End Violence Against Women Coalition

DRAFT Submission to Government Consultation on the Online Harms White Paper

Ahead of the DEADLINE: 23.59pm 1st July 2019

How to respond to the consultation

The consultation closes on the 1st July 2019.

You can read more about the consultation on the Government website here: https://www.gov.uk/government/consultations/online-harms-white-paper

A Complete PDF of the paper is available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

You can respond online here: https://dcms.eu.qualtrics.com/jfe/form/SV_5nm7sPoxilSoTg9

Or you can email your response to: onlineharmsconsultation@culture.gov.uk

There is no need to answer all the questions – in fact, very few survivors, workers or experts would have the knowledge and expertise to do so. Please do use our answers to guide you if that is helpful. We have tried to write as broadly as possible and to include 'general principles' as a way of answering questions where specialist knowledge might be needed.

If you have any feedback or if there is anything you would like to see added please get in touch with Rebecca our Campaigns Manager at rebecca.hitchen@evaw.org.uk

EVAW will make updates to this document before the 1st July deadline, as we receive advice from our members.

About the End Violence Against Women Coalition

The End Violence Against Women Coalition is a UK-wide coalition of more than 85 women's organisations and others working to end violence against women and girls (VAWG) in all its forms, including: sexual violence, domestic violence, forced marriage, sexual exploitation, FGM, stalking and harassment. We campaign for improved national and local government policy and practice in response to all forms of violence against women and girls, and we challenge the wider cultural attitudes that tolerate violence against women and girls and make excuses for it. Our trustees include women who are globally renowned for their pioneering work in setting up the first domestic and sexual violence crisis services, for their academic research in this

area, and for having successfully campaigned for considerable legislative and policy change in the UK to end and prevent abuse over the last four decades.

Executive Summary

The EVAW Coalition believes that new law and policy being considered by the Government, in close 'negotiation' with the big tech giants, is a critical area where abuse of women and girls is very real, is increasing and needs specific naming and commitments. Any proposals in this area need to focus on changing the behaviour and attitudes of those who perpetrate online harms and the systems that enable them, rather than telling individuals how to 'stay safe' online.

Our Recommendations to Government:

- The Government's analysis and framework for regulating and attempting to prevent online harms should include detailed recognition of Violence Against Women and Girls ('VAWG') in all its online forms (in line with the Home Office-led Violence Against Women and Girls Strategy and Action Plan). The Government's approach should be clearly gendered and have regard for other inequalities which drive online harm (such as inequality related to ethnicity, age and sexuality), and the Government should seek to recognise and describe these harms as victims and specialist organisations see and experience them, not by the tech companies.

- So-called 'online VAWG' should be recognised as a wide and growing set of harms including but not limited to; image-based abuse, online harassment, the sending of unsolicited explicit images, coercive 'sexting', the creation and sharing of 'deepfake' pornography and much more. These harms should be recognised as related to one another because they have common drivers: women's and girls' persistent inequality, and other inequalities which intersect with this, such as the particular misogynistic racism targeted at Black women online, who research shows receive the most abuse from strangers on social media.

- Financial provision for support for victims of online harms in order that they are able to receive independent, specialist and trauma informed support and advocacy from organisations that are experts in responding and working with online harms related to inequality.

- A regulator with the teeth and independence to hold tech companies meaningfully to account in addressing and preventing online harms.

- Legal reform in relation to online VAWG – such as that recommended by Professor Clare McGlynn, and robust enforcement of existing laws.

- Mandatory transparency reports for tech companies which are just that - accessible, easy to find, with high levels of disaggregated data on the types and instances of harms reported, and demographics of victims and perpetrators, together with the response provided and satisfaction of the victim with said response.

- The liability for online harms to be recognised as resting with the tech companies and their designers as well as individual perpetrators; responsibility/liability for harm never imputed to a victim who should have "kept themselves safe".

- Relating especially to 'private communications' enabled by online platforms, there should be a new high level tech commissioning and design stage related principle which is: a company should be required to take into account, and to address and reasonably mitigate against potential harms, if it seeks to build in private chat for users whose identity is not verified. This should apply for applications aimed and marketed at adults or children, and would include for example gaming platforms aimed at children and young people; dating sites; social media aimed at children and young adults. It is clear that platforms and social media have already been built, and which are very profitable due to their reach and users, are ideal spaces for adults and young people who seek to 'groom', deceive and abuse through anonymised usernames and private chat which is invisible to others. Similarly, other platforms provide ideal 'conducive contexts' for individuals and groups to 'pile on' and harass and shame vulnerable individuals with impunity. When the potential for serious harm and abuse is clear at design stage, it should be acknowledged by the company and mitigated against. The regulator should make a high priority of enforcing this norm.

- A commitment to 'future-proofing' in the area of online harms including online VAWG regulation, to ensure that in particular the ever growing use of AI (see deepfakes) and other ways in which online harms will be perpetrated in future are within scope of the emerging policy and the regulator's powers.

Question 1: This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

-

The internet has undoubtedly been a force for good in promoting community and activism. When approaching these questions we have tried to balance the high levels of abuse and violence that women and girls face online, with the opportunity provided for free speech, community development and amplification of voice. #MeToo is a great example of the type of activism that is possible using social media and we would not want any regulatory measures to stifle or silence marginalised voices, nor for any regulator to become a de facto enforcement arm of the state.

-

Women and girls are subject to disproportionately high volumes of violence, sexualised abuse and hate online. This is known as 'online VAWG', but should be understood as part of a continuum of abuse which is often taking place offline too (such as harassment by an ex both on and offline). This can include but is not limited to:

- Harassment and stalking
- Monitoring and surveillance (linked to above)
- Threats of violence

- Sending unsolicited images and pornography which contain extreme sexual violence.
- So- called 'revenge porn'/ image based abuse.
- Generating and sharing 'deepfake' images.

As with offline forms of VAWG these activities are a cause and a consequence of women's inequalities and are also deeply related to intersecting inequalities including ethnicity, age and sexuality.

As Clare McGlynn points out, rape porn and image-based abuse, as well as harming the individual 'victim' in a deeply gendered way, also cause 'cultural harm', in that they 'may help to sustain a culture—a set of attitudes that are not universal but which extend beyond those immediately involved as perpetrators or victim-survivors of image-based sexual abuse—in which sexual consent is regularly ignored. By extension, this means that acts of sexual violence which are also predicated on an absence of consent are perhaps less likely to be recognised as such.[1]' Upskirting is a prime example of this, where the minimising of this behaviour, alongside the common occurrence of such imagery in pornography and even in tabloid media, creates a cumulative impression that the abuse is trivial if not harmless.

We are alarmed to see that porn as 'harmful' is only considered in terms of under-18s. There should be acknowledgement of the societal harms that sexual violence in mainstream porn creates[2]. In particular, how the existence and use of extreme pornography contributes to the cultural context within which society fails to take sexual violence against women seriously.

There is within the paper a disappointing lack of analysis as to how the extent and nature of online harm is disproportionately experienced by women, as well as sexual and ethnic minorities, and there is no real attempt to recognise these intersecting oppressions faced by individuals.

Research shows that this online abuse is even more prevalent for women of colour and LGBT+ people. Research by Amnesty International states that 1 in 5 women in the UK have been subject to online harassment or abuse[3]. A 2017 report by LGBT organization Stonewall commissioned by YouGov surveyed more than 5000 LGBT people across England, Scotland and Wales found that 10% of LGBT people experienced homophobic, bi-phobic and transphobic abuse or behaviour online in the last month[4].

---

[1] Clare McGlynn, Erika Rackley, Image-Based Sexual Abuse, *Oxford Journal of Legal Studies*, Volume 37, Issue 3, Autumn 2017, Pages 534–561, https://doi.org/10.1093/ojls/gqw033

[2] Fiona Vera-Gray et al, 'Sexual Violence as a Sexual Script in Mainstream Online Pornography', forthcoming.

[3] https://www.amnesty.org.uk/online-abuse-women-widespread

[4] https://www.stonewall.org.uk/resources/lgbt-britain-hate-crime-2017

In another piece of research Amnesty International also demonstrated that BME Women politicians are subject to massively disproportionate levels of abuse online[5]. Recent research by the disability charity Leonard Cheshire shows that reports of on-line disability hate crime are up 33%[6]. A recent petitions committee enquiry[7] also found high prevalence of on-line hate crime against disabled people, and stated that social media companies need to accept their responsibility for allowing toxic environments to exist unchallenged. They must ensure that their mechanisms and settings for managing content are accessible to and appropriate for all disabled people.

As established in the White Paper there is a significant risk that women and those from minority communities will be silenced by this abuse. Particularly as the 'solutions' currently offered by social media companies force women to do the 'safety' work and offer breaks as means of dealing with abuse, as such the 'solutions' are in themselves also silencing.

It is clear that there needs to be a gendered lens when considering online harms, but there also needs to be an intersectional analysis which recognises the multiple oppressions faced by individuals. This is lacking across the White Paper. It refers to online anonymous abuse of politicians but fails to draw out that it is Black MPs such as Diane Abbott MP who receive both sexist-racist abuse.

Given that government has committed time and money to a VAWG Strategy[8], as well as being signatories to a number of international treaties and conventions which identify VAWG and commit to tackling it, we would like to see a regulatory approach which specifically identifies VAWG as a sub-category harm in its own right. International and domestic law and policy around prevention of violence against women and girls (e.g. the Home Office VAWG strategy and the Istanbul Convention) recognise that policy should be joined-up and that tackling VAWG necessitates a commitment from all policy areas. Having specific strategies, regulation and guidance around this issue will act to ensure that social media companies which have been particularly slow to respond to and be accountable for 'online VAWG' will respond appropriately.

Having considered current 'transparency reports' the data shared is fairly meaningless as it is lumped by categories which do not give a clear picture of what is happening. For example Facebook has a category for bullying/ harassment but that

---

[5] https://www.amnesty.org.uk/online-violence-women-mps

[6] 2016/17-2017/18 https://www.leonardcheshire.org/about-us/press-and-media/press-releases/online-disability-hate-crimes-soar-33

[7] https://www.parliament.uk/business/committees/committees-a-z/commons-select/petitions-committee/inquiries/parliament-2017/online-abuse-17-19/

[8] https://www.gov.uk/government/publications/strategy-to-end-violence-against-women-and-girls-2016-to-2020

includes all types of bullying and harassment; as such it is unclear what proportion is racial hatred or homophobic etc. Data is only useful if it is disaggregated. In order to prevent and regulate online harms it is vital the government, regulator and the public understand the extent of the issue and are able to spot patterns of abuse. This is only possible if data collected is disaggregated in terms of different forms of harms. This enables targeted approaches and where there are links with other policy areas such as criminal justice it allows policy makers to have a joined-up data-set.

Transparency reporting should therefore include a separate VAWG category which could include abuse such as 'rape threats', image based abuse etc. Companies should show how they are taking steps to remove users who commit 'online VAWG'.

Transparency would also be improved if companies were to seek feedback from users on how they felt a complaint was handled and were asked to report on this too - in essence user satisfaction. All the above should be accessible, and easy to find and the regulator should compile these reports – with analysis – and potentially a rating system on their website.

Additionally, as recommended by Amnesty in their report '#Toxic Twitter'[9] we would like to see social media and others signpost to sources of support to those who have reported abuse. This goes hand in hand with a specific funding allocation for said support services.

Question 2: Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances?

Yes in theory we are in agreement that designated bodies should be able to bring a 'super complaint', however it remains to be seen if the 'super complaint' model is an effective means of holding bodies to account given the police super complaints system has only just started. In order for super complaints to be meaningful they must result in action. We see super complaints to be a recourse for the more marginalised in our society and would expect charitable organisations to be designated bodies.

We assert that if the regulator considered online VAWG as a 'harm' in its own right this would make the identification of thematic issues far easier. There is risk in making the circumstances overly narrow as the bringing of 'super complaints' will be a way for trends to be identified and brought to the regulator's attention. It is also important that the terms in bringing super complaints are not too overly narrow and restrictive given the fast moving and changing pace of the online world.

We would not wish for any regulator to be reliant on the super complaints system to draw attention to issues which require exploring. The regulator needs to have a pro-active approach at assessing and tackling online harms.

[9] https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/

Additionally, there should be a mechanism for individuals to bring complaints where there are no other options available to them and/ or they have exhausted 'internal complaints' procedure.

Any super complaints system should include scope for appeal of the decision.

Question 2a: If your answer to question 2 is 'yes', in what circumstances should this happen?

This should probably operate in a similar manner to the current super complaints system, where complaints are thematically grouped in order to better identify systemic issues. We would like to see any super complaint process apply to single companies as well as groups of companies for example a complaint about Twitter or a complaint about social media companies which would take in all providers of social media operating in the UK.

If super complaints are only to be brought by designated bodies we feel there needs to be a process in place in which the individual can appeal to the regulator having exhausted the company's complaints procedures.

Question 3: What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

Because companies' voluntary codes are commonly inadequate in responding to online VAWG, we need a mechanism of appeal or option to approach the regulator directly when online harms have been experienced and the company response has been inadequate. Too often companies rely on the existence of their terms and conditions in response to complaints about harmful activity. However, as the White Paper itself states there is a perceived lack of transparency around the implementation and enforcement of these policies. 70% of Britons consider that social media companies do not do enough.

In addition to the regulator there must be effective enforcement by police and CPS where criminal offences are committed online. Women's organisations hear frequently about police officers not taking online harm seriously where there has been specific illegal activity reported. There is a lack of understanding among officers of the use of online spaces to perpetrate abuse and a lack of understanding of the harms it causes. The existence of a regulator and complaints procedure must not create any police perception that it is not their responsibility to deal with reports and that online harms are somehow "less serious".

Particularly problematic is that many forms of online VAWG are not criminalised, or are criminalised with critical gaps in the law, for example related to intent. The Government should urgently extend the anonymity granted to victims of sex offences to those reporting online VAWG.

There is an absence of provision for support of those impacted by online harms. As Professor Clare McGlynn, a leading academic on image based sexual abuse, notes, there is no recourse for victims in getting material taken down. In her paper 'Shattering Lives and Myths – a report on image based sexual abuse' (Published 1st July 2019)[10] she found that for many victims their first imperative is for material to be taken down, but that this is difficult, cumbersome and time consuming. The White Paper makes little if any reference to this, when victims place it as high priority.

Any white paper that seriously wants to tackle online harms needs to properly consider the harm caused to individuals and society and the support that should be provided to individuals who have experienced harm. A preventative approach must include provision of support, and that means establishing a requirement for it, as well as funding and resourcing. We know that specialist organisations – the ones which women are most likely to turn to when they have experienced offline and online abuse are severely underfunded and unable to respond to the huge levels of demand they face[11]. The strictures of funding and commissioning models means that these specialist organisations are hard pushed to deliver their core work, and therefore unable to grow at the pace needed to be able to respond to these additional forms of harm.

Question 4: What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?

Parliament should have scrutiny over the impacts of the regulator, particularly in regards to the its independence, perceived and otherwise from tech companies. We are concerned at the potential for the independence of the regulator role to be compromised by assigning it to individuals overly connected to the companies they were meant to be regulating. While there is a need for the regulating body to be comprised of experts in the field the body needs to be able to have a robust and critical analysis of the tech companies.

The UK Council for Internet Safety could also be a mechanism by which to assert additional scrutiny of the work of the regulator. However, while this body has ministerial leadership it is not a funded body, thereby potentially limiting its potential in this respect. We support and endorse the work they are planning in the coming year.

Question 5: Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

[10] Clare McGlynn et al, Shattering Lives and Myths – a report on image-based sexual abuse (1 July 2019). And see discussion in: https://www.huffingtonpost.co.uk/entry/upskirting-image-based-abuse_uk_5c0e1fe7e4b0239a97100d80

[11] Violence Against Women and Girls policy briefing UK Women's Budget Group (2018) https://wbg.org.uk/analysis/2018-wbg-briefing-violence-against-women-and-girls/

We are concerned that this white paper lacks ambition and analysis of online harms in view of its scope. We are also mindful of the power and influence of global, powerful 'tech' companies. We hope that the scope of the white paper, and remit of the regulator, remain a robust response to the lobbying of vested interests.

We are pleased that the scope is broad enough to cover all social media sites, as well as pornography sites, as they share user-generated content (users upload material). In relation to scope of the harms we would note that the use of term 'revenge porn' is unhelpful and problematic - abuses of this kind should be referred to as image based abuse.

The white paper also does not recognise the harms of 'fakeporn' when discussing AI and #deepfakes – it fails to consider that a key way in which deepfakes are being used and indeed what is driving some of the technology development is to create fakeporn. In this context a discussion of the development of AI and deepfakes must take into account the use of these technological developments to harass and bully women. Fakeporn[12] is a serious problem and victims suffer significant harms when this material is made and created without their consent. Scots law does criminalise fakeporn but English law does not and so far the Government has failed to extend the law (see question 17 below).

We also have a concern that this white paper is not 'future proofed' against further technological advances particularly in relation to AI. It is playing catch up to some of the existing issues regarding online harms but is not forward looking enough to respond to ways in which AI and other advancements can and will be weaponised to harass and abuse women and others.

We are disappointed at the absence of any acknowledgement of the dark net and the illegal activity found there – particularly relating to child abuse images and networks of abusers. We recognise the inherent difficulties of the dark web and yet feel that its existence should be factored in to government efforts in this field, and explicitly referenced. We are aware that end to end encryption for example makes linking to the dark web easier – and suggest this is considered in relation to what constitutes private messaging.

Question 6 In developing a definition for private communications, what criteria should be considered?

From a VAWG perspective this is a difficult question. Online messaging and private forums enable people to build networks and share ideas with like-minded people, they have been utilised by communities such as the LGBT+ community to reduce loneliness and isolation and we would be keen to avoid over interference. However, we know that private messaging and forums have been used by groups intent on harm, e.g. men sharing child abuse imagery, also groups promoting fascism and

[12] https://metro.co.uk/2019/05/31/deepfake-porn-ethics-able-watch-whatever-imagination-desires-9526079/

racist violence, and there are a number of forums created by and populated by those who wish to spread hate and misogyny.

In relation to the companies in scope of this paper we know that they see their private communications channels, particularly when encrypted, as a significant selling point of their product, and for many a USP. They are creating a market which incentivises private communication. When a company builds a product and profits from it, it stands to reason that they should additionally be accountable for the social consequences of that product.

There is a responsibility which should be placed on those making concerted design choices which will allow (and could in fact encourage) online harms to be perpetrated. An example here are gaming platforms specifically targeted at children where users are enabled to engage in online private communication. There are vulnerable users and the company which designs and profits from their use should also be accountable for their protection. They are creating a conducive context for abuse to occur, and for perpetrators of child sexual abuse to target and groom children and young people. This is predictable given the knowledge held around perpetrators' behaviours and motivations.

It is not enough for tech companies to shrug their shoulders and assert they are not responsible for the "bad things that bad people choose to do" they are an active participant by virtue of owning the space and therefore liability should extend to them. Another example in this vein is online dating sites where women can be abused online and encouraged to arrange offline meets by deception. We have long placed the burden of preventing harms on offline companies such as pubs, clubs and betting shops. Where it is clear that a place or 'product' can create a possible setting for harm then the company benefiting should share liability if harms occur, and aim to prevent in the first place.

Question 7: Which channels or forums that can be considered private should be in scope of the regulatory framework?

This question is beyond our expertise.

Question 7a: What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

These channels and forums should be subject to the design principle described above – when their product has potential for abuse, they should be required to set out how they would mitigate this. They should also be required to collect data on usage ad reported harms.

Question 8: What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?

This outside the expertise of EVAW and will not be responding to this question.

Question 9: What, if any, advice or support could the regulator provide to businesses, particularly start-ups and SMEs, to comply with the regulatory framework?

The regulator should develop more detailed guidance on the design principle/duty described above – where those building platforms/applications where there is potential for online VAWG must set out how they will mitigate this – and proactively share this with start ups and their investors.

Question 10: Should an online harms regulator be: (i) a new public body, or (ii) an existing public body?

Our priorities for the body are that it be independent, effective and responsive in its duties, with adequate "teeth" in order to encourage or require compliance. We do not believe we see a regulator as so described in existence currently so have some concerns about endorsing any existing public body (such as Ofcom or the BBFC). A new body with appropriate expertise for this sector should be established, and then required to make good working links with the existing media industry regulators.

Question 10a: If your answer to question 10 is (ii), which body or bodies should it be?

Question 11: A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

The tech industry should contribute based on a percentage of their overall income. These contributions should be required and paid over in such a way that no influence on regulator policy and practice can accrue to the media companies.

Question 12: Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?

Yes to all of these as regulator powers. The risk of disruption of business activities can be effective in ensuring that due consideration is given to the statutory duty placed upon companies.

We welcome the strengthened audit functions of bodies such as the ICO.

Question 13: Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

We are concerned about the complexities of jurisdiction for any regulator, and the ways in which enforcement can be carried out in relation to companies based abroad. We support the proposal for a nominated representative in the UK and EEA, but we seek assurance that any such circumstances would be transparent and not afford any preferential treatment to companies based in certain countries.

Question 14: In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

It is EVAW's view that a Judicial Review is sufficient.

Question 14a: If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?

Question 14b: If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

Question 15: What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

This is generally beyond the expertise of EVAW, but we wish to state, in case this is implied in the question, that the ability to innovate should not be framed as in conflict with or hindered by the duty to create a safe products. When thinking of other sectors we do not regard safety as a hindrance, but rather as a bottom line. The tech sector arguably needs to catch up on its social responsibilities in this area.

Question 16: What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

Creating 'safety by design' is of vital importance when considering the prevention of online harm. There needs to be ethical frameworks and online harm analysis when designing software and devices that mean that the default setting is the software/device at its safest for all potential users to navigate, and the least likely to nudge and encourage users into participating in forms of online hate or abuse; or being exposed to these. Having features which have to be actively enabled by the user means that users are making informed choices. However, the onus cannot rest solely on the user, they must rest primarily with the software designer, the tech company, those financially benefitting from the product and the data collected by it.

'Safety by design' requires an analysis of the product with a view how it could be used to enact harm. Organisations need to have an understanding of VAWG, and its

impacts, and the ways in which abuse is perpetrated, together with an understanding harm and trauma. This training should be provided by specialist services. For example heating appliances inside the home that are controlled by a mobile device seem convenient, but understood within the dynamics of a domestic abuse relationship means the perpetrator monitoring and controlling his partner's home environment, even when he is not present in the house. Similarly creating a product which emphasises privacy and encryption means that it will be more likely to be used by individuals looking for ways to communicate and share content which is illegal and/or harmful.

Question 17: Should the government be doing more to help people manage their own and their children's online safety and, if so, what?

It is paramount that Government actively helps people understand harms online and that children are educated about risk but also taught of the impacts of using social media to commit harms such as bullying. In terms of online VAWG this preventative work could be done through the new Relationships and Sex Education (RSE) lessons.

Public awareness campaigns should also be regularly run which highlight harms, not just financial scams and the risks of sharing information online but of bullying and abuse, the effects of this but also the fact that some of this is illegal and can result in prosecution and imprisonment.

Glitch[13] are an example of an organisation who are doing excellent work in this area. We fully endorse their digital citizenship approach[14].

Rape threats are a particularly common abuse tactic employed by those who would wish to silence women, when there is a crisis in the prosecution of rape[15] these kinds of threat left unchallenged are particularly damaging to the individuals receiving them but also to society as a whole, together they trivialise the harm caused by rape. We would like to see more robust action taken on this most routine but pernicious type of abuse, including an awareness campaign that highlights how unacceptable this would be in other circumstances i.e. anonymity does not make this OK.

In regards to children and young people and the sharing of explicit images, there is a lack of understanding of gender as a key driver. It is predominantly girls who are asked and coerced to take images and send them, it is predominantly boys who ask for the images and share them without consent.

The White Paper does not canvass law reform options but, if we want to 'reduce online harms' one way is to have a proper, comprehensive criminal law that covers

[13] https://fixtheglitch.org/

[14] https://fixtheglitch.org/digital-citizenship/digital-citizenship-our-definition/

[15] https://www.endviolenceagainstwomen.org.uk/campaign/rape-justice-fail/

all forms of image-based sexual abuse (amongst other abuses) and properly resourced (and trained) police[16]. Additionally, there should be better enforcement of existing laws, for example the extreme pornography laws[17].In relation to extreme pornography offences, there remain few prosecutions and the vast majority are for bestiality images, rather than rape porn and other serious violence[18].Notwithstanding the recent Ministry of Justice announcement of a review of sexual online offences[19].

Question 18: What, if any, role should the regulator have in relation to education and awareness activity?

The regulator should play a role in making the public aware of how companies are regulated and what their rights and protections are. This should be through a number of media but as starting point would be to ensure that as part of the regulation of companies they are mandated to outline to users in clear easy to understand language what harms they are protected from on their site/ platform, how they are working to address harms and how they can raise concerns.

However the problem with a focus on education means that there is a focus on the individual to 'stay safe' rather than focussing on changing the behaviours of perpetrators. We exist in a society which is far more likely to blame and shame victims than apportion responsibility on perpetrators. We see this often with offline sexual offending -particularly in the lessons and guidance around Childhood Sexual Exploitation which focus on 'spotting' signs of abuse etc. We are concerned this would be replicated here – with the attention being placed on telling girls not to take and send images rather then educating boys not to share without consent. By not focusing on perpetrator actions and on broader cultural attitudes, any 'awareness raising' will be problematic and incomplete.

We are also concerned that any such work will divert energy and resources much better spent in ensuring implementation of the statutory duty and codes of conduct.

There should be an ongoing conversation between the Department for Education and the regulator – particularly in relation to Relationships and Sex Education and Safeguarding guidance. Online harms should be incorporated in all RSE curriculums, with a focus on how to behave online that does not purely focus on safety and avoidance, predominantly by girls. Schools should be funded and empowered to

[16] We have already extensively cited the work of Prof Clare McGlynn

[17] All Party Parliamentary Group on Sexual Violence Inquiry into Pornography and Sexual Violence 2018 Evidence Submission from Professor Clare McGlynn, Durham Law School, Durham University: https://claremcglynn.files.wordpress.com/2018/05/appg-porn-mcglynn-hyperlinks-final-2-april-20181.pdf

[18] Idem.

[19] https://www.endviolenceagainstwomen.org.uk/review-of-image-and-online-abuse-laws-is-too-little-too-late/

work with parents and the wider community regarding online harms as part of their Whole Schools Approach.

Contact:
End Violence Against Women Coalition Policy and Membership Manager, Beccy Shortt:
beccy.shortt@evaw.org.uk / 07903 265 643 / www.evaw.org.uk