Ofcom Illegal Harms Consultation VAWG Sector Roundtable Transcript

The below transcript has been approved by all named individuals, on behalf of their organisations. This transcript is to be submitted and considered as evidence to Ofcom's Illegal Harms Consultation. For any questions or queries please contact rebecca.hitchen@evaw.org.uk

This roundtable took place online on the 6th February 2024.

Attendees:
Maeve Walsh, **The OSA Network (Chair)**
Lorna Woods, **University of Essex and The OSA Network**
Clare McGlynn, **Durham University**
Rebecca Hitchen, **The End Violence Against Women Coalition, EVAW**
Janaya Walker, **The End Violence Against Women Coalition, EVAW**
Sophie Compton, **My Image My Choice**
Seyi Akiwowo, **Glitch**
Eva Blum-Dumontet, **Chayn**
Colette Collins-Walsh, **5Rights**
Saskia Garner, **Suzy Lamplugh Trust**
Sheila Amedodah, **Imkaan**
Rani Govender, **NSPCC**
Stephanie Grimshaw, **Welsh Women's Aid**
Liz Speight, **Centenary Action Group**
Sophie Mortimer, **Revenge Porn Helpline** - Not present at roundtable but evidence presented to the group in advance and transcript is endorsed and supported

Maeve, Chair: Thank you all for joining. As you're aware, this is a contribution to the Ofcom illegal harms consultation, which closes on the 23rd of February. We've brought together this group of people because you've all got very significant expertise and specialisms and interests in the issue of violence against women and girls. And while we're aware obviously that Ofcom will be producing guidance on that topic in due course, that's probably not going to arrive until early next year. Ofcom will be consulting quite widely on that but there are a lot of issues within the illegal harms consultation that directly affect the things that we all care about. And indeed a number of criminal offences that, again, are primarily those that are experienced by women and girls. So we felt collectively it was really important that we pull together the evidence and the insight from these groups present today to feed into that consultation and that by having a facilitated discussion today, we would be able to most efficiently bring all that insight together.

So thanks to Rebecca we've pulled together a structured agenda. We've got a number of organisations that have already identified that they want to speak about particular issues on that agenda. So we'll ask those to lead off on each of those topics. But then the floor is open to everybody else to contribute. I'll try and keep us on time because

we've got a lot to get through but obviously if we don't cover any of those specific topics, or we don't get to the contribution that you want to make, then those can be submitted afterwards when we pull this together into one formal consultation submission.

So without further ado, we were going to kick off with discussing the issue around the business-centric focus in the Ofcom consultation, particularly the primacy that's given to issues around costs, presumptions that firms are going to comply with the duties as set out and then a separate point at the end about the way that the consultation process has been framed. So I wonder if EVAW would like to kick off on that now.

Rebecca, EVAW:
Yes, absolutely. I can begin and just to say a big thank you to you, Maeve and to the Online Safety Network in general, who've just been such a helpful point of contact for information and holding the thread around the Ofcom regulation and the Online Safety Act in general. I'm very grateful to you. So one of the first points I wanted to make was around this disproportionate focus on the cost and resources to tech companies without any parallel consideration given to the cost and resources associated with the harms to women and girls and wider society. In Volume Two when it talks about the risks of harm, it has a real focus on the impacts of harm to individuals, but it doesn't then translate that into consideration of the financial cost that harm then entails.
Obviously that's not a lens that the VAWG sector will normally take when we're looking at the harms enacted to women and girls but given that Ofcom is doing that, and has chosen this line of approach we feel necessary to provide evidence to that. Quantifying cost of VAWG is inherently slightly problematic as it is so difficult to measure as it falls across a wide gamut of areas. But there are ways in which to sort of attempt to quantify costs when it comes to violence against women and girls and harms, This has been done in a number of resources.[1] But to give examples of how significant the cost is, but also how hard to measure which I know Sophie from My Image My Choice will be able to draw out in greater detail in case studies - a very non exhaustive list would include the loss of employment for women, women who have had to relocate or move due to stalking or the impacts of deepfakes. There's the moving house, there's the loss of

[1] https://eige.europa.eu/newsroom/news/gender-based-violence-costs-eu-eu366-billion-year?language_content_entity=en.
https://eige.europa.eu/sites/default/files/documents/20213229_mh0921238enn_pdf.pdf
Cost of DA calculated at £66 billion
https://assets.publishing.service.gov.uk/media/5f637b8f8fa8f5106d15642a/horr107.pdf
Award of £97,000 awarded to victim of IBSA in civil case: https://inforrm.org/2023/03/24/case-law-fgx-v-gaunt-damages-for-image-based-abuse-andrew-willan-and-nataly-tedone/#:~:text=On%2027%20February%202023%20judgment,publication%20on%20a%20pornographic%20website

community, loss of peer support. There's the loss of sexual relationships that she may not feel able to participate in due to fear of unwanted additional sexual violence, because of the sexual script created from mass viewing of porn that encourages acts such as spitting, choking and slapping. And there's, and this point I know will be made later on, but there's those wider costs of women feeling more inhibited in online spaces and less able to participate in society, including in political life, and which is so significant and obviously very, very difficult to quantify, but does have a cost attached to it that I think Ofcom need to recognize as part of this work.[2] Recognising this costs stresses the importance of a proactive regulation approach rather than the approach they seem to be currently taking which solely considers the potential business costs involved.

Maeve, Chair:
Thank you, Rebecca. That's really helpful. A really useful framing. Would anybody else like to come in on this specific point about the focus on costs? Sophie?

Sophie, My Image, My Choice:
Yes, I can add some colour to that really helpful framing Rebecca based on the survivor stories that we've worked with, and like Rebecca, the framing of this in terms of financial cost does sit quite uneasily with me. However, I do think that it is helpful to build that other case, because one thing that we've seen is that with victims and survivors of image based sexual violence, including deep fakes, that it has a very direct impact on their careers. For example, one student that we've worked with Julia wanted to become a Twitch streamer, but after being deep fake decided that that was too dangerous. And this is symptomatic of people not pursuing their dreams, people looking at the career of being a politician, of being a journalist of being an activist or being outspoken in their work and deciding not to do that job. I mean, the cost to society is absolutely vast if you think about that on a broad scale. Lauren said, you know, if I ever became anything, it felt like the image was ammunition that could be used against me for the rest of my life.

We have women who work in online professions or high profile professions who are in the spotlight, such as YouTubers, such as Gibi one of the women that we work with, she's an ASMR artist with a big following. And she says, I operate under the sick reality that women creators have to accept that you will be abused. I know I personally am a lost cause. I will always have digitally created porn of me online, for my future children to see and that will survive long after I'm dead. So she's decided against all the odds that she wants to continue in that profession, but she has countless people contacting her daily saying ‘I want to be a streamer but I don't know if I can hack it” and she has to be transparent with them that it will that will be part of what they have to experience.

[2] https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-5-5/

That is not going to encourage more people to enter that career and that goes for many other different instances.

But also again, framing this in terms of cost feels slightly uncomfortable, but we have seen with so many of the women that we've experienced the level of PTSD, the depth of the mental health Impact is so severe. One woman Chrissy told us having severe PTSD after her case of image based sexual violence ravages every aspect of your life and your ability to hold on a job, maintain relationships, maintain mental health. Lauren told us 'it's like my body would show up but my brain was off somewhere else, 100 times a day thinking about this experience'. Lauren said' it was an entire year of my life. I almost feel like I don't remember that year. I was going through the motions of trying to stay alive.' And we have seen people take their life as a response to this. There was a 17 year old who, who did so and Lauren and Chrissy and many other women I've spoken to have talked about suicide ideation. So the cost to these women's participation in society, the cost of business is vast. And finally out of all of the survivors I've spoken to every single one of them has changed their relationship with social media, and has either decided to participate less or decided to come off entirely or decided to come off these platforms. So if we're thinking about online safety and online participation, that mass scale silencing of people, not just survivors, but their peers, their friends, the girls in their group at school or college. We don't have a quantitative study, to lay out the scope of that. But I know from personal experience that it is consistent with every single survivor that we've worked with.

Chair Maeve:
Thank you for that Sophie.

Lorna Woods: Excluding women has real profitability consequences - see what World Economic Forum says, summarising reports from elsewhere:
https://www.weforum.org/agenda/2023/05/women-board-directors-dei-profitability/
See also: https://onlinelibrary.wiley.com/doi/full/10.1002/ijfe.2089

Sophie, My Image My Choice: Also Amnesty International's The Silencing Effect - https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-5-5/#:~:text=The%20silencing%20and%20censoring%20impact,and%20freely%20express%20themselves%20online.

Jess, Refuge: Our research with domestic abuse survivors also echoes Sophie's point on silencing - 38% said they felt unsafe or less confident online as a result of tech-facilitated domestic abuse - https://refuge.org.uk/wp-content/uploads/2021/10/Unsocial-Spaces-for-web.pdf

Liz, Centenary Action Group: The Jo Cox Civility Commission report might also be helpful on online abuse as a threat to democracy https://www.jocoxfoundation.org/our-work/respectful-politics/commission/

Chair Maeve:
Elena if you'd like to come in now as well, that would be great.

Elena, #NotYourPorn:
Survivors end up having to take on additional jobs being investigators, advocates and play so many other roles and they end up having to do this all around their day jobs and managing their trauma. Just picking up on that point about profitability, I think we really need to emphasise this idea that safety is profitable more and more, as much as that is an uncomfortable term.
I think businesses/companies and Ofcom need to understand that investing in these measures to take a lot of the burden off survivors is crucial for their profits, because unfortunately that's what a lot of them care about - profitability.
And just going back to talk more about evidence to do with survivors over the last five years of campaigning, I've seen the burden on survivors who are not only trying to manage the mental and physical toll that this takes on them. There's not been enough research done at the moment about the physical effects of undergoing trauma from online violence. But there are plenty of studies that show being subjected to domestic abuse has also a physical impact. Autoimmune diseases are the illnesses that people then have to manage within a healthcare system that systematically ignores women and girls and their pain. But also thinking about the fact that they have to take on this unpaid job where there are no safeguards, to the extent that they have to chase companies to take them seriously, monitor where this content goes and have it taken down. So really it's a huge imbalance of power. A company that has a budget should be doing this and has a much stronger intervention point to deal with this kind of harm. Yet it is being treated as if “Oh, it's too onerous for you”. Well, what about the survivors that have to do it day in and day out as if it's a second, third, fourth job, and every single survivor that's come to us has played that role? And that’s because of the deficiencies in the system that is supposed to be there to support them. So I think it's really important to emphasise that by backtracking on responsibilities of companies, regardless of their size, because this should be in place across the board, what you're actually doing is perpetuating/facilitating the harm and contributing to mental and physical harm on those individuals.

Chair Maeve
Thank you so much Elena. Seyi would you like to come in and then we'll move on to the compliance and the consultation points as well?

Seyi, Glitch
Unfortunately I think we have to reconcile the fact that we have to make a financial case around this. This is regulation. This is not human rights legislation. So I think we need to grieve that. We're not going to win that argument because Ofcom need to be able to make the business decisions to the tech companies.
I have a question about children, when we're talking about children's harm when we're talking about sexual violence against children, do we have to make a business case there or have children already won the moral argument? That's just a question I have.
Two going back to the finance and working on their terms. This is why we campaigned for there to be a tech tax. So there was a proportion of profit that was generated, that goes back to ending violence against women and girls online. And that would look like mental health support, that would look like documentation that would also look like data on the cost of this all. That is my suggestion, that we have a consensus in the wording around how they are going to track the financial costs of violence against women and girls, and how they going to make that intersectional because all of the conversations about survivors having to do two, three jobs. Black Twitter has been doing that since 2007. So it's been there. People have been doing this. So there's a lot of evidence that we can be drawing upon, and making sure that when we're asking for the evidence that we're making sure it's intersectional.
My final point here is I think we can also talk about this being the public interest. If we look at other forms of regulation, ie Ofcom for the media ITV. I'm thinking of Nella Rose, I'm thinking of love island. I'm thinking of those incidents in certain instances, there has to be a threshold of them taking cases because it needs to be in the public interest. I wonder if we want to still bring in the Human Rights element that we can can put in an argument that says that says that Ofcom have to put in mitigations when they reach a threshold of this being a public health issue or a public interest issue.

Maeve, Chair:
Thank you Seyi. Thank you for that. I'll try to brigade specific suggestions like that as they come in and then we might circle back at the end to talk specifically about what we might ask for. I think there's the importance of evidence - obviously, every time we speak to Ofcom obviously they're asking for evidence - but I think all of these points about what we then suggest they might do in response are really important too. So as they come up, I'll brigade them all and we'll come back to them at the end. Can we now move on to the cost of compliance? EVAW, I think you are going to kick off with this and I know Refuge had some points to make as well. So Janaya over to you.

Janaya, EVAW
Thank you Yes, and supporting all of the points that have been made. So far. I think connected to the criticism about the way in which the documents are framed I think there's a complementary point about the fact that it feels as though there is a good faith

assumption towards tech companies in terms of the expectation that they will comply and that they will adopt a kind of best practice approach. On this point, I think it's worth reiterating that as we all know, a key part of the thinking behind introducing this legislation in the first instance, was consensus among parliamentarians, and wider society and civil society, that self regulation and relying on the voluntary initiative of tech companies themselves to make the internet a safer place and to reduce harms was not working, hadn't worked and was not going to work. We can go back to Hansard - there are various quotes within parliamentary debates which speak to this. We've got the online harms White Paper back in 2019, which says that the patchwork of regulation and voluntary initiatives have not gone far or fast enough. And we had Nadine Dorries, during the second reading of the bill, saying that without the right incentives, tech companies will not do what is needed to protect their users, and too often their claims about taking steps to fix things are not backed up by genuine actions. But EVAW's perspective is that in direct contrast to this, what we see in volume five, and throughout the documents is there's a default position that the companies will be compliant, and that they will have processes for assessing illegal content that are of a higher benchmark than what Ofcom has set out in volume 5. And that sort of best or good practices are enough as a starting point. So for example, there's a quote that says "many services will already have Terms of Service or their equivalent in place that are more expensive that are more expansive than that in defining what content may be deemed violative and will already be taking down content above and beyond what the law requires in terms of preventing users from encountering legal content". Just to restate the point that this feels quite counterintuitive and against the evidence that we know we know that systems that have been created for profit in particular, they have a bottom line and they don't generally like to go the extra mile as unless it's part of their USP and a profit driver. There has to be an incentive to. We've seen this in other sectors too in terms of think about consumer rights, environmental rights, the financial sector. And specifically when thinking about the Online Safety Act, there's considerable evidence that platforms don't adhere to their own terms and conditions. So thinking about the research that Professor Claire McGlynn has done. Fiona Vera Gray as well. We can quote Glitch and EVAW's Ripple effect report. It's very easy for the policy teams to state what should happen and furnish these documents on request, but its how it's actually implemented. The reality on the ground is another matter. So I think there's a huge question mark for VAWG organisations about how compliance will be addressed by outcome but also how they perceive the current compliance. Thank you.

Elena, #NotYourPorn Happy to provide case studies of when accounts haven't been removed despite breaching the community standards across a number of years

Maeve, Chair

Thank you. Jess from Refuge did you want to just come in on that point?

Jess, Refuge
Yes, just to echo Janaya's points really and as we will all of know, from our experience, for example, as Refuge as a frontline service provider, we have a tech facilitated domestic abuse team, with considerable experience and expertise, and experience of platforms not adhering to their terms and conditions at the moment. I think that's something that - you'll see lots of nods - everyone will have examples of that kind at the tip of their fingers. And I think I'd echo that point from Janaya as well that we sometimes see good effort from policy teams, heads of Trust and Safety teams, etc. in showing commitment. But then saying the right things externally but that's not translating into practice for the survivors that we support. So some research that Refuge did last year - we interviewed some survivors and over half of them 53% said they didn't receive a response from a social media platform when they reported domestic abuse related content. So just at the forefront they're not even receiving a response to content that does breach terms and conditions. And we have other instances as well of social media companies saying content flagged doesn't breach the community standard, even when content is clearly abusive or harassing or intimidating. And we've also had some instances as well of survivors that we've supported being informed that the content that they've reported to the platform has been 'lost'. So no further action can be taken. And almost all of the survivors that we spoke to for our research (called 'marked as unsafe') - 95% - said that they weren't satisfied with the support that they received from social media companies. So there's lots and lots of case studies and evidence in this space of just showing that platforms are not adhering to their terms and conditions currently. So we really need to see that sea change. And I think a kind of different approach from Ofcom in approaching this assumption of compliance.

Maeve, Chair:
Thank you, Jess. Seyi, I'll bring you in and then Jess we will be coming back to you again, on the points about consultation because I'm conscious I'm already running over my agenda time here. So, Seyi come in now and then Jess,

Seyi, Glitch
I'll be super quick. This is just intel from sitting on trust and safety councils for a while, the new way in which they're getting around compliance is just to deamplify so when we took when we went to all the platforms with our digital Misogynoir report in the summer, we gave them cases of horrific misogynoir and misogynistic content on their platforms. And they said, "Oh, don't worry, we de-amplified it". We said 'What does that mean?' They said "Oh, it means that we have basically changed the - if it Tiktok it's the 'For

You' page, if it's meta, it's that timeline so that it doesn't appear in people's feeds, but the content will still stay.
So I think there is a need for us to think about tighter compliance language as well so that they don't do things like de-amplification or give more warnings. I think what we want is an opportunity for learning and opportunities to call people, an opportunity for people to say okay maybe I didn't mean to repost that x, y z, and then actually platforms making it very difficult for accounts to come back. Yeah, so I think that there's a way in which they're getting around compliance already, and I'll be worried that they'll just find another way to to do ring around on Ofcom.

Maeve, Chair
Thanks Seyi, that's really useful insight. And Stephanie, and then Jess. Thank you.

Stephanie, Welsh Women's Aid
Yeah, around that and around flagging images and things like that. We're really concerned that there's no obligation on the smaller tech companies to have to even signposts or, or even put up a warning. We think that it should be for all organisations at a bare minimum and base level. I was quite shocked to read in the process that it it that didn't apply to all companies.

Maeve, Chair
Thanks Stephanie. Yeah, that's a that's a broader issue that - certainly from the Network perspective - we're going to be picking up in our submission too. But I think it's really important to make the point, particularly the evidence, as to how that's going to play out for some of the sites that are deliberately set up to harm women and girls.
Jess, Okay, last bit of this first topic, Jess, back to you on the approach, which I know is something that we've all got gripes about to say the least.

Jess, Refuge
Thanks Maeve. I think this point around the the format of the consultation and how tricky that has made things for civil society organisations to engage with this. So I definitely recognise that Ofcom have been responsive, they've engaged with meetings and highlighted certain areas for focus to some organisations, which has been helpful but I think the reality is that the whole consultation, the length, the complexity, has made it extremely difficult for lots of VAWG sector or wider third sector organisations to engage. Part of the issue as well is that because so much of the consultation is interlinked. So having to understand how the risk assessments proposals, to understand volume 2 to see how that feeds into the codes means that it is quite hard to also just cherry pick certain bits to get involved in. Having to read 2000 pages for organisations that are very, very busy. Many of us are frontline service providers as well. And we are all really keen to engage and we know that this is important work. But just to point out that we would

encourage Ofcom in future to see if there are alternate ways to run these consultations and to engage the sector. There is also a point around engaging survivors and victims with lived experience as well and making sure that meaningful engagement with those people, in a safe way as well, can be achieved in future.

Maeve, Chair:
Thanks, Jess. And I think the point about victims and survivors and those with lived experience not having a mechanism to feed into this as well in a safe way, and I think Ofcom not really having considered that, is an important point. It's one we'll pick up in our Network response too .I know from the perspective of some people who are survivors of grooming, they've been approaching Ofcom themselves to try and do this and really that's not a scenario that should be happening. There should definitely be some kind of safeguarded way for those insights to be brought in. And I think this is a practical issue that hopefully Ofcom can consider for the next consultation. They've got time to obviously think about how they want to run the children's one in that context.

Okay, thank you all for that: really, really important and really helpful contributions there. So I'll move on now to our second topic: “in harm's way”, we've called it on the agenda. Kicking off with a look at the wide societal harm. And I know Professor Clare McGlynn was about to lead off on that.

Professor Clare McGlynn:
Yes, thank you. A few things, I think we're all concerned about the lack of recognition of the wider societal harms of online abuse of women and girls. And I think this manifests itself very briefly in a couple of main ways. First of all, in relation to human rights, there are human rights obligations within the Act, but as Lorna Woods has detailed in a very helpful comment, the focus in most of the Ofcom consultation is on the human rights of users/ abusers and of companies. There is an insufficient focus on the impacts on women's human rights, of the silencing effects and other impacts that have already been discussed today. So that needs to be in the balance. Secondly, many people have already talked about how online violence against women has a wider impact in shaping women and girls behaviours, particularly changing how they interact with online apps and online messaging and I think that needs to be recognised more widely in relation to the harms.
I want to give a particular example about the lack of focus on the wider harms in relation to pornography. The discussion about harms takes a relatively individualistic focus; in other words, can viewing a particular piece of pornography lead to that user carrying out particular acts, particularly violent acts? This neglects the wider impacts of much extreme pornography, including the government's own commissioned research, which talks about: ‘there's a substantial evidence of an association between the use of pornography and harmful sexual attitudes and behaviours towards women’.

Now, that piece of research isn't about extreme pornography specifically, but it does provide the overarching framework within which the harms of extreme pornography is a priority offence must be considered. And particularly when you compare this with the way other offences are taken into account in the consultation.
For example, in relation to firearms, the consultation talks about the glamorization of firearms and weapons by young people is of particular concern and is a particular manifestation of harm.
What I think many of us would say, is that the glamorization of rape through extreme pornography is a particular harm. That was why this legislation was introduced by David Cameron in announcing this legislation said rape pornography 'normalises sexual violence against women and girls'. That's why it was introduced. And that's why we should recognise the wider societal harms of that form of priority offence.
I'd also give you another example of foreign interference. The Ofcom consultation about illegal harms talks about how there is not enough available evidence to draw robust conclusions about the impact and harm of foreign influence operations. But despite that lack of 'direct insight', there's clear potential of risk of harm to individuals, hence why action must be taken. And that's what I think we'd like to see about the wider societal impacts of online abuse, even if there might not be some direct causal links. You can never have that study in the first place. But even if there isn't, there is clearly potential or risk to harm to individuals and that needs to be taken into consideration.
Lorna Woods's comment re human rights here:
https://www.onlinesafetyact.net/analysis/ofcom-s-approach-to-human-rights-in-the-illegal-harms-consultation/

Maeve, Chair
Thank you very much, Clare. That's really helpful. And really powerful too. Thank you. So if anybody wants to come in on that particular point on societal harm, although we've touched on some of this. The point about the onus on platforms to provide the evidence of safety is relevant here. So if there's anybody else who wants to pick up on those aspects there, please do put your hands up.

Seyi, Glitch
Again, just to bring in some insights that the trends that companies are on, at the moment even able to keep on top of and we want this to be a future proof legislation and I don't know about you, I'm not gonna have eight years in me to do this again. One thing is the trend of clipping themes from Game of Thrones from EastEnders where a woman is just about to be hit, just about to be raped. So it's not quite graphic. But we all can read the lines and that's the level at which we are seeing bad actors organise. And that's the level on which we need to be specific so that it is broad and future proofed but it means that there is no wiggle room.

I don't have the answers just now. I don't have the answers just yet. But I think there is a naivety around people doing this by accident and that's why I am sometimes in favour of there being a focus on perpetrators. I am in favour of there being a focus on the grooming that we've seen happen significantly since Andrew Tate has become mainstream. That causes societal harm and therefore then women are on the receiving end of that. And it is these trends where they will get around a stated measure or a stated illegal harm that users shouldn't be engaging with. They'll get around it. And so how do we use a framework? I think, Lorna, you talked about this in our council meeting a couple of weeks ago about proportionality that gets us from having to chase the next trend, the next vile trend, towards women and girls. Because I don't think we're going to see people naively now uploading original content, as we saw with deep fakes. I think you're going to see people being more and more creative. How do we define behaviours when we can't get evidence of intent?

Maeve, Chair:
Thanks, Seyi. That's really important. And I think something that, as you say, Lorna has been particularly grappling with recently. Lots of hands up which is great. So Sophie from my image, my choice next and then Janaya and Rebecca.

Sophie, My Image, My Choice
I just wanted to completely second that, but also add that we're talking about societal harms, and in our experience, we have been framing looking through sites and the growth of sites around deep fake and image based sexual violence, we've been viewing this as a form of radicalization. Because we've seen individuals who have started to take participate in these cultures and have them become extremely enmeshed in these cultures, which are very anti social, which valorize misogyny, and build bonds and identity based on the violation of women and the violation of consent.

And that is correlated with the recent finding in The Guardian, that Gen Z boys and men are more likely than Baby Boomers to believe that feminism is harmful. And I think that we actually cannot downplay the potential risk to society and the kind of frontier of feminism that we're on when we're allowing these cultures to spring up and to take root. And I think the other thing that we have to think about is the normalisation of these practices. You know, in the case of deep fakes, given the lack of regulation, I think we're going to talk later about Google and I will bring that up later on. But given the lack of regulation, given the fact that these sites have been allowed to become not just communities that are perpetrating this abuse, but thriving businesses. I've seen deep fakers hiring other people to be their assistants. They are clearly making money off of this, and the message that that sends to the young boys at school who might be sharing that content, believing it's another genre of porn without the cultural framing that this is

abuse material. Of course we're seeing results like this recent study about Gen Z boys and men. So I just don't know how much more quantified impact of societal harm is needed. You know, this question of there isn't enough evidence. Like I believe all of the things that have been said today is very clear evidence of societal harm, and it should belong to such.
https://www.theguardian.com/news/2024/feb/01/gen-z-boys-and-men-more-likely-than-baby-boomers-to-believe-feminism-harmful-says-poll

National Crime Agency evidence on the “radicalising” effect of in this case viewing ai-generated child sexual abuse imagery and joining online communities where these are shared - ““We assess that the viewing of these images – whether real or AI-generated – materially increases the risk of offenders moving on to sexually abusing children themselves.” https://www.theguardian.com/society/2023/jul/18/ai-could-worsen-epidemic-of-child-sexual-abuse-warns-uk-agency

Chair, Maeve
Thank you, Sophie. And I think this discussion today will be a strong contributor to that. But certainly when we've been talking to Ofcom, this has been the response to some of those concerns. It's “show us the evidence” so you know, there is that cyclical thing where the burdens are on civil society to demonstrate the harm. I think also demonstrating what those solutions might be will be really important as well. So Janaya and then Rebecca.

Janaya, EVAW
It's a connected point to whatever I was just said, what we want to convey really is that the approach taken by Ofcom is saying show us the evidence of the harm and evidence the risks so the onus is on us to demonstrate that these things are harmful or how they impact women and girls, as if the online world is inherently neutral or safe. But given the conversations we've been having about the cultural wallpaper, the cultural fabric of violence against women and girls, and how it sort of permeates every part of life, that starting point and that perspective is wrong. We've suggested that onus should be on the platforms themselves to provide the evidence that their business models are safe, that they have inclusive policies that they don't facilitate illegal content, for example, rather than the other way round, to work on the assumption that the companies are good faith actors and platforms are neutral, they should be demonstrating that, particularly because of all of the evidence that the business model itself can run counter to the aims of the Online Safety Act itself and also the regulator's aims.

Chair, Maeve:
Thank you. Rebecca.

Rebecca, EVAW:
I wonder if Mr. Deepfake hiring employees would count as a SME according to Ofcom, in terms of them having particular consideration to costs and proportionality and without a requirement of governance. And I think that this a really good example from Sophie about those small sites single risk that are causing significant harm and I was actually just going to bring in the same point as Janaya. Around that lack of neutrality and what seems a willful naivety of Ofcom's approach to the evidencing of harm.
And when we talk about 'the internet' it's all of the different components that contribute, the AI, the algorithms, the search engines. None of those separate elements are neutral either. So it's just sort of like a continued torrent of bias, which normally includes a lot of misogynistic tendencies and racist tendencies as well. And I also just wanted to add to the point that Sophie raised about the misogynistic influences and how popular they are and the impacts that that they're having on young men and young women's understanding of rape myths and of harm. So, Sophie mentioned the Ipsos Mori poll, but there's also the CPS have done their own evidence, which shows that particularly younger people hold these dominant wrong narratives about rape and what constitutes rape. And when we think about what they are in terms of future generations, it's seriously worrying and, and feeds into that point around wider societal harm.

Maeve, Chair:
Thank you, and Lorna would you like to come in before we move on to the next topic?

Lorna Woods:
It's a question. From memory, Volume Two said there was no evidence that the business model contributed to harms in this space. What I'm hearing from people around this table is that there are examples where the business model is providing an incentive for the creation of this sort of content. So if anyone has examples of that or evidence, then perhaps it would be good to add in to make the case that the business model is part of the problem as well.

Maeve, Chair:
Yeah, a really good point, I think so we can hopefully capture that. Okay, so we'll move on to the next part of the agenda. This is about whether the approach set out by Ofcom in its illegal harms consultation is setting the bar too low. There's quite a minimalist approach to the measures that are suggested in the codes of practice. And very much kind of coming from a non-interventionist perspective as well. And this brings us on obviously to the issue about small sites and high harm as well. So Rani, from NSPCC, I think you were going to kick off on this particular minimalist approach aspect, and then we'll move on to other contributors.

Rani, NSPCC:
Thanks Maeve. Something that I think struck a lot of us from different conversations and meetings we've been in is the gap between Volume 2, the analysis of the scale and impact of harms that women and girls face online, and then the lack of ambition in the codes of practice and what is actually being proposed in terms of tackling these harms. A lot of the measures are focused on what users can do to protect themselves - which is not in line with the government's own principles for what safety by design looks like - measures like reporting, blocking, muting, default settings on children's accounts. They have an important place, but they certainly can't be seen as the whole solution.
There is a real gap in terms of what proactive steps platforms are going to be taking to prevent this harm, to detect and disrupt it.
I also think there are two key concerns we particularly have for the precedent this is potentially setting for Ofcom's approach to codes. So the first, something that Lorna and Maeve have worked on a lot, is the incredibly high evidential bar for proving the efficacy of measures. It's not always clear where that's being set. But it's particularly worrying that there seems to be a dependency on recommending measures which are already widely adopted within industry. The reason why the Act is so important is because measures that industry are using at the minute have not sufficiently protected users. They've led to this huge scale of harm. And so this bias towards measures used by industry is not going to bring systemic change. It's a problem in this code, and it'll be a problem with the regulation as a whole if it continues to be implemented that way.
The other concern is what does this mean in terms of incentives for innovation. This comes back to the point that the codes are safe harbours - if you are complying with the codes, you're seen as compliant overall. It's tricky to see how trust and safety teams, and people and organisations, that are trying to push to do more, for more innovative proactive solutions, are going to be able to justify the investment when not only do they not need to do that, but actually, they might be just creating more work for themselves. Because if they prove the efficacy of a new tool, that might be added to a code. Whereas if they actually say no, that's too difficult to tackle, then there's less evidence and less likelihood of them being made to implement something new.
We want to see greater ambition in these codes of practice and for a focus on proactive efforts by tech companies to be much more at the forefront of future codes.

Maeve, Chair:
Thank you, Rani. That was really helpful. I just want to acknowledge as well that Elena I know you've put a lot of really good stuff in the chat on risk assessments. I see you had your hand up there. So if you want to come in on that specifically, otherwise we'll pop it into the document with the recommendations. Lorna, do come in now.

Lorna Woods:
A couple of points about I suppose solutions and what's not being suggested which is possibly stretching it a bit to fit in this bucket, but it is linked. The point is that when Ofcom is looking at this, they focus very much on ex post measures. They've not really looked at the design, and they've not considered the possibility that if there is something that is demonstrably harmful, e.g linked to a feature or functionality, and nobody knows how to fix it, then why is it still there? And I know for some of them, this is going to be fundamental to the service, and that there may be lots of benign uses for the particular functionality, but Ofcom doesn't actually go through the process of analysing whether a removal of a feature would be appropriate and proportionate. That is a big gap in the analysis.

I'd also like to pick up a point that Clare made earlier about whether you have to prove that x feature taken in isolation has a particular effect when in real life it operates in conjunction with lots of other stuff to have, in particular cases, a particular result. That's the way academic research sets about things really trying to isolate and prove causality very, very closely, but that is an impossible bar. You're never going to prove that, so this question about what is the standard that Ofcom is using is really, really important because if they are looking for the impossible, then where do we go from there? So I think something that is much more related to civil burdens of proof and what may be lawyers do which is on the balance of probabilities, then that would be a more helpful place to stick the evidential threshold.

Chair, Maeve
Thank you, Lorna. And again, that's something that obviously runs through all of the areas of harm that are covered by the consultation too. So that is something that we'll be picking up in our overarching submission as well. Sheila from Imkaan would like to come in.

Sheila, Imkaan
I don't think that Ofcom goes far enough to ensure that the intersectionality of violence against black women and girls is recognised when considering safety online. There should be mandatory training for moderators and content moderators to recognise that intersectionality, especially when black and minoritised women girls are thrust into the limelight. The examples given previously of Nella Rose. She previously had a predominantly black audience, which was safe for her but when she went on “I’m A Celebrity, Get Me Out of Here!” that was then pushed further. She's now open to an endless barrage of racial abuse. There also needs to be recognition of a lot of dog whistle racism. So things which if you're not present in a certain online space, you might not recognise that for example, some people just comment 13%, which to anyone else might seem a bit innocuous, but to people who have experience in those realms, it's

clearly oh black people make up certain percentage of American population but a certain amount of crime wherever it was. Dog whistle racism is very prevalent for a lot of black women and girls online and it makes space especially uninhabitable for public figures who are black and minoritsed women, for example Diane Abbott, Dawn Butler, so much so that they've had to close their public surgerie. That also goes back to the real life impact, as they now they can't do their jobs as MPs as they're open to threats of physical harm, which stem from racialised misogynistic abuse online.

Maeve, Chair
Thank you and the point about training, I know you want to pick up on this as well. But also that's an aspect in the distinction between small and large services in concentration as well where even the straightforward training is only expected in its entirety of the larger platforms. And it lets a lot of the other small platforms off the hook.

Jess, Refuge
And following on from Maeve's point - even the recommendation on training for moderators is quite vague, it doesn't specify if it should be delivered internally or externally by experts, or what training should be in, frequency etc

Elena, #NotYourPorn
So I'm going to try and keep it brief to the three areas I want to talk about are: business case, training and then looking at this risk assessment. So first, going on in terms of starting with a business case, I think we actually have ample evidence to show why safety by design is really important from the outset. If you look at what's happened to Pornhub and MindGeek, you look at what's happened to Only Fans with their decision to remove adult content after Rihanna Croxford's 'under the skin of OnlyFans' investigative report, if you look at what's happened to Facebook and Meta, because of essentially dealing with things after the fact they had to then put in place measures which cost them - I don't know the exact statistics but I think I read a report where it was double or triple what it would have been if they had just been monitoring it in the first place.
So I'm sure I know that we've got a tight sort of deadline, but I'm sure that there is evidence out there for us to say why you need to listen to us. And maybe that is something we need to talk about. I know that there are several journalists we've worked with in the past and I believe EVAW has as well, that we can contact that have written about this and have written about the impacts and maybe that's a potential hook to say if you just get this right from now and you start putting things in place safety is profitable and won't harm your profits.

Moving on to risk assessment. One of the things I find really infuriating about this whole consultation is the approach to risk assessments, there's no defined structure for it. If

we're going to really start curbing behaviour, we need to have smaller, more impact risk assessments that are going to take a month as opposed to an extended period of time, you know, and some kind of checklist. I know that may be arbitrary, but something to be able to assess what's happening immediately. This also needs to interact with different measures across the sector, it needs to be integrated into other systems. So if there's a reporting function, for example, on Ofcom's website, there's a distinction between the public and say, civil society, where civil society can say we've seen this number of cases on this specific site, can you send an alert that they need to do a risk assessment, if we can't have direct contact with them for example. Then Ofcom, perhaps, I don't know how the communication works, but send an alert as well to maybe other companies to say you need to conduct a risk assessment on this as we've seen a trend, if they're playing the central function, and then using risk assessments in this way from the very beginning. That's just kind of to explain my core points, but there are more in depth points about this in the comment that I've written.
In terms of training there are two things: the smaller sites are one of the biggest issues we have with what I call the filter through problem. I'm not talking about the smaller companies which are trying to be compliant but are being unfairly penalised because they are engaging. I'm talking about the smaller companies which thrive on exploitative practices. Also, it's all very well someone at the top putting the measure in case but if it doesn't filter through to all the employees who may potentially interact with sais survivor, or dealing with non-consensual content, then that content, regardless of what the level risk associated with it, will not be dealt with appropriately. So with training, I would argue it's even more important that smaller sites, their employees have appropriate training, because I can give you ample examples. I mean, last year, I spent six months arguing with a much smaller social media site about a form of content where the moderator hadn't even looked at this content that I said was IBSA and it took essentially threatening them to get them to take it down. And in those six months or however many months where's that content gone?

So as much as I am concerned about bigger sites in many ways I'm more concerned about smaller sites, which are slipping through the net, and I can provide ample case studies. So just let me know what's needed.

And the other thing that really irritates me too, about training is that, you know, as a part of my day job, I work with vulnerable children and it is mandatory now. Every single year I must do PREVENT training and every single year I must do safeguarding training, regardless of how many years I've done it. And I think it should be mandatory that there is some kind of online safeguarding training not specifically on safeguarding children but also for adults as well. If a demand is created for this kind of training, it is reasonable to believe training companies will move into this market. We can say to Ofcom, you know,

you can say that companies need to implement this training within 18 months or something to have their first initial training. We can say part of the PREVENT training comes from the government so you can just do the training online, maybe something similar is needed for safeguarding children, adults and particularly minority groups online. I don't know how many people have done this before. And there are loads of companies which have online e-courses for safeguarding. You know, I don't think it's really given all the money that companies/key institutions have to put into learning and development anyway, I don't think a small (just to begin with) online safety training that's mandatory every year regardless of the workforce size and a training that is tailored to specific roles is actually that much of an ask.
And we could probably even work out how much it would cost to roll out a training like this. From what I do in my day job, safeguarding training, the companies that contract me pay for an inexpensive subscription. Also, I think that if we're going to think about money, I think we can work out the costs (especially in comparison to the financial cost on survivors), and actually show why this is relevant and really in comparison to what they're spending on whatever else this is actually a very small ask, relatively.

Maeve, Chair:
Thank you. Thank you for the very practical recommendations there as well. That's really, really helpful and Seyi just to come in. And I think also we've touched on it a number of times, but it might be worth just having a dedicated section on the small platform point as well just to mop up any of the other specific recommendations after this. Seyi, over to you.

Seyi, Glitch:
Thank you just to backup the points around the the annoying smaller sites. Glitch's Digital Misogynoir Report found that men and women were practising their misogynistic content and their racist content on the smaller platforms where they can get away with it. And then having more of a sophisticated approach on the larger platforms. So they are ping ponging between the two so we need to see them as small and large but then also as an ecosystem because that's how they are organising. On the code of practice, 100% back the training, and I find it exhausting to see amount of people called the gender team or the sexual abuse team who will have to answer and be the consultants internally for the entire organisation. You're lucky if it's two people, you're lucky if it's four. So there is a capacity issue. There is a competency issue. There is a resourcing issue on expertise internally, and then of that, how many of them are understanding intersectionality? So just to backup Sheila's point there around training needs for moderators.

I had the pleasure of being in Mexico, the unpleasure, if that's a word, of watching content moderators at Tik Tok. And there was a woman who had her cleavage showing

and that was marked and flagged as sexual content. They were able to then flag which geographies would be able to see that content and knew that in certain countries and conservative countries it would not be appropriate. So they are able to filter out the algorithms they are able to review and assess. And obviously there was a whole conversation about a woman's cleavage not being sexual content anyway. But it's at that level. I think the reason why it comes across so minimal is because that is where they are at. Like the questions that are being asked in consultations in the conversation being had, with TikTok and X and Meta are these basic things. So we need to make sure they're Ofcom are resourcing themselves, so the training that Sheila suggested needs to be for Ofcom also. I think they have to be accountable to us and saying that they are going to be able to pick up misogynistic and misogynoir content online. Including in the Code of Practice. So already a lot of tech companies in the lead up to the rumoured Online Safety Act began doing annual reports. These reports are very vague, and it's a PR stunt. I think we should be asking for a lot more detail around the monitoring and documentation of certain types of abuse and ensuring that we're seeing improvements year on year. I think we should be using financial terms back at them. I think we should be using capitalist market terms back at them. What are KPIs you want to be seeing? What's the harm reduction we want to be seeing? Let's get them to start benchmarking some things and then Ofcom to be able to assess how it has been able to contain the beast.

And then finally, I would say open audit. Sadly, we have left the EU but one thing that I have loved about the EU was that once a year, they would have all EU institutions open their books, open their buildings physically so that you could come in and understand how the courts work, or the European Council. Something similar happens in the council. So when I was a Labour Counsellor, many years ago, when we had this horrific year of six women dying by domestic violence we had to have an open case review to look at where did we fail? I think there should be that level of auditing and monitoring and case study review to ensure that there is a continual feedback loop because I've seen their feedback loop for profit. How can we make sure we're having that same feedback loop to safety by design?

Lorna Woods: Just randomly usurping Maeve's seat while she opens the door. First Janaya then Sophie.

Janaya, EVAW
Thanks for stepping in Lorna. And I think they're two points that have come up in the recent discussion. One was just to reiterate what's been said around smaller sites where the most significant harm is often situated and also the most extreme content. We know that organisations like Revenge Porn Helpline have researched the sites

which produce the highest number of images reported per domain which we can provide. And many of those are not big sites. They can be really small businesses that currently would manage to avoid any substantial regulatory requirements. And also, I think there's a point that although a platform may not be widely used by the general population and so 7 million threshold they're often sites which are highly popular amongst particular groups, women, children, people of particular age groups, for example. And similarly, those platforms avoid significant governance and the Code of Practice requirements despite the risks that they pose to those groups. So I think that's building on what others have said around small sites.

Then to go back a step as well, building on what, Lorna, I think you've said around many of the measures being ex post. I would say from EVAW's perspective, there's sort of a mirroring here in that the document is replicating a wider societal dynamic in which violence against women and girls is primarily addressed through interventions *after* the harm has occurred, which largely rely primarily on the victim themselves in terms of their own motivation and action to bring about resolutions - rather than being preventative or systemic. So it feels like there is a real lacking in terms of a systems based approach, which looks at safety by design, and which is not geared so heavily towards the removal of items content in a singular or isolated way, but looks at how the entire service operates and what sort of behaviours it can incentivize and exacerbate. Not only behaviours, but what sort of harmful social norms as well can proliferate. Going back again to the parliamentary debates and Parliament's expectations of the Bill to do, I think there was a higher expectation looking at sort of product testing or design measures and that kind of language and thinking about how users engage with different services, how content is disseminated and reaches different groups, but it feels like there's a comparative lack of that kind of thinking and volume 4 and in the draft codes.

Maeve, Chair
Sorry for the brief disappearance there. Sophie and Lorna, I think that you've still got your hands up. Sophie?

Sophie, My Image My Choice
Yeah, so to the point about small sites, I think that this really speaks to the need for Ofcom to grapple with the fact that what they're dealing with is the internet. It does not have the kind of solidity of one person in a place. And we have to look at the network and the ecosystem and how things are connected. So in terms of small sites, like let's take Mr. Deep Fakes, the biggest deepfake porn website, probably not even a small site at this point. But sites such as Mr. Deepfakes are dedicated to image based sexual violence, that is the purpose of their existence. They are likely to be hosted overseas.

They are likely to be shady operators, they are not likely to be compliant. So that's going to be a real challenge for Ofcom. And I really don't believe that Ofcom have understood the scale of that challenge. These are savvy internet natives, who know how to use VPNs, who know how to hide away and so you're not going to get them to stop what they're doing. But what you absolutely need to do is stop that site from being accessible. So Google in recent research which can be made to be supplied to Ofcom has found that Google search is responsible for 70% of traffic to sites that are dedicated to image based sexual violence. So it's not just that these sites appear on Google, it's that Google is actively promoting these sites. It is up ranking them. It is delivering these results. For example, if you Google the name of a female politician such as Alexandria Ocasio Cortez, and thoughts on deep fakes, you will pull up image based sexual violence of Alexandria Ocasio Cortez. If you Google the name of a female celebrity and porn, whether there's that person acted in porn or not, you will pull up non consensual image based sexual violence of that person. So there's a whole system of how search, as one case study, is driving traffic to these sites. So yes try and get that site shut down. Yes try and get that site blocked and I completely support that. But in lieu of that we have to look at how the mainstream companies such as Google are enabling the small sites, and if Google's risk assessment does not include its requirement or responsibility to down rank and block sites like Mr. Deepfakes - it's about how you conceive of the relationship between Google and those sites. Like Google is not hosting the deep fake content. It is two steps removed, but Google is driving the traffic to those sites. And if you look at what companies say and what they do, for example, there are some social media sites that say we do not host deep fake non-consensual abuse on our site. However, what they do do is host apps for people to make deepfake porn content. They do host ads for people to go to other sites to start participating in that culture. So really, really thinking about small sites high harm, yes, but also the whole ecosystem and network around that. And just a final point on the broadest scope, I'm really concerned that the approach to these risk assessments is just not going to succeed, because here's a problem - a problem of deepfake abuse as an example, is the risk assessment, is the approach, is the protocol, going to stop that problem? It seems like we're negotiating with Google and they are going to have to improve their safety protocols to a certain extent. We've seen time and time again, how these kinds of violence against women and girls issues are not prioritised not considered to be important, and they fall through the cracks. So we need to be creating a shelf at the bottom of this regulation

and these risk assessments that are actually robust. And I'm concerned about what I'm hearing that that's not going to happen.

Janaya, EVAW
To give an example on that point around lack of interventions to prevent harm - cyber flashing and unwanted sexual images is one example where platforms have the tools to introduce 'nudges' and friction. Platforms will know for eg whether there is any previous interaction between users, will know if they follow one another, and if an image of genitalia for eg is being sent to an unknown user in that context

Maeve, Chair:
Thank you, Sophie, Lorna now and then we will move on from this, Lorna.

Lorna Woods:
I'm asking questions again - for examples and evidence. It is driven in part by what Sheila was talking about the unwanted publicity, but also what Sophie and others have talked about in terms of the business model and the ecosystem. I was made aware, some years ago now, of a case of a feminist writer, who was on Facebook, and the algorithms started promoting her content to people who were not in favour of feminism. So they all piled on and told her completely what they thought about her. She hadn't been asking to be promoted to those people, but what was happening was engagement. Or at least that's my best guess. If we go back to the case of Caroline Criado Perez, who tried to campaign for Jane Austen on the banknotes, she got a lot of abuse that even managed to pass the criminal threshold. And the people who did that were interviewed after they finished their community service, and they said they didn't have a view on Jane Austen. But what they wanted to do was to participate in a discussion that got them lots of likes, and that was piling on a woman. So going back to the fact that Ofcom is missing the point, or only seeing part of the point, with a focus on ex post, take down are there are there other examples of the way the system and the business model actually make things worse. So we can shift attention upstream. So it is not just give a user a safety tool, but actually fundamentally redesign these things.

Maeve, Chair:
Thank you, Lorna. I think that is a hugely important contribution that we all can make in this consultation stage is providing that kind of evidence and examples and so forth, so

that we're not going around the same discussion again when Ofcom reissues these codes.

Elena, #NotYourPorn
I'm just going to quickly respond to that point. Can we submit videos? I know that a lot of us have Googled, for example, have used Google to type in deep fakes and deep fake apps. And then there's loads of lists that have come up. I don't know if we're allowed to submit video or photographic evidence, but it's there. Just last week I opened the app store and just typed nudify, and loads of apps came up, which are overtly showing taking people's clothes off and all of that, like they're clearly very openly advertising. And yet, as part of the app store's guidelines they don't allow sex education charities to have apps there. The disparity and the power imbalance between these kinds of businesses or apps is huge. The point I was going to make is back to this idea of the filter through effect. I can find examples of times I've had conversations with employees of different platforms who have said 'Oh, that doesn't happen on our site'. And then you literally type a word into their site and show them and they're almost in disbelief like that can't happen. So I think that, as much as there is willful ignorance, there is also a drift between the reality and what employees really understand about the harms online. (I think this is also true of key stakeholders like Ofcom.) And I think that this is also what contributes to cultures within companies of not thinking that safety by design is necessary - I just wanted to add those points.

Janaya, EVAW: https://www.thetimes.co.uk/article/social-media-companies-profit-from-misery-spread-by-misogynistic-influencers-6bzbd2g23

Saskia, Suzy Lamplugh Trust:
https://www.theguardian.com/media/2024/feb/06/social-media-algorithms-amplifying-misogynistic-content

Maeve, Chair:
Thank you, and I absolutely think we should be submitting videos and photographs. Everything is evidence and it may be that we kind of find some way of creating a folder for them that we can link to in the written submissions that can be accessed by Ofcom, or by sending them directly. We can talk to them about the practicalities of that. But I think to your point just now as well - it is incredibly important aspect of this, sort of

negligence if you like really, because so much of the way that Ofcom is framing this consultation is around adopting best practice and kind of saying “well lots of sites do this already so therefore that is all that we're asking”. So I think being able to demonstrate that actually, even if they say they're doing something they clearly are not actually seeing it through, is really important too. I'm minded to move on, although I see Claire and Seyi have some brief points.

Seyi, Glitch

I just wanted to offer another insight that I got to speak to one of the creators of the For You Page, and I asked around data sets. We spoke earlier this is not just around moderation, this is not just around risk assessment, but it's about the design and design also starts with the data sets. Platform still don't have a data sets, still don't have a taxonomy, on types of harm related to misogyny, let alone misogynoir. And I think that is one key KPI we can ask them for when it comes to code of practice. That is something that can be open source, that can be something Ofcom creates, whatever it is that it can run through its list of top 10 types of misogynoir or misogynistic content, running it through platforms to check what still gets left. Platforms are creating their own datasets to do this, but we know they do use for copyright issues when it comes to music. I can't post my dancing videos without someone now trying to take it down because Universal Music wants to see me. So how do we create that same data set, that same taxonomy, on our agreed top 10, top 20 and keep adding to the list as we keep hearing new evidence, new forms of organising. How are we making sure that their benchmark is alighted to our benchmark?

Maeve, Chair

Thank you Seyi. And thanks, Claire - we'll come to you now in a moment. Okay, so let's move on. We are now going to come on to the part of the agenda when we're looking at the approach to assessing illegal content, non compliance, risk of reliance reports and the background of the CJS guidance as well. So I think Claire and Lorna, were going to kick us off from a legal perspective and then we're going to come to EVAW, Refuge and NSPCC on the reliance on reports and complaints issue.

Lorna Woods

So this is really about the definition of illegal content, and the reason why illegal content definition is important is because it describes the scope of the entire regime. The duties are linked to illegal content. So if you don't think it's illegal content, then the duties don't apply. So I have some questions here about Ofcom's approach to the definition of illegal content, and in particular, how we see that in the illegal content judgments guidance. Now to be clear, Ofcom has got to work within the scope of the Act and that Act is a little complex, but it is ambiguous. In interpreting the provisions quite narrowly I think Ofcom has overlooked the need to have a definition that works with a systemic approach. So what we have got is this problem that illegal content is using the criminal law to define when a civil regime applies. And the criminal law when you use it to criminalise people is understandably very tightly defined, and has requirements not just about what people are doing, but what they're thinking and whether there are any defences. And this is where the illegal content judgement guidance comes in. When can companies infer that, when is it reasonable? Ofcom has gone for an approach that implies individual items of content. Now, that makes sense if you are thinking just about takedown because takedown can operate on individual items of content. The issue is the regime is not about individual items of content, it's about systems. So if we just take the obligation to operate a system designed to allow content to be taken down fast - that's an operational choice, but it's also a design choice. And you can't do design based on individual questions about can we infer user X has this mental intent or that - or at least not so closely. I think the signals for inference in the system's context have to be broader or weaker than they might be if you're making a decision whether or not to take an individual item of content down. So if you're thinking more broadly, about how you weight your algorithm, for example, whether you have nudges about whether this is nice behaviour or not, or whether you have content revenue sharing system, these don't tie in very well with the idea of understanding 'mens rea' and defences very, very tightly. So I think there's an issue there that in the focus that we see in the consultation on this being more or less about takedown and not about upstream safety by design - this is part of that story. There is an ambiguity, though, in terms of the word content, and in terms of the way the connection between the content and illegal content is defined, and the extent to which it is associated but I think you have to interpret it to make the regime make sense. And at the moment, I think there's a bit missing in the illegal content judgement guidance. There's a sort of question also about whether when we're doing this, we're expecting providers to say, is there an illegal act taking place, or is this

content content that has been connected with an illegal act, and I think the example there is the re-posting of intimate images. My suggestion is the regime is focused on content, and that once you have linked the content to illegality, it remains illegal content. The regime is not about giving an extra penalty to criminal offenders. It's about safety. It's about protecting people. So I would suggest that we have got a slightly narrower focus there that is not helpful and is not required by the terms of section 59 which is where a legal harm is defined. The final point I'll make is about the strength of the signals that we need to make the inference. We're allowing companies to make the inference, it only needs to be reasonable and I think we need to understand that in the light of the fact that this is a civil regime, not a criminal regime. And in a civil regime, if you were in court, we'll be talking about the balance of probabilities rather than beyond a reasonable doubt which I'm sure Clare will correct me if I'm wrong, is the test in a criminal crime trial. So I think that whole judgement piece maybe needs to soften or make clear that we are not looking about the criminal threshold. We can look for broader softer inferences when we are looking at categories of content, and that's what we look at when we are designing systems.

Clare McGlynn:
A couple of brief points. First, to emphasise the significance of what Lorna is saying about the illegal harms element of the consultation and how they interpret the criminal offences, because much of what we've been discussing about the broader impacts and harms will come to nothing if we can't actually get a proper systems approach to the priority offences. And this has a number of ramifications for much of the discussion we've had so far. If we take deepfakes: first of all, in relation to the actual discussion of harms, there is very little on harms of deepfakes in that part of the consultation, partly because the law hadn't yet been changed, but that definitely needs to be strongly put to Ofcom so that they develop that element of the harms. But the second point relates to, whilst it is Google that's facilitating some of the deep fakes etc, the way that priority offence about non-consensual distribution of intimate images, which includes deep fakes, has been very narrowly drawn. So it asks providers to focus on each individual posting of a piece of content, which as Lorna says, means that instead of seeing an image, ie a non consensually shared intimate image, and then removing all of that type of image, there will be no such obligations on providers. The baseline is not removal of those all those images. Ofcom say that best practice would be that they would remove them all, but they won't necessarily and they won't have to.
The second point relates back to our evidence and how we think about the evidence and the approach that Ofcom takes. Many people have already talked about how the

assumption is about neutrality, instead of the whole point of this piece of legislation was that we know that there are harms. So for example, in relation to cyber flashing the whole point about a criminal offence of cyber flashing was we know that it is prevalent and that it's harmful. But instead the approach taken to interpreting that offence - is that there is no harm unless you've proven that there is some additional intent element attaching to a particular image. But, for example, we could take the approach that the victims do not wish to receive unsolicited dick pics, and we know that that's the harm that many women experience of unsolicited dick pics, and we take that as our starting point because there are reasonable grounds to infer that most of the dick pics that are sent to women particularly where they don't know each other on a particular messaging app might be harmful.
Also on cyberflashing - the consultation talks about prevention not being the issue, as the user can just delete. This totally misunderstands the harms.

Lorna Woods
Section 10 of the OSA imposes a range of duties on "user to user" services (social media) in relation to illegal content. This includes at 10(2)(c) the duty "to take or user proportionate measures relating to the design or operation of the service to ...(c) effectively mitigate and manage the risks of harm to individuals, as identified in the most recent iteration.
DCMS came up with principles of safety by design in 2021 - the first such principle was that "Users are not left to manage their own safety"
https://www.gov.uk/guidance/principles-of-safer-online-platform-design

Maeve, Chair
Thank you, both Lorna and Claire. And just in terms of submitting evidence, Lorna has written up a very good analysis of the issues that she's just run through there on the illegal content judgments guidance, which we will be publishing on the website shortly (link here), but we'll also have as a PDF so we can attach that to the submission we put in on this specific topic as well as more generally. And thanks to Clare for those specific relevances as well. Elena's put a comment in the chat, and I wonder, Lorna, if you might be able to respond to that there because I'm keen to move on to the issue of reliance on reports and complaints. Saskia, sorry, I think I've overlooked the fact that you wanted to come in here and then we'll move on to the specifics on reports and complaints.

Saskia, Suzy Lamplugh Trust
We want to echo what has just been said about a need for a systems approach, particularly when we're talking about course of conduct crimes which won't necessarily

have specific, harmful incidents in and of themselves. There is a lot emphasis in the Ofcom identification of the harm section on specific threats and aggressive behaviour and threats to harm and so on - which of course, is a key part of of stalking, but often what we will see is repeated unwanted fixative behaviours that are extremely harmful to the victim but won't in and of themselves in the current way that harms are being outlined here, be identified and picked up. I just wanted to also echo a comment earlier about the availability of technology of this kind of communication. That technology exists, let's not fool ourselves that we couldn't be picking up these repeated perpetrators across multiple platforms, if the intent is there, and I would really advocate that that intent should be there and looked at more closely. We're particularly concerned that in volume two the conclusion is that no specific evidence has been found on how business models may influence risk of harms to individuals for stalking. We find that fairly astounding, really, when it's quite clear that a number of settings across multiple of these platforms will be enabling that for example, automatic settings to public by default, pushing potential contacts and associations through these platforms, people that you might know, do you want to connect with them, that kind of a thing. And just really echoing that this sort of minimalist approach by Ofcom to mitigate these systemic behaviours. Also, finally, just to make the point that we really want to draw the connection between how online behaviours also promote and link to in-person harms. We know that very few stalkers will just stalk online, and that once a threat has been made, 20 to 50% of those perpetrators will act on those threats in a real life in-person harmful way. We cannot just be looking at the online impact which is massive, in and of itself over 95% of stalking victims, 100% of whom have online elements, say they are negatively impacted by the stalking. But we really need to look at and others have mentioned it - the link between online harms and the promotion of in-person violence and that cannot be disputed. A couple of case studies I'll just mentioned one quickly - a stalking perpetrator forming multiple fake Instagram and snapchat accounts, threatening and intimidating a victim continually changing identity and platforms to perpetrate these kinds of behaviours, including threats of sexual violence, kidnapping, and others. Police were struggling to gather evidence that this is coming from a particular individual. But we know it's possible to identify people using multiple platforms and we really would like that to be better looked at in the mitigation of harms.

Maeve, Chair

Thank you so much, Saskia. That's really, really helpful. We'll go onto the reliance on reports. EVAW did you want to kick off and I think we've got 25 minutes left on the call and I'm conscious that we are slightly running over time now, So, if we can have quite specific contributions that we absolutely want to have captured in this transcript as evidence, and we'll hopefully get through all the other topics by the end of the session.

Rebecca, EVAW

In terms of assessing illegal content - it talked about relying on where reports had been made, but also that was caveated which is concerning, but I think there cannot be a reliance on reports and complaints being made as a way to measure a harm that is being enacted on a platform. So it would also not be appropriate to do risk assessments in that vein because of the lack of reporting. There's a lot of research around this where particularly young people and young girls, they don't bother reporting to platforms if they experience online harm, because it's seen as so normalised. It's seen as part of the fabric of being online and being on the internet. And so I just wanted to make the point that there that can't really be a reliance on that because there is a host of reasons why women and girls don't bother reporting, and it's because they don't think anything will be done, that they think that it's normal, and they are concerned that even in reporting that the person who has harassed them or perpetrated the harm will somehow be alerted, and it will escalate the harm that's happening. I think with any reliance on that reporting or complaints, there's a wider point as well around the links with what Seyi was saying earlier about data and how are they measuring their targets and how is it being tracked, how is it being quantified. I will also say that when women and girls do report it, from the Ripple Effect report we did with Glitch, it found that Black and minoritized women and girls had a worse experience of reporting to platforms, and they felt to a greater degree that their complaints weren't properly addressed. So again, speaks to systemic issues with racism within platforms.

Maeve, Chair

Thank you. Rani and then Jess, your perspectives on this please.

Rani, NSPCC

I completely echo Rebecca's points and just to broaden it out a little bit for girls. When we think of child sexual abuse crimes like grooming and CSAM, they disproportionately

impact girls. As Rebecca said, parts of that abuse, like cyberflashing, are so normalised that it's something that girls have to laugh off, and to be honest, to process that abuse and report it every time would be a huge burden on them. If you look at something like grooming though, that's a bit different. Firstly, it can often be that children are unaware of the dynamics of grooming, which stops reporting, but also exploitation, blackmail, coercion are often integral to this form of abuse. So, to assume that a child can just make a report to stop it ignores the layers and complexity of that form of abuse. And it goes without saying, but offender to offender interactions are not being reported. So if offenders are creating Facebook groups to share child sexual abuse material, they are not then reporting - so if Meta aren't proactively identifying and disrupting these forms of abuse, they'll go unnoticed.
And just on using user reports to inform risk assessments, I think it's really important that when we're looking at the core evidence and extra [enhanced] evidence that it going to be used to inform risk assessments, there needs to be more external third party input because otherwise relying on these internal tools to assess harm is going to miss some of the important nuances that I think we've all touched on today.

Maeve, Chair:
Thank you, Jess from Refuge.

Jess, Refuge:
I think it's really important that we do get the reporting and complaint systems right. That's really important. We get lots of survivors facing issues with that, as we've kind of spoken about before, but I agree that we can't have an over-reliance on this. And I think just to bring in some of the evidence and some of the research - 2 in 5 (41%) of survivors that we interviewed, said they were unlikely to report again to a platform after they had experienced reporting domestic abuse related content. So that is for survivors who have received support, quite often from a specialist support organisation as well, who are reporting - then face barriers and are put off doing reporting in future so that becomes this kind of circle. Really. So reports are just being probably the tip of the iceberg and more and more people may be put off in future not reporting future events - that will affect the systems that have been put in place as well.

Maeve, Chair:

Thank you, Jess. We'll move on now to an additional aspect of this Elena from #NotYourPorn, you wanted to make a point about the issue around non compliance with terms of service.

Elena, #NotYourPorn:
In addition to problems with reporting, what also happens from the perpetrator side is that more often than not accounts don't get removed after clearly violating the terms of service and the community guidelines. So from a behavioural perspective, what we've seen is one perpetrator who becomes potentially emboldened by this and continues to perpetrate not just on that particular platform, but across different platforms. And I think a point really needs to be made to Ofcom that this happens across the board on every single platform, no matter what they say about their terms of service and community standards. And it shows a general approach to support the rights of the individual user, despite the fact that they're being abusive, and that those rights are more important than the rights of survivors and victims. I think this power imbalance has been referenced in many different forms in this conversation already, but I think we would need to hammer home - just like if you're suspected of terrorism, you should have your account removed, so should be the case with abusive behaviour - why is it any less significant because the harm is against a woman or a girl, as opposed to the state as a whole, and arguably is also harmful to society as a whole?

Maeve, Chair
Thank you so much for that. Rebecca.

Rebecca, EVAW
I just wanted to come in on the point around Terms of Service and I know it's been made, but just to say about the concerns about how companies will hide behind them and what the next steps are then for Ofcom because we've got serious concerns about the information gathering powers and the extent to which companies will be challenged and the ease with which they will be able to evade those gathering powers and similarly, the business disruption powers. It feels like a requirement of transparency and data sharing is so necessary when thinking about this issue of non-compliance with their own Terms of Service, and it just isn't sort of factored in this consultation at all. If you're going to say that companies need to be setting targets, there needs to be subsequent

processes in place where those targets are reviewed and monitored with that third party consideration that's been mentioned before. And I think particularly, this is where Ofcom are so important and why it's so important that this is got right as soon as possible. I know Ofcom has talked about the fact that these are going to be iterative, but echo Seyi's point earlier about how there isn't the time for that and Ofcom are under time pressures, but they cannot just keep sort of pointing further down into the future as to when things will improve, which I feel that there is danger of them doing at the moment. And I think it links in with the fact that there is a complete absence for individual redress with this regulation regime, and a number of us here have raised concerns around that particularly in relation to super complaints essentially being that that only recourse and the fact that the criteria, as it stands from DSIT, is extremely high.

Claire McGlynn:
This is why the illegal judgments is so important since if the minimalist approach is taken, people will be even less likely to report.

Sophie, My Image My Choice
To echo that point, women who are targeted by deepfakes including higher profile women / YouTubers / people whose career is in the public eye also don't report - there is a feeling of powerlessness and that this will never change, as well as a fear of exacerbating the harm

Clare McGlynn
Need to add in re illegal content - the absence of obscenity and section 127

Lorna Woods
The fact that Ofcom ignores it doesn't take the offence outside the regime but it does send a signal that these offences don't need to be thought about and I think that they are likely to be useful as catching content that falls outside more specific offences for technical reasons.

Maeve, Chair
Thank you, Rebecca, and I think also as well as the iterative nature of the proposals that have been set out here, there is also the problem that this is only a small part of the regime they're consulting on. So for instance, to your point about information gathering powers and so forth, those have only just come in. But also their guidance on transparency reporting is further down the line as well. So there is a tendency by Ofcom

to keep pointing to the other bits that they will show us at a later stage. But without seeing whether those are going to be robust enough, you're being asked to make a judgement then on this part of it without that full picture. I do have sympathy for Ofcom with that because obviously they've got a huge amount to do. But it doesn't help really in terms of reassuring about the specifics that they've consulted on here.

We'll take the last point about the challenges with the CJS system as it is now. I wonder if we could have a contribution that is ideally quite brief but gets to the point about the context in which these codes are being produced. EVAW or Refuge - would you like to pick that up?

Rebecca, EVAW
I can say briefly and then go to Jess on it. We're talking about illegal content and illegal activity but the fact is the criminal justice system, which is geared towards illegality is essentially broken. It's not able and was never particularly designed to tackle violence against women and girls. And as it stands, there are huge, huge delays, and there are completely inadequate resources across police services and CPS services. And it's not just a question of of resource, it's also a question of intention - they aren't bothered to investigate cases like this in the small instances that they are reported to the police - because there is a connection to what we were saying about reporting is that often, issues even of quite extreme harm aren't reported to the police because they feel that they will be dismissed and not be taken seriously - which sadly, is the case in a lot of instances.

Maeve, Chair
Thank you. Jess, did you want to add to that?

Jess, Refuge
I echo what Rebecca said about this crumbling system, which is the backdrop that we need to bear in mind when we're talking about the criminal justice system. Also the survivors that we talk to often say that the immediate priority for them when they have experienced online abuse, online domestic abuse, for example, intimate images have been shared online - the immediate priority for them often is get action on that content, get it taken down, make sure it's not going to go viral, that is often their immediate

priority really, and the criminal justice system is not there to do that. Really, that is a much longer process quite fairly - it should be a longer process to look through that. We've got to the point now where there's so many court delays it's far too long a process, but that is not what the criminal justice system is really there to do. It's what social media platforms and search platforms can be doing and should be doing. In this world that we want to get towards it is a role that they could be playing and playing really effectively, and we're just so far away from that. But it is something that I think we would really like Ofcom to bear in mind as a goal - that they could be playing this really important role in society.

Rebecca, EVAW
We cannot consider criminal law as a realistic vehicle in tackling this issue. It needs to be regulation that does this work, it is the only way to solve the issues we've spoken about today. The law cannot meaningfully do it.

Maeve, Chair
Thank you. I'm afraid due to my shocking chairing we are running out of time now. What I would like to do is still have a discussion, which won't be enough I'm afraid, on image based sexual abuse. I know that Sophie, My Image My Choice, has a number of lived experience examples and I wonder if we can take it that we will add these to the transcript so that they will go in in the form that you want them to go in. *[See Annex A]* I will come to you just to make a few points in a minute. Also Revenge Porn Helpline weren't able to be on the call or stay on the call but they have already provided some evidence that we will put straight into the transcript. [*See Annex B*] Sophie, if we can come to you for a few minutes on cyber flashing, intimate image sexual abuse and that whole area, and then ideally leave about five minutes at the end just to mop up anything else and to agree next steps and again, apologies for now being slightly rushed at the end.

Sophie, My Image My Choice
Well, I think we've actually all covered a lot of topics around image based sexual abuse so I don't feel the need to add a huge amount more and also Claire is more of an expert on cyber flashing than I am. But we can supply further testimony.

Maeve, Chair

Great stuff. Thank you. Clare - is there anything you wanted to add in here that hasn't been said already? No, that's a shake of the head. Okay, good stuff. So there's an opportunity now if there's anybody who hasn't made the points that they wanted to make or hasn't been able to contribute in any part of the agenda so far, do please feel free to put your hands up now. If we can't take the detail, we can at least flag again that this is something that we will add into the submission.

Colette, 5Rights

We've talked a bit about how the various offences and how the business model just isn't identified as a risk for the facilitation of that and I think it's to do with the way that Ofcom is interpreting it. So it's saying that, for example for CSAM its as if you can advertise CSAM on a service and that is a direct risk. But of course for grooming, it recognises that recommender systems are a big risk for connecting vulnerable children with adults or with offenders. But then it says there is no evidence that the business model revenue model is helping to facilitate grooming. But obviously those are all connected. This is how Ofcom is obviously interpreting - it's very literal, the business model and how it's facilitating these risks, but that's not the intention and that's not what was meant. I just wondered if there's value in lifting from the weeks and months and years that they've talked about this in Parliament, ministers words, words of Parliamentarians where they talked about the business model, and there will be examples of this and explaining that back to Ofcom. So Ofcom is interpreting the act in this way, but we have years where they discussed this Act and the purpose of it›.

Maeve, Chair

I think you're right and there absolutely is, and we've started trying to do that with the safety by design points as well, where obviously there was an awful lot of discussion and reassurances that's the way that the Act was going to apply that don't read across then as well. So I think that would be helpful to do.

Janaya, EVAW

The NPCC's Strategic Threat Risk Assessment identifies online VAWG and the forums its committed on as an 'intelligence gap' : https://www.npcc.police.uk/SysSiteAssets/media/downloads/our-work/vawg/vawg-stra-public-official.pdf

Jess, Refuge

A point following on from earlier about stalking and the lack of recognition of that as a course of conduct, I think we'd like to see much more in the consultation around coercive control as well and that being a priority illegal offence, and the chapter on that in volume two is fairly short. I think I'd like to see some more detail in that particularly around the gendered nature of risk and identifying coercive control, and more being pulled out about the link between control online and physical safety, tracking, that sort of thing. And then I think we follow that through to the codes of practice itself, it's very minimal on coercive control, really, it's only mentioned a couple of times, and mainly in relation to recommendations around platforms should have in place measures to allow users to block or mute other users. I think that exists on pretty much most major platforms already so if we're talking to a survivor of online coercive control and saying what impact these codes of practice are going to make for them, it doesn't at the moment look like a whole great deal will change in terms of their experience in future. I can pull out more for our joint submission but just wanted to make that point.

Maeve, Chair

Thank you, and just on that, the big table that we've done as well comparing the evidence that's in volume two with the measures that are recommended in volume four I think will be useful. In that work, we've gone through all the kinds of functionality and the specific offences identified as exacerbating or facilitating harm, and then showing that there are no mentions of many of these in the code practice. So we can certainly drop that into this submission as well. (*Please see Annex C Volume 2 and Volume 4 Analysis)*

Okay, we've got five minutes left. Thank you all so much. That was an amazing discussion and, and I think everybody's contribution to this has been invaluable. And what a powerful way of doing it, too. This has been really important. We did talk beforehand about whether Ofcom should be “in the room” or for this, pros and cons but I think certainly the power and the importance of this will come through in the transcript that we send over.

ENDS

Annex A My Image My Choice Survivor stories

Taylor, Engineering student, 22. The perpetrator uploaded six deepfake videos to several porn profiles including on PornHub. He impersonated her on these profiles, including her real name, college, hometown, profile imagery, and encouraged men visiting the profile to contact her. She experienced severe OCD and anxiety, questioning if she was going to drop out of school.

Ellesha. Intimate footage was captured secretly by a former partner and uploaded to PornHub on the day they broke up. He also created fake accounts on Tinder. She discovered he has a record for DV and was wanted by another police department for a similar incident, but the CPS questioned her testimony asking whether she and the other victim were conspiring against him.

Ruby, teacher, late 20s. On a single day she and 30 women reported to the police that explicit images on them had been found on a forum that lists victims via local area. Some images were taken from social media, some hacked from icloud storage, some posts shared personal details The women felt extremely physically threatened. The police gathered no evidence, misclassified several crimes, and were at times victim-blaming and insensitive.

Chrissy, Youtuber. Her ex partner got her extremely drunk, sexually assaulted her, and captured videos of this incident. He released it to her fans and widely on the internet years later. This led to severe PTSD and trauma.

Lauren, student/writer. She was spiked and sexually assaulted when she was 22 and the following morning discovered that the perpetrator had taken pictures during the assault and shared them with friends. She continued to experience harassment from the perpetrator on social media. Lauren dealt with serious PTSD, anxiety, eating disorders and suicide ideation as a result, with repeated panic attacks.

Gibi, Youtuber with 5m followers. She has experienced deepfake harassment and many types of online harassment. She has had to create fake identities and physically move house as a result. She's found websites making money by deepfaking her specifically, and knows of discord forums dedicated to deepfake abuse content of her. She has experienced vicious harassment and stalking.

Julia, 22, student. Julia found deepfake videos and imagery of her on various 4chan threads, alongside information about her college, name, and local area. The images were also accompanied by degrading and explicit comments. As a result of this abuse she decided not to pursue her dream career of being a Twitch streamer.

Helen, 34, poet and creative writing teacher. She was sent a link to multiple fake images of her in porn websites, depicting her in extremely explicit, degrading ways. This had a huge impact on her confidence, identity, sense of self. She sstarted experiencing panic attacks after discovering that she had been targeted.

THEMES

Cost to business

Direct impacts on your career / job prospects

- Julia, 22, wanted to become a twitch streamer but after being deepfaked decided that was too dangerous. “because then I'd be putting hours and hours of videos of my face on the Internet for someone to use however they want, for random strangers to watch me, to judge. So I think you kind of have to take all that into account and how, you know, the thoughts, judgments, opinions of other people can affect your mental health. I think it definitely will probably follow me for the rest of my life, I think I'm always going to have a grain of doubt with every interaction that I have”
- Lauren “if I ever became anyone or anything, if I ever followed my passion, like I want I want to be a writer, what if I write a book and this image shows up of me at age 22, terrified and sobbing. It felt like the image was ammunition that could be used against me for the rest of my life.”
- Gibi “My full time job is creating ASMR videos. I posted my first video in 2016. In 2016, I also made my first police report because I had received a few hundred too many emails from the same man who told me he was going to find me. The police were confused, but gave me their card, and told me there was nothing they could do unless he showed up. I walked to classes my final year of school terrified. But I kept posting. Over the last 7 years, I have published over 1,000 videos, garnered 4.8 million subscribers and 2 billion views on YouTube alone - something I’m very proud of. But it also made me an ideal target for deepfake pornography. I did not want to make sexual content. I spoke openly about how I did not consent to being used sexually. Of course, they did it anyway. And it was easy. And there was nothing I, the police, the law, or cybersecurity professionals could do. There was nothing the police or the law could do. The gold standard advice was: ignore it. because otherwise, they might do it more. I was contacted by a brand new service who offered to remove those horrible deepfakes of me - for $600 per video. I operate under the sick reality that women creators have to accept that you WILL be abused. I know I personally am a lost cause. I will always have digitally created porn of me online - for my future children to see, that will survive long after I’m dead.
- Helen, who is a poet and creative writing teacher, “I couldn't write, I couldn't read, I couldn't concentrate… I was getting behind with my work. Really anxious and hyper vigilant all the time.”

Impacts including on mental health, professional reputation, ability to do your job

- Lauren it “was an entire year of my life that I almost feel like I don't remember that year. And I was going through the motions of, like, trying to stay alive”
- Chrissy “It's like my body would show up, you know my brain was always off somewhere else, oftentimes 100 times a day thinking about this experience… having severe PTSD literally ravages every aspect of your life and your ability to hold down a job, maintain relationships, maintain mental health.”
- Chrissy “The daily impact included very quickly becoming bed-ridden, because I couldn't move, I couldn't think, I couldn't function without this being at the very forefront of all of my thoughts. It just became very easy to think about how death would be much easier than living this hell”
- Taylor experienced serious anxiety and OCD as a result of being deepfaked, shut down from social groups, feared that her professional reputation will suffer: “I was very

paranoid. It was just constant worrying about, like, are more people that I know going to see this? Are they going to see this type of stuff on like background checks? I would spend hours of those days like searching about it, thinking about it… It consumed what I did."

- Lauren "when your mental health gets that bad to the point that you're feeling like you have PTSD, depression, anxiety, eating disorders—those things are deadly. You know, like I am lucky that I didn't decide at one point to, like, take my own life. [This] could kill someone if they don't have the same resources I have."
- Julia "I'm very much more reserved around people, even friends that I have known for years now. I feel like I can't trust them"
- Julia "He can, in just a few hours of his life, put out content like this that can have the power to affect our lives forever"
- Gibi "There are so many women who don't end up pursuing their full potential or doing anything in the public realm due to fear. People who are afraid to go out, some who don't trust their partners, who suffer impacts on their mental health, reputation, their relationships, their lives. I am terrified for women and girls."
- Helen "Every time I left the house, I got a sense of dread. Everyone I passed in the street, I just felt like they knew."

Women withdrawing from social media

- Out of 30 survivors we have spoken to, *every one* of them had withdrawn to a certain extent from online spaces.
- Julia "My use of social media since finding out about the deepfakes has definitely dwindled. I don't think I've posted on Instagram in a few years."
- Taylor rarely engages in social media now, as she wanted to "block every single person that I think did it on social media" but as she cannot be sure she thought "I should just delete my social media." She very rarely engages with social media "even to this day."
- Helen talks about this making her aware of how she is watched, especially on social media, and that made her feel "alone and scrutinised. I didn't think I'd ever feel like [I could share things publicly] again. I'm going to go into hiding."

Annex B - Revenge Porn Helpline Additional Information (CONFIDENTIAL INFORMATION REDACTED)

Operation Makedom, Offender sentenced to 32 years: https://www.bbc.co.uk/news/uk-england-birmingham-59614734 He targeted up to 2,000 women and girls worldwide.