography available sites. So those social media sites need to have particular oversight and enforcement action against them.

In relation to the drivers of violence against women and girls generally, there is evidence emerging of violent pornography, and not just illegal but violent pornography, as being a significant risk factor in harmful sexual behaviour, especially amongst young boys. So a significant risk factor is being identified such that it's making a difference to behaviours, particularly to the perpetration of sexual violence against young girls.

Also, in relation to pornography on choking and strangulation, Ofcom's guidance does provide some detail on the illegal nature of some of that material. However, it does not appear to cover all choking/strangulation porn, and there is very direct evidence about when individuals view more pornography, they end up viewing more choking and strangulation. They themselves acknowledge they then engage in more choking and strangulation. The medical evidence that is emerging is finding that frequent choking and strangulation is in essence giving young girls, in particular, brain damage at an early stage. So we need to be particularly mindful of all forms of choking and strangulation pornography.

I also endorse what CEASE said in relation to incest pornography, emphasising here that we are talking about pornography promoting sexual activity between family members, not just step mum as a kind of synonym for an older woman. We are concerned with material involving sexual activity between family members, particularly the incest pornography promoting sexual activity with very young girls. Not all of that material is unlawful at the moment, but the evidence is clear that it promotes and legitimises and strengthens incest conduct.
Thank you.

Maeve Walsh, OSA Network: Thank you. I think we're going to go back to [redacted] from Refuge now on some of the law enforcement issues.

[redacted] Refuge:

There are two elements around law enforcement that we'd really like to see added to the guidance. Survivors tell us that whilst the abuse experienced online is horrendous, one thing that they think could be helpful in their cases against their perpetrators is that, unlike some other forms of domestic abuse, there is a clear data trail and clear evidence linked to the abuse that is perpetrated against them online. However, in reality they're really struggling to access that evidence, and we know that police forces are also struggling to access that evidence from tech companies. When a survivor reports to the police and that case is taken forward, survivors are asking for two things to be added to the guidance - one is recommendations for how tech companies should cooperate in a timely fashion with law enforcement agencies with caveat that that should always be where a survivor has made a report, and the law enforcement agencies are taking action. We are not asking for or requesting tech companies to report individual cases themselves. But secondly, survivors really want to be able to quickly and easily download a record of the abuse that's been perpetrated against them on platforms and the action that they've taken to report or stop it, and survivors are telling us that they might speak to the police about having reported hundreds of bits of content and the responses from platforms together. It can form really valuable and vital evidence of the of things like coercive control, harassment, communications offenses that are perpetrated against them, but they find it almost impossible to

evidence that or demonstrate it. So there's some really practical measures that tech companies can take to support survivors who are being abused on their platforms.

Maeve Walsh, OSA Network:

Thank you, [redacted].
And just on that, well, both those points, certainly the last one, I remember being at an event in Parliament a number of years ago, and we were still trying to get the Code of Practice adopted, where exactly these issues were being raised. This is not something that's new and it's very much a practical aspect that should be a requirement on companies, so I think that absolutely is something where the evidence is there and it needs to be included in this document, so thank you for that.
Just mopping up now on any further gaps, I think Clare, you wanted to come back in on some human rights issues, and if there's anything else anyone wants to add in, do put your hand up or put a message in the chat now.

Professor Clare McGlynn, University of Durham:

I'd like to add to the discussion of gaps in the guidance.

On human rights, there could be revisions.Obviously Lorna Woods' explainer around these issues is particularly relevant. So I want to just highlight that whilst the Annex does refer to the human rights impact of online abuse on women and girls, particularly Article 8 privacy rights and Article 10 rights to freedom of expression, it does so predominantly in the context of impacts on platforms and perpetrators' rights to freedom of expression. It does acknowledge that online abuse can impact on women's freedom, but it doesn't do so in specific terms as breaching women's human rights, and I think that it would be good to strengthen the fact that some of these forms of abuse breach women's human rights.

In addition, online abuse can actually breach women's rights under Articles 2 and 3. I think it would be really important to strengthen this guidance to emphasise those human rights of women and girls that need to be respected and protected.

Maeve Walsh, OSA Network:

Great. Thank you, Clare. I wonder if we can bring in Professor Lorna Woods now to elaborate a little bit on the analysis you did, and indeed we could provide a link to thatin the transcription as well. (Link to Prof Woods' analysis is here.)

Professor Lorna Woods, University of Essex:

Thank you and thank you for raising the issue.

Ofcom quite rightly notes that it has to take freedom of expression into account, and it also rightly summarises or restates the baseline test the European Court of Human Rights takes as a starting point in those cases. But I think the point to note is that that baseline phrase is a starting point. The court's case law is much more extensive and nuanced about how you balance conflicting rights. So the baseline is one thing where you have got general public interests in issue when the right of expression is prioritised, but you have to take a slightly different

approach when you have got multiple rights and issues. You can't automatically prioritise one person's right to freedom of expression over another person's right - say the right to life or the right to freedom from torture. So I think it would have been helpful had Ofcom elaborated a bit more on how it proposes or how it went about engaging in that balancing exercise.

There are two other points to note. The first one is that not all speech is equal, even within expression falling within Article 10. There is a priority given to freedom of expression where political speech is an issue, but lower protections or lower oversight for artistic speech, and then commercial speech. Ofcom's guidance doesn't recognise these different types of speech and nor does it engage with the fact that some speech falls outside protection entirely when it is aimed at undermining the objectives of the Convention or the rights of others. I think some of the activities that can be characterised as speech because they are just online would be undermining the rights of others. If we look at a rape and coercive control, and similar sorts of things, it is hard to see that they're not undermining the rights of others. The other thing is that the guidance, and Ofcom's analysis in general across the board, is silent on, is the extent to which there are positive rights to protect people's human rights in their relationships with others. In some circumstances, the courts have said the public bodies are obliged to intervene. Admittedly, the case law here is less clear on how a body like Ofcom might be subject to positive obligations, but it is striking that there's no consideration of the issue. So I think a more detailed, nuanced review of how Ofcom was planning on thinking about balancing would have been helpful.

Maeve Walsh, OSA Network:

Thank you, Lorna, for that really clear explanation of an excellent piece of analysis which is very detailed and does need to be considered in its totality by Ofcom.

We'll move on from gaps in the guidance now to look at some of the suggestions around future proofing that I think people on the call wanted us to discuss. We'll go first to [redacted] from Institute for Strategic Dialogue, if that's possible, to talk about algorithm design.

[redacted], Institute for Strategic Dialogue:

Thank you may for the introduction, and also for coordinating this opportunity to provide Ofcom with further feedback on the guidance. When we talk about violence against women and girls, we need to move beyond individual bad actors and also recognise that there's a systemic role of platforms and their design. Social media platforms aren't just hosting harmful content, they're also recommending it. While the guidance does acknowledge that algorithmic systems can contribute to the harm, and this is a crucial step, it doesn't yet go far enough in addressing how these systems can actually drive users, especially young men and boys, down pathways that normalise and amplify misogyny, further normalising this. Research by ISD and others, such as across TikTok, YouTube and Instagram, show that algorithms actively guide users towards such misogynistic and abusive content, not by accident, but by design.

I wanted to mention a couple of examples from our research on this just to illustrate the issue. First of all, ISD found that TikTok search engines reinforce misogyny through auto complete in

Germany when typing in German ‘are women’, Tiktok automatically brought up suggestions like a ‘plague’, ‘stupid’ and ‘expensive’. This bias isn't user driven, it's algorithmic surfacing how harmful stereotypes are being pushed even before our user has finished typing.

In Australia, ISD created new YouTube accounts to pose as just typical teenage boys, and within 5 clicks these YouTube accounts were being recommended manosphere influencers, which themselves were promoting male supremacy, anti-feminist conspiracy theories and sexual entitlement. While this content is considered fringe and part of the manosphere, these pathways weren't fringe, they were mainstream by the recommender systems themselves.

Finally, ahead of the 2022 US midterm elections, ISD searched for prominent women politicians on Tiktok and Instagram. Both platforms pushed abusive hashtags in the top ten suggestions for search terms. So when users were starting to type into the search, common hashtags were “#KamalaHarrissucks”, “#RachelLevinisaman”, or “#GretchenWhitmerisabitch”, excuse my language. In some cases such hashtags with just a few dozen posts below them were boosted above neutral ones with more traffic, a sign they were actually being artificially prioritised compared. While the guidance rightly acknowledges the risk of algorithmic recommender systems, it's still under plays the broader systemic role that these platforms play in shaping user pathways into misogyny. Research shows that platforms don't just host harmful content, their design actively promotes and entrenches it. These aren't isolated incidents, but algorithmically reinforced trajectories that normalise abuse and escalate these over time.

While the guidance touches on algorithmic systems as a risk factor, it does not yet go far enough in recognising that algorithmic amplification itself is a harmful activity, one that actively contributes to the normalisation and the spread of VAWG related harms at scale. Also, risk assessments must cover, not just content moderation systems, but also how design choices shape user journeys, especially for users such as boys and young men being radicalised into misogyny.
Thank you.

Maeve Walsh, OSA Network:

Thank you, [redacted]

A really powerful contribution, and it all links back to safety by design, but also certainly forward as well to some of the discussions that we need to have around enforcement. We have seen elsewhere in Ofcom's work that there is quite a big gap between identifying the risks quite comprehensively, but not actually then going so far as to identify what the respective response should be. Whether that's a compulsory measure, like in the code, or indeed something that's in guidance, that should be - as we've been speaking about - a more ambitious set of interventions. (Link to relevant OSA Network analysis on gap between risks and measures to mitigate them here.)

I'll bring in [redacted] now from UCL on the future-proofing, points.

[redacted] **Gender and Tech Research Lab, University College London (UCL):**

Thank you so much.

Our main future proofing point is related to the role of emerging technology. When referring to emerging technology, we include connected technology such as Internet of Things (IoT) devices. Our research indicates that this type of tech, which includes devices in the home, plays a really significant role on how perpetrators of domestic abuse conduct their crimes.. The current language in the guidance is around ‘online domestic abuse’ which we feel creates or indicates a more narrow focus around what's important or what should be considered by companies or platforms, compared to more traditional terminology such as ‘technology-facilitated abuse.’ The language is important because it will infer different things to different people - we have just concluded a study on the definition of technology-facilitated abuse which demonstrates that the language which is used in this context means different things to different people - and that could distort what people then feed in or report to platforms.

Companies who are conducting user surveys or engaging directly with perpetrators or victim survivors may therefore get a distorted view of how harms are actually being conducted on their platforms or using their devices or services. The phrase online domestic abuse may give connotations that connected tech and many emerging technologies should not be reported.

Our recent study used Refuge’s data to understand help seeking behaviours and support needs for victim-survivors of technology-faciliated abuse., This showed that technology-facilitated abuse is not always immediately recognised by victims-survivors, and we know from our work with perpetrators, that they don't recognise their behaviours as abusive (particularly in the early stages) either. Therefore the language around ‘online domestic abuse’ could reduce how people feed in or what people report, where it is not fully recognised as domestic abuse by the individuals involved (at that stage.)

The term 'technology-facilitated abuse’ is also used in key policy documents, and in the STRA, so it would be more consistent for the Guidance to use the same terminology - which may support understanding and adoption more broadly and not create confusion.

More broadly, we'd fully agree with [redacted] point about securing evidence and how important that is, and we'd really like to make sure that also includes survivors having a mechanism to access logs of deleted or altered content also - and much of that will be held on connected devices or emerging technology platforms.

Maeve Walsh, OSA Network:

Great. Thank you very much [redacted]
Clare, if I can bring you back in now on some of your concerns.

Professor Clare McGlynn, University of Durham:

Yes. So regarding future proofing, there are 3 main examples I’d like to give, but the overarching point being consistent with what many have said already. This guidance provides an opportunity to go beyond some of the existing requirements where specific activities which are already illegal, and to try and frame and think about some of the ways in which these forms of abuse are going to develop in the future.

The second kind of overarching point is that obviously this guidance does need to relate to the activities which are in scope, and some of the developing technology might not fall within the Online Safety Act. But some of it will.

So first of all, I'd like to talk about when we refer to intimate image abuse or image based sexual abuse. Mostly existing laws and existing regulations tend to refer to that in terms of representing photorealistic images and videos. But we are beginning to see avatars being used in non-consensual sexual ways. So these are forms of image based sexual abuse that are avatars that are representing individuals, but they're not photorealistic. Now this is a new way in which forms of abuse are going to be perpetrated, and particularly the legality around them is not clear. So it would be good to see some sort of recognition of these new ways in which some of these forms of image based sexual abuse are already being perpetrated and are likely to increase.

Another example is the abuse in Metaverse, or immersive worlds and virtual reality contexts. Again, many of these are in a user-to-user context, though not all of them are. We know that violence and abuse against women and girls is already being perpetrated in the Metaverse. We know that safety by design is not embedded yet because many of the protections have only been introduced after women and girls have raised the alarm about experiencing abuse. That's evidence that even in this new and emerging world, safety by design is not being considered, so that's absolutely vital. But also that the mechanisms for reporting and mitigating the harms in these metaverse immersive contexts need to be better developed and better made aware to everyone.

The third context is in relation to chat bots, and again some of these might not fall within the Online Safety Act, but many of them will do, and these can be used in many different ways, including in relation to some of the other harms we've already been talking about such as stalking. But there's also the recent evidence of where some of the Meta AI chat bot options were “submissive schoolgirl”, and so these are chat bots that are able to be accessed by adults as well as teenagers that are reproducing harmful and abusive experiences and narratives against women and girls. It doesn't look like some of that material is to be included in this guidance. So those are my 3 examples of emerging areas of tech and abuse that I think could be helpful addressed in the guidance.
Thank you.

Maeve Walsh, OSA Network:

Thanks, Clare. That's helpful.
And again it's back to that point too, isn't it, about the status of guidance in relation codes; and the evidence thresholds that Ofcom has imposed on itself, if you like, in relation to codes being different. There doesn't seem to be a huge amount of argument as to why you shouldn’t include those emerging areas, even if the robustness of the evidence one often ideally wants to draw from isn't quite there. Wee know that there are risks and threats and it’s the thinking ahead required by companies that is really important.

We will be including in the transcript, some contributions from the Revenge Porn helpline on deepfake abuse. Unfortunately, they're unable to attend the call today but have a huge amount

of expertise there.
Rebecca, would you like to come in on this section?

Rebecca Hitchen, EVAW:

Yes, just briefly. I want to recognise the fact that the Revenge Porn Helpline expertise isn't here in the room, but they are members of online VAWG network and I know will be making a separate submission. Just to tag on to what Clare was saying around that understanding, it's also the fact that take up and the scale of it is huge as well, and we've seen that with deepfakes. We've seen the number of generated imagery used to abuse women and girls rise exponentially, I've got the Revenge Porn Helpline stats from 2023, but just the number of reports from 20/23 to 20/22 was 106 percent increase, and then within the last couple of weeks the Internet Watch Foundation have published some of their data and of their reports that relate to AI generated material, 98% of those were girls, and there has been a 380% increase in the number of URLs containing AI imagery of child sexual abuse over the last year.

Apart from AI imagery, overall, the increase of reports is an increase of 6% just in the last year, and of those more general images, 97% of those are girls, so I think that helps illustrate just the scale of it and also the significantly gendered nature of these issues.

Maeve Walsh, OSA Network:

Thanks, Rebecca. Really important contribution there.

So the next part of the discussion was going to focus on the remit of the guidance, and there's a few things that I might just say upfront about small but risky platforms, which is more in the context of the wider application of the Act and how this affects some of the issues that organisations on the call care about. Throughout Ofcom's approach to the work on the codes of practice, across illegal harms and the children's protections, their interpretation and their standard for proportionality has been something of a problem: the requirements on bigger platforms are determined based on resources and on economic costs rather than looking at the potential severity of harm to users of the service.

So even within the Illegal Harms Code and the Children's Code, there are different levels of requirements according to size on the platforms that are regulated, for example a difference between “core” and “enhanced” duties, or variations in e applications of the measures based on the size of the platform or the level of risk that Ofcom ascertain. That's one part of the broader foundation that the VAWG guidance is sitting on in terms of the application of the illegal duties and the children's duties. It's been somewhat exacerbated then by Ofcom's decision on the categorisation of services within the Act. This is to determine which services go into category one or category two or two A, and there are a few additional duties then that flow from that categorisation.

The advice that Ofcom gave to the department and the regulations that the Department of Science, Innovation and Technology subsequently laid in in Parliament - which are now in force - determined that the categorisation would only be based on the size of platforms, despite the fact that there was a late but important amendment to the Act to ensure that Ofcom could make a judgement on those categorisation thresholds based on size **or** risk. This would have

potentially caught a number of the small but risky platforms that often are the source of some of the most egregious and impactful abuse of women and girls. Often these are platforms that are facilitating and hosting content that is harmful and abusive across a wide range of issues, but particularly in that manosphere world where we are increasingly seeing the combination of far right or extremist views, with incel or misogynistic ideologies; these communities are often very much encouraged and facilitated within these small platforms. So there is an issue here really: obviously the guidance does apply to part three services, but within the enforcement of the duties, a different decision on categorisation would also potentially get at some of the platforms.

So in relation to the Illegal Harms or the Children's duties that would possibly sort of address some of that type of specific and targeted content or activity that represents a risk to women and girls Ofcom has unfortunately left a number of them out of scope: the additional duties including things like transparency reporting and the user empowerment tools and the enforcement of minimum terms of service as well. I think in the context of where the guidance is looking at that issue, those platforms I think have already got something of a free pass in terms of the way that Ofcom has determined their responsibility across their other duties too.

We will then move on to [redacted], who I think is going to come in from and violence against women on issues around supply chains.

[redacted] **EVAW:**

Yes, thanks Maeve. I think that feeds into this point really nicely about which services and platforms won't fall into the remit of this guidance or the codes of practice.

As Maeve mentioned, the guidance will only be applicable to those large category 1 services. In the VAWG Code of Practice that organisations on the call developed, we highlighted the importance that regulated services must not avoid responsibility for VAWG through outsourcing or ignoring the human rights and harms risks arising from it. We know that it's increasingly common for services to contract out parts of their business function, including contracting out their safety measures, and the impact of that could be felt by both platform users as well as those working for a service. It means that the VAWG guidance won't be applicable to areas of work that have been contracted by other organisations, meaning there is a significant regulatory gap. Risk assessments need to include an assessment arising from business relationships. It is not enough for service providers to just draw supplier's attention to the Terms of Service and Community Standards, but should also include provision in any contractual documents, and ensure that those provisions are enforced where necessary.

Regulated services which outsource any part of their business and that includes the moderation of content, their applications, GIFs, images, or any other content or tools, as well as safety tech, need to ensure that the vendor adheres to the social media provider's Terms of Service and Community Standards, and take action to enforce those standards where necessary, and that they have employee and mental health protection policies in place that adhere to the same standard at least. Those outsourced user safety tools need to be fully compliant with the platforms' duties through the Codes, which is important to ensure that regulated services don't

seek to avoid responsibility for VAWG through outsourcing or ignoring the human rights and harms risks arising from it.

Maeve Walsh, OSA Network:

Thanks [redacted] and I think [redacted] wanted to come in here too.

[redacted], 5 Rights Foundation:

Yeah, I just had something quite small to add. I think [redacted] has just framed the importance of supply chains incredibly well, and I think with regards to safety by design that there is a really important element for supply chain team with regards to some emerging technologies, for example like AI, where a lot of AI systems are some of these, in many of these systems, an aspect of them will be outsourced from third parties, whether it's the data or it's the model itself.

Being able to map and evaluate that supply chain very early on is particularly relevant and any intention to implement these sort of systems on a service should form a quite key very early consideration as part of the risk assessment. I think, as [redacted] says, this is something that we've discussed as part of our Children and AI Design Code, which we published relatively recently, that we've designed in consultation with experts including computer scientists in this area, and addresses the need for them to make that assessment early on and then be able to map upstream and downstream users of things like the data in the system so that there can be prevention strategies in place for any harms that come from that or any emergency incidents that may form. So I think I just wanted to add on that, particularly for AI, the supply chain point is incredibly relevant and incredibly important that services adopt and undertake.

Maeve Walsh, OSA Network:

Thanks very much, [redacted]
If we can go back to [redacted] from UCL now on some other concerns about the remit.

[redacted], University College London:

Thank you.
I'm going to keep this short and sweet because I think we touched on some of this in the previous section, particularly Clare's points around in scope and out of scope services, so I fully endorse everything that was said there. This is more about making the point that again, if this is guidance and people should be going further, why allow companies to just cherry pick the things that are in scope and not adopt or be encouraged to adopt a holistic, company wide approach, which prioritises safety by design, usability testing and all these other things, as a companywide default process. I would add that there is a risk of an unintended consequence in that if we do stick to just in scope services that the focus of certain companies or platforms could shift away and just focus on the things they ‘have’ to do, and actually the overall approach worsens for ‘out of scope’ products or services - such as IoT devices.

There's nothing at the moment that we've seen in terms of a baseline survey of how widely these kind of processes are already undertaken by services to give us an indication that we could assess against in future..

So I think it leads to a secondary point around the clarity really needed on how services are actually going to be assessed as to how well they're doing, and assessed against what baseline? Is it going to include things like survivor feedback or self-reporting, or an independent audit, or a combination of many of these things? Looking at companies on what they're doing more broadly in their approaches would be a key part of that, depending on what regime is taken forward.

Thank you.

Maeve Walsh, OSA Network:

Thanks [redacted]
And we'll move on now to the final substantive part of our discussion on enforcement. But we will then have time just to do a little bit of a wrap up at the end for any further points that have occurred to people during the call or anything that people feel has been missed.
But first of all, on the enforcement topic, can I go to Rebecca from EVAW?

Rebecca Hitchen, EVAW:

Thanks Maeve.

As has been mentioned already by others, the current landscape is one where protections for users are being eroded, and the general trend of tech providers delivering just the bare minimum when it comes to safety. We're seeing a rollback of user rights on major platforms, such as Meta getting rid of fact checkers and other user safety measures, so that context is really key. Looking at this guidance and the fact that it is guidance only – and I really do hope that we have made the point throughout this discussion that Ofcom does seem to understand the harms and they've laid them out well in the guidance - but as we've named with the Illegal Harms Consultation, the issue is the measures to mitigate, reduce and prevent those harms.

The Revenge Porn Helpline, I'm sure, will be able to add in some colour into the experiences that they've had and the time and effort needed to create and maintain relationships to support the takedown of images and to get platforms to partner with NCII tools, but 5 Rights mentioned earlier some of the whistleblowers and what we know happens internally when people are trying to improve and reduce the harm created by tech companies. So basically without the guidance being enforceable, the good measures that are in it are very much undermined, and Ofcom is hamstrung by the fact that the proposals are voluntary only and there is no actual requirement on tech companies to put in place the recommended good practice.

What we really need to understand, and it feels important to include in the guidance, is the routes by which the regulator are going to incentivise and are going to track take up of the guidance and how and what its impact is. As [redacted] just mentioned, what are they going to be using? The transparency reporting, survivor feedback, independent audit, self-assessment, etc. It's really important to understand how the guidance will be monitored over time, and I know we know that they've indicated that they will utilise their transparency reporting powers to track and monitor, but it really requires a formal statement on how this will work in practice and exactly what information they will be requesting from platforms in that first iteration of transparency

reporting on the basis that we hope that would be strengthened and expanded over time as transparency reporting becomes more embedded. That's the key issue underpinning all of this and goes back to the fact that it needs to have that code of practice power and strength, so that's absolutely our key recommendation. That this is used as a very first iteration and then the next steps taken by government are to require this to be made into a code of practice so that Ofcom does have the power to ensure that measures are introduced and that there is that ability to enforce against bad actor tech companies who continue to prioritise profits over women and girls.

I know that we've heard from the Secretary of State that he's aware that there are some gaps that exist on the Online Safety Act and there is potential that there might be new legislation introduced. We feel that that is absolutely crucial, but that given that the passage of the Online Safety Act took five years, as we'll all be aware on this call, I think as well as entering into the new legislative process there needs to be urgent and immediate steps taken to close the gaps in in the current legislation, and part of that would be making this into a code.

Maeve Walsh, OSA Network:

Thank you, Rebecca. If I can come to Lorna now as well for some other views on enforcement and how this might be embedded.

Professor Lorna Woods, University of Exeter:

I think I'd like to talk about the status of guidance as a legal document, and I have two points to make. The first is the implication that because the guidance is not a code it is not binding, and I think the word voluntary has been used. There's an implication that companies can just ignore it, and I don't think that matches public law doctrine at all. I think guidance has been put in the Statute for a reason. Parliament had an intent, and while it is not binding, I think there should be an expectation that companies engage with it, that if they choose not to follow what we might call good practice, if not best practice, then they should have a reason for doing so, but they should have thought about it and maybe done something different that they think is better, or there's a good reason not to. I think this is backed up in case law, which says you've got to engage, so perhaps Ofcom, rather than emphasising the voluntary nature of the guidance, should stick in the preface to the guidance some reflection of the legal position on statutory guidance. Obviously there's no set threshold for that, but it might be a useful reminder to regulated entities.

The second point is whether it is entirely unenforceable through the provisions in the Act at all, and I would suggest that as regards to risk assessment that actually Ofcom could use the suggestions relevant to risk assessment to understand the meaning of suitable and sufficient risk assessment in the Act, and it can enforce against suitable and sufficient, and so this guidance, which has the same status as the guidance on how to do a risk assessment, should be something Ofcom takes into account when looking at suitable and sufficient. This ties back to the first point that a company is more likely to show it suitable and sufficient if they've actually engaged in thinking about what's here rather than just ignoring it.

Maeve Walsh, OSA Network:

Thank you for thatvery practical but important suggestion for Ofcom. I think that that's really valuable. [redacted] do you want to come in now on the wider points about framing and to add in any of the safety by design points as well that you wanted to make earlier on?

[redacted] **Glitch:**

Yep. So just to lead on from Lorna's very good points, there's also a question there in terms of how Ofcom's VAWG team are working with their colleagues who are working on the enforcement of the illegal codes. So the guidance mentioned an 18 months window for a kind of assessment of how companies are doing and the uptake of the guidance. What we'd really like to see is the VAWG team actually working alongside the team working on the illegal code of conduct. So speaking to Lorna's points about the relationship between the risk assessments being suitable and sufficient, and the response to the guidance being a practical engagement linked to that, we feel it would be far more effective therefore if Ofcom aligns this guidance with other its mandatory assessments, particularly given the crossover of illegal harms mentioned in both the guidance and the Codes. This could also forge positive ways of working internally, preventing the VAWG team from becoming siloed from other relevant teams. Also, Ofcom needs to ensure that by including measures in the guidance, rather the Illegal Content Codes and Children's Codes, that they've not weakened the overall regulatory approach. We believe for example that a gendered lens to risk assessments should be part of the Codes, as we originally called for.

Ofcom has talked about its guidance aiming to summarise the different types of content and activity affect women and girls online, and to demonstrate to industry the 'pressing need to take action'. To do that, they've provided practical and achievable recommendations for providers.

We strongly believe that the industry has all the evidence needed to take action on violence against women and girls, and have done so for years, and that companies are well aware of the pressing issues, and actually it's there inaction that has led to the UK Government to mandate the sector guidance in the first place. Understandably, Ofcom's case studies in the guidance are illustrative because there are lots of different ways that these issues could be addressed, however, in a number of points in the guidance, Ofcom mentions that these are good practice steps that providers ***could*** take to further improve the experiences of women and girls. Whilst the case studies are one thing, the guidance in general should not be taken as a stretch target that *could* be achieved by these companies, but rather framed as current industry standards - given that all of the examples are from existing standards that are happening across industry.

Linked to that, under each action we have 'foundational steps' and 'good practice steps', but the foundational steps should actually be framed as *minimum steps or minimum standards* because of their connection to the illegal codes, and the good practice steps are *existing industry standards*.

A point around Ofcom's broader language. We understand Ofcom themselves want to be 'holistic', want to be 'ambitious', but actually in practical terms, the guidance is a base of existing good practice, or existing practice even, and so if Ofcom use the language of calling it ambitious and holistic, actually providing examples of existing practice that maybe don't always go as far

as we'd like them to go, then there's a bit of a clash there. By using more grounded language and positioning,Ofcom would be clearer about where the guidance actually sits i.e. a very clear framework of existing practice/existing industry standards, which allows an analysis of where companies are in terms of protecting women and girls.

Also, Ofcom's language around 'encouraging' service providers to take action to achieve a safer life online for women and girls should instead be framed as getting companies to 'catch up with' or 'raise the bar' of current industry standards and I think Ofcom should be really clear about that. It's not really encouraging them to care enough to take steps on this - it's what should be done, what can be done, what is currently being done and where companies are not doing that.

Maeve Walsh, OSA Network:

Thank you, [redacted]
Those are all really strong points and coupled with Rebecca and Lorna's suggestions as well, I think there is much that Ofcom can be doing, both in terms of better framing of the guidance, but also how that internal wiring works as well as where it sits internally with the teams, how they're joining up, and how it is embedded effectively in all of the regulatory interventions and conversations that they have within the organisation and with companies too.

OK, just in terms of any final points, I know that [redacted] from Zero Tolerance wanted to come back in. If there's anything else that anybody else wants to raise at this point, please do.

[redacted] **Zero Tolerance:**

Thanks. Just as we move to mop up, one overarching comment that Zero Tolerance wanted to make was that whilst there's a really strong gendered analysis throughout the document, with Ofcom recognising that all of these harms are disproportionately perpetrated against women and girls and experienced by women and girls, the fact that men disproportionately perpetrate online violence against women and girls is never mentioned, which renders the perpetrator invisible and stops tech companies from being able to address the root cause of the problem, which is gender inequality and harmful masculinity.

There's a lot of passive language used throughout the document, so, for example, and I quote, it says things like "women can be coerced and exploited through the creation and circulation of intimate or sexual content, including through livestreams", rather than using more active language which positions the perpetrator - like "men use the creation of and circulation of intimate or sexual content, including livestreams, to coerce and exploit women". Language which identifies the perpetrator will help tech companies to understand that technology is misused and abused by men to perpetrate violence in a way which reflects broader social power structures.

Zero Tolerance would recommend a full check of the guidance with specific scrutiny of this language and rewriting the sentences that are written in the passive voice to frame the perpetrator and the way that technology is misused and abused.

Maeve Walsh, OSA Network:

Thank you, [redacted]
If there are no further contributions, if people want to get on record now, I might just say a few things in conclusion.

The first is obviously a huge thank you to everybody who's been on the call today and who's contributed the expertise and insight and commitment across the organisations represented here today. It is hugely important and should be a massively important resource for Ofcom in ensuring that their guidance is as strong as possible, and indeed to have the impact that we all want it to have too.

So I'm hugely grateful to everybody for giving up their time today and for the preparation that's gone into to this as well, and for EVAW for coordinating this too. I suppose in conclusion, I know I started with a bit of reflection on how we got to this point and the fact that the guidance exists is important and something to be noted. Indeed, we started with Rebecca's initial observations that there's a lot in it that is to be welcomed, and there's a lot in there also that has been included as a result of representations from organisations on this call and elsewhere.

So the commitment of the Ofcom team to responding to that feedback and to trying to get the guidance into a good place is to be commended. But I think the overall sense from people's contributions today is that it could go so much further, and I think there is an opportunity through the contributions and the submission of this evidence, and through further conversations with Ofcom before they publish the final guidance to really ensure that it is as ambitious and as impactful as it can and should be. That's not just in terms of what might be missing, whether it's specific gaps or specific links back to what's in the codes; there was a lot of powerful evidence on the call about the priority offences and whether those really have the importance that they deserve within the guidance, and how the guidance on how to deal with that content related to those priority offences needs to be framed. But it's also about gaps in terms of emerging technology, and the emerging risks that we now know are there too.

As we know from engaging with Ofcom, it obviously takes quite a long time for consultations like this to happen; from the initial proposals to be worked up, to being consulted upon, for them to then be reissued in their their final form. So this really will be a missed opportunity, I think, if some of these additional points, that very much fit within the approach that Ofcom is taking and are very much going with the grain of the Act and the grain of the intention of the Act and the intention of Parliament when it passed, aren't really included.

So I think while there will always be more iterations, and this is the start of a longer conversation, I think there is still an opportunity in the next few months, off the back of this consultation period, for Ofcom to really make what is a good start even better, and to really deliver the improvements that we all want to see online for women and girls.

So I'll close there in terms of the official bit of this discussion and just say thank you again to everybody for coming and look forward to speaking to you again soon.
Thank you all very much.