Written evidence submitted by Glitch

DCMS Sub-Committee Call for Evidence: Online safety and online harms

September 2021

About Glitch

Glitch is a UK charity (no. 1187714) that exists to end online abuse and to increase digital citizenship across all online users. We believe that our online community is as real as our offline one, and that everyone should work together to make it a better place. We work to promote good digital citizenship and address online harms such as online abuse, online hate speech and information disorders, and have developed bespoke training programmes covering Digital Citizenship, Online Active Bystanders and Digital Self Care and Self Defence. As part of this, we have delivered training to women in public life.

We are submitting evidence to the DCMS Sub-Committee's inquiry because we believe that the Online Safety Bill has the potential to make a significant difference to the prevalence of online abuse experienced by internet users in the UK. However, for it to appropriately serve those disproportionately affected by online abuse – women, and especially Black women, and racialised and minoritised people – Glitch believes that the Online Safety Bill needs to be strengthened, with their lived experiences at the core of this legislation.

Summary

Q1: ***Words matter:*** *The change from harms to safety shifts the focus from the perpetrator of abuse and places the onus on the target of abuse. We are concerned that the Bill does not adequately recognise the disproportionate impact of online abuse on women and marginalised communities, which has increased in prevalence since the start of the pandemic. The regulator's enforcement powers need to be strengthened and the Bill needs to work with existing commitments, strategies, laws and policies that aim to end all forms of gender-based violence, of which online abuse is a part.*

Q2: ***Women's inclusion in the Bill must not be left to chance:*** *We are concerned that the primary legislation does not recognise that women are disproportionately impacted by online abuse and therefore their inclusion in the Bill is left up to secondary legislation and processes. We believe the provision around those with "combined characteristics" needs to be strengthened. Processes for determining harm can not rely on AI, which is often biased and un-nuanced, and human moderators need to be supported in a holistic manner which recognises the psychological impact of the work.*

Q3: ***Far greater emphasis on harm related to platform design, systems and processes needed:*** *We believe large category one platforms could comply with the current approach without creating change on platforms that meaningfully improve the user experiences of those most at risk of being targeted by abusers, and the current approach does not take into account the legal but harmful online abuse that occurs on non-category one platforms. Current business model of tech companies does little to discourage online abuse on platforms and much more needs to be done to create safer online spaces.*

Q4: ***Women are missing from the Bill:*** *those who are most targeted by online abusers are not explicitly included in the Bill. Rhetoric around the Bill states that racist online abuse will be stopped and online misogyny tackled, yet it is unclear how the Bill will achieve this. Anonymity is not mentioned, despite being debated by politicians earlier this year. Freedom of expression and increased regulations to end online abuse should not be seen in opposition – online abuse is a behaviour that deliberately silences and is a threat to the freedom of expression of victims of abuse.*

Q5: ***Most online abuse is legal but harmful****: removing legal but harmful provisions from the Bill – as some suggest – would weaken the provisions for most online abuse, which falls into this category.*

Freedom of expression is not the freedom to abuse. Any Law Commission recommendations that may be adopted into the Bill should be strengthened by expert advice, to remedy any unintended consequences or weaknesses. The Bill must align with existing CEDAW and Istanbul Convention commitments, as well as the Tackling Violence Against Women Strategy.

Q6: ***Existing international legislation with gendered, intersectional perspective:*** *As well as paying close attention to the Digital Services Act, lessons could be learned from the Australian e-Safety Commission, which focuses both on women and diverse groups, recognised to be most at-risk online. As other countries develop new legislation in this area, we will be noting where women are appropriately included. The UK Government should also consider its pre-existing commitments in the area of all forms of gender-based violence and the forthcoming Law Commission recommendations on hate crimes.*

Full evidence submission

Q1: How has the shifting focus between 'online harms' and 'online safety' influenced the development of the new regime and draft Bill?

Glitch acknowledges that the UK Government has stated that there has been no shift in focus and not to read into the name change on the face of the Bill. However, we believe that words matter and therefore highlight our concerns below.

The shift between harms and safety in relation to online abuse against women can be compared to how violence against women offline can be seen as an issue that women are told they need to mitigate against themselves – women are frequently advised to alter their own behaviour to "keep themselves safe", such as not walking alone at night - rather than there being a focus on the violence or "harms" done to them by perpetrators. Similarly with the change in narrative around the Online Harms/Safety Bill, the syntactical shift suggests that the onus is on those harmed to take steps to increase their own safety, rather than the legislation making meaningful inroads to reduce the harms they routinely experience in the first place and hold perpetrators of online harms and abuse, and companies whose platforms and apps allow and profit from it, to account. Cultural theorist Jackson Katz outlines the pervasive preference to talk about violence against women in a way that masks how it is a male violence issue. We believe that 'safety' rather than 'harms' performs a similar shift with this Bill.

Frequently, women are advised to leave the online space "for their own safety" when subjected to abuse, or platforms offer women extra tools to mitigate against the impact of being abused online, rather than reducing the abuse and improving the user's experience by allow her to use the platform without experiencing abuse and threats through seeing and hearing harmful content. We believe that 'harms' conveys the range of harms that can take place online and the spectrum of approaches or manifestations that have physical and psychological impact whether illegal or not.

By contrast, the term 'safety' is very reductive, free from the worst types of online abuse and free from violence. Safety fails to convey the importance of flourishing, not just mitigating negative experiences online, and enjoying freedoms online. It also fails to convey the role social media companies must play in ensuring these rights and freedoms become a reality for women on their platforms and online more widely.

A better, more effective approach would be to enact effective ways to reduce online abuse in the first place, by investing in good digital citizenship education, as well as changing the way that social media platforms' current business model champions the volume of interactions, whether these are of

positive, negative or neutral impact to the user, and thus profits from online abuse as generated content, data and attention given to the platform.

The Online Harms White Paper was welcomed but fell short when addressing the disproportionate levels of online harms faced by women and marginalised communities. Despite commitments from the UK Government and social media companies, online harms, abuse and harmful content continues to thrive in online spaces. The COVID-19 pandemic has fuelled new forms of online violence and exacerbated gender-based abuse (which online abuse is a form of), epically for those with multiple intersecting identities such as LGBTQAI+ women, Black women, women of colour and disabled women, presenting unique challenges for our collective safety online.

Published in September 2020, Glitch and the End the Violence Against Women Coalition Covid-19 and the Ripple Effect report showed an almost 50% increase in online abuse for women and non-binary people in the UK during the first UK lockdown, with these figures worsening for those from minoritised backgrounds. The unique circumstances we are experiencing due to the pandemic have made the introduction of robust legislation to address online harms more urgent. We welcome the UK Government's recognition of the severity of online abuse, particularly racist, antisemitic and misogynistic abuse, as well as calls for greater transparency from technological companies. However, as civil society organisations working across sectors in the UK to address online harms, we have concerns about gaps in the forthcoming legislation and programme of work to support this.

Glitch wants to awaken a generation of good digital citizens, rather than advocating for increasingly severe punishments for those who perpetrate online abuse. Perpetrators of online abuse are users of platforms that reward and do not adequately dissuade or impose consequences for bad behaviour. If we are to see the online space as part of everyone's right to be online, which we at Glitch believe we should, and as the new 'virtual town square', we need to ensure that the UK Government invests in awareness of what it is to be a good digital citizen, in the same way that we raise awareness of other societal changes in the offline world. For example, demonstrating the harm of not wearing a seatbelt in a car by providing information of the potentially devastating impact this could have on ourselves and those around us, as well as legal changes, rather than changing the regulations without raising awareness and simply punishing abusers online for behaving in a way that we have never told them not to.

Digital citizenship is key in addressing online abuse and should be made available to young people and adults alike in settings such as workplaces, industry organisations and trade unions. ***All individuals have a right to safely and freely engage in all online spaces without discrimination. Digital Citizenship is respecting and championing the human rights of all individuals online, and encompasses three key elements: individual, social and institutional responsibilities.*** Glitch believes that digital citizenship is an essential solution to ending all forms of online abuse. Our approach and perspective on digital citizenship is built on definitions from the Council of Europe and Australian Curriculum.

Our report on COVID-19, The Ripple Effect showed that 9% of victims faced online abuse from a colleague or superior at work - this means that employers need to put in place robust harassment policies in the workplace and introduce digital citizenship training for their employees, bearing in mind that the latter can also be perpetrators.

Greater investment in digital citizenship initiatives for adults would ensure that organisations providing such training can deliver their services at scale. The government and policy makers should also ensure that digital citizenship resources are widely distributed to the greater public.

During the Secretary of State's statement in December 2020 on the Online Harms White Paper and throughout more recent rhetoric around the Online Safety Bill, there has been little mention of the types of harms that women - especially those with multi-intersecting identities - face. The Secretary of State did make reference to anti-Semitism in his oral statement in December 2020 but failed to

acknowledge the intersection of race and ethnicity with gender and other identities that, because of tech design, make people with intersecting identities more likely to face online abuse. While we welcome the inclusion of "combined characteristics" in the Bill by way of addressing the intersectional nature of the disproportionate way online abuse affects people with different protected characteristics, we would like to see this further developed to reduce ambiguity as to how this will be impactful to those who are experiencing online abuse.

Globally, women are 27 times more likely to be harassed online than men. A poll conducted by Amnesty International (2017) across eight countries including the UK and USA showed that nearly a quarter (23%) of the women surveyed across the eight countries said they had experienced online abuse or harassment at least once, including 21% of women polled in the UK. A 2018 report by Amnesty International found that in the UK and the US, Black women are 84% more likely to experience online abuse than white women.

The COVID-19 pandemic has exacerbated online abuse targeting women and marginalised communities. In our most recent report 'The Ripple Effect', Glitch found that almost 1 in 2 (46%) women and non binary people reported experiencing online abuse since the beginning of COVID-19 and 1 in 3 (29%) of those who had experienced online abuse prior to the pandemic reported it being worse during COVID-19. Online abuse not only violates an individual's right to live free from violence and to participate online but also undermines democratic exercises.

While some argue that increased regulation threatens freedom of expression, there is often little attention given to the way that the current status quo, where communities and groups of people are disproportionately affected by 0nline abuse and have their own rights to freedom of expression impinged, through tactics that deliberately threaten, silence and drive users from particular demographics out of the online 'public square' altogether.

Some also argue that one can make a distinction between online and 'real life', however at Glitch we make no such distinction as the online and offline space increasingly merge and online actions can and do lead to offline consequences, for example through psychological and physical harms. In recent weeks, the impact of harmful content online and its offline consequences has been evidenced by the mass-murder of five people in Plymouth, including the gunman's mother, at the hands of a man with links to the 'incel' (involuntary celibate) movement; it has been suggested that the murders may have been fuelled by online anti-women propaganda.

The Bill also needs to worth with existing work and not in silo, particularly in relation to the implementation of the UK Government's Tackling Violence Against Women and Girls strategy and Domestic Abuse Strategy.

Online gender-based violence affects our society as a whole, both online and offline. It is also a huge digital threat to our democracy in the UK and in democracies across the world. Research has revealed that online abuse is one reason many women MPs choose not to run for re-election. More diverse political representation at all levels of politics makes for stronger democracy that should serve all, not just those who are in the same demographic as the vast majority of politicians (older, white, males) who are not systematically driven out of political careers through campaigns of online abuse.

Technology companies cannot fulfill their duty of care to online users without addressing the disproportionate gendered impact of online abuse. We acknowledge that whilst increased accountability for technological companies - including annual transparency reports - is a positive step, there are limitations for how we can truly make the online space safe for all without an increase in digital citizenship education.

We call on the UK Government to include specific recognition of the disproportionate impact of online abuse on women. Women have a fundamental human right to live free from fear and threat of violence and abuse. Women have fundamental rights to be able to use the internet without having to

decide how to keep themselves safe. Women do not just need extra tools on platforms to support themselves or report abuse they have already experienced, and the solution is not for women to come off the internet. The UK Government must accept and acknowledge the high levels of online violence against women and girls in the legislation, not in a subcategory of harms, to be decided later in the legislative process through Ofcom's recommendations.

While financial sanctions against technological companies and the enforcement of the duty of care are essential in addressing online harms, more investment in impactful digital citizenship is needed to make the Internet a safer space. We believe that much more is needed in this Bill by way of prevention: through the promotion of digital citizenship education and building on the newly published Media Literacy Strategy. We also want to see the enforcement powers of Ofcom strengthened, to ensure that the regulator can meaningfully hold companies to account.

Online abuse is a form of violence against women and can be a tactic used by strangers to silence women in the online space, and particularly target racialised and marginalised women. It can also be used in intimate partner violence as another controlling, violent behaviour against an individual, alongside offline behaviours. The specialist violence against women sector has a vital role to play in protecting survivors of all forms of violence against women, including online abuse but this work also needs to be funded.

As the UK Government looks to introduce new laws to make the UK the safest place to be online, we are urging the Chancellor of Exchequer to ring fence 10% of the new digital services tax to help achieve this. The Digital Services Tax of 2% on tech giants like Facebook, Google and Twitter is expected to raise an additional £400m a year (£70m (2019/20); £280m (2020/21); £390m (2021/22); £425m (2022/23); £465m (2023/24); £515m (2024/25)). It is essential that the UK Government provides funding to the the specialist violence against women sector and online abuse organisations to support victims of online abuse and helps fund the vital work of ending online violence and abuse, such as through training on good digital citizenship and online safety, providing resources and awareness raising and supporting survivors of online abuse and violence. By ring fencing at least 10% of this new tax annually for ending online abuse, the UK Government can commit £4m+ to further establishing online standards which are fair and necessary to the growing digital economy, funded by the tech giants where these societal harms are pervasive. Through no negative deficit, using money from tech giants, the UK Government can take decisive action.

Q2: Is it necessary to have an explicit definition and process for determining harm to children and adults in the Online Safety Bill, and what should it be?

It is imperative that the definition of harms for both women and children includes online gender based violence. We are concerned that without a definition that includes an intersectional understanding of the gendered and racialised nature of online abuse in the primary legislation of the Bill (which take into account the combined and intersecting identities of those affected), we risk the chance of this Bill failing to make real changes to those who are most frequently affected by online abuse. However, we acknowledge that the pace of technological advancement and the ever-shifting nature of online abuse means that any such definition should be flexible enough as to apply to emerging harms and not be easily made irrelevant or less effective in the near to distant future. The definition should also take into account the impact of harms that may be physical and/or psychological for the intended victim, as well as other users affected by viewing the content.

We believe that processes should be trauma-informed, and produced in collaboration with victims/survivors of online abuse, who are appropriately supported and remunerated for their input. We believe that over-reliance on AI technology to identify toxic and harmful content has limitations - for example, active bystander interventions or discussions about issues such as racism from good digital citizens can be flagged as offensive by AI software which blocks content based on words used rather than sentiment. Online abuse can be personally targeted in a way that would be too nuanced for

AI systems to highlight, particularly by a perpetrator known to the victim. Perpetrators of online abuse adapt strategies to bypass AI systems, for example, by using different or special characters or spaces in offensive words to get past detection.

While we support the use of human moderation, the role of a content moderator takes an incredibly heavy toll on the person's psychological and mental wellbeing, as they are tasked with reviewing potentially harmful and upsetting content for hours at a time, therefore the risk of vicarious trauma is high. While moderators themselves are not the primary target of the abusive content they are reviewing, they may be from the protected class being targeted or be psychologically triggered in other ways. Such work tasks must be supported in a holistic manner, with good psychological support for the moderator's wellbeing. Human moderation is far more advanced and nuanced than AI, but it comes at a human cost that we cannot underestimate.

Q3: Does the draft Bill focus enough on the ways tech companies could be encouraged to consider safety and/or the risk of harm in platform design and the systems and processes that they put in place?

We do not believe that there is not enough emphasis on risk of harm related to platform design and the systems and processes they put in place. We believe that the current suggestion of a risk assessment based approach for category one companies and no provisions for those that are not category one when it comes to legal but harmful content. A large proportion of online abuse falls into this category, and its exclusion for non-category one companies is very disappointing as we do not believe that the current approach will bring meaningful change with regards to the disproportionate impact of online abuse on women and girls, as well as those from racialised and marginalised communities. We believe that big technology platforms (category one) can afford to comply with the regulations in a way that may not do enough to prevent harm to users and this system does not challange the current business model of tech giants, which prioritises the attention of users at any cost - i.e. interactions based on targeted racism, sexism, ablism, transphobia, homophobia, anti-Semitism, islamophobia etc are as beneficial to the company as the sharing of a harmless comment.

Reporting and moderation mechanisms can add to the emotional and psychological burden when it comes to reporting abuse, where users are asked to report each individual piece of abuse to the platform, who then reportedly frequently respond in a less-than-timely manner, often stating why such content does not violate their policies. Even when content has been judged to violate platform's policies, the content has often been left on the site while such an assessment is made, meaning that much of the intended damage has been done.

Despite platforms' growing investment in content moderation, we have to recognise that moderation policies are not achieving good enough results and are not properly enforced. By comparison, we have seen what is possible on platforms that have made commitments to appropriately address Covid-19 misinformation, where companies have acted with urgency due to the seriousness of the public health threat relating to the pandemic. Online abuse also has huge public and individual health implications - and can be a matter of life and death - therefore it should be treated with similar urgency, resourcing and intervention by tech companies.

As online abuse continues to thrive on social media:

- Platforms should ensure their policies are properly enforced and constantly reviewed to reflect changes in language and take into account mechanisms that allow abusers to bypass their detection mechanisms
- Platforms should make their content moderation policies as clear and understandable as possible
- Platforms should improve their reporting mechanisms. In particular, platforms should acknowledge all reports of inappropriate behaviour and notify the user of the steps being

taken to address the issue. They should review those reports within 24 hours, send a warning to the flagged users, and then, if the problematic user persists, remove them from the platform
- Existing features and optional tools for personalising user experience on the platforms should be made available and more obvious to all users, rather than relying on platforms mentioning tools in news articles once perpetrators of online abuse have already targeted victims (as was the case following the England Football European Championship 2020 campaign) or charities such as Glitch raising awareness of pre-existing features to small cohorts of online users at a time

While policies are in place, they are still not always properly enforced and reporting mechanisms are complicated to navigate for victims of online abuse. Beyond content moderation policies, social media companies' content moderation processes need to be changed to provide greater transparency, including:

- Algorithmic transparency: the independent regulator - Ofcom - should be able to audit tech platforms' content moderation algorithms
- Transparency about the number and nature of reports received and why content moderation decisions are made

The design of social media platforms has allowed harmful behaviours to thrive, by allowing content to go viral unchecked. Platforms' business models are also closely linked to the attention economy, with recommendation algorithms presenting social media users with ever more extreme and sensationalised content to capture our attention. We need to recognise that platforms' business priorities cannot take precedence over the online safety of users. The Online Safety Bill has set out a 'duty of care' for platforms towards their users. Platforms therefore need to change their processes to ensure they do not fuel online abuse - for example by reducing virality mechanisms or making sure repeat offenders who have been banned from platforms cannot create new accounts.

Q4: What are the key omissions to the draft Bill, such as a general safety duty or powers to deal with urgent security threats, and (how) could they be practically included without compromising rights such as freedom of expression?

Abuse of women online is endemic and legislation for online safety/harms needs to recognise this both in the rhetoric around the legislation, as we have seen from DCMS ministerial announcements, and explicitly within the legislation itself. It is important that women are explicitly named in the primary legislation and our inclusion not left to chance in the secondary legislation process, relying on the assumption that women's inclusion will be recommended by the regulator Ofcom, and subsequently agreed and passed by parliament.

A gender-neutralised piece of legislation and policy agenda imposed on a highly gendered issue, as online abuse is, does not deliver a gender-neutral outcome, as we have seen from supposedly gender-neutral policies implemented by platforms, which position white, straight males as the 'norm'. These do not acknowledge the multiple intersecting privileges that this small demographic - who are driving the tech agenda in the vast majority of big tech companies - hold in global society, both offline and online. Treating 'sexism against men' as equal to sexism against women or so-called 'racism against white people' as equal to anti-Black racism on a platform is a driver behind the harmful online environment that we so desperately need to change. What's more, it champions white, straight male rights to freedom of expression over everyone else's (i.e. over the global majority).

Despite the vast majority of participants (96%) of Glitch's workshops stating that post-workshop, they feel that they now have the skills to be safer and more resilient online, 69% of participants have told Glitch that they will continue to censor themselves online due to anxiety or fear of how others will respond. The perceived and/or actual threat of violence towards women and particularly Black

women, racialised women and minoritised women both online and offline is a behaviour of oppression that is part of and reinforces the systems of white superiority and patriarchy. It is no surprise then that women, who are disproportionately affected by online abuse, have their rights to freedom of expression compromised deliberately within the same power structures that we are subjected to offline.

The UK Government has stated that the Online Safety Bill will bring a stop to racist online abuse and tackle misogyny, yet it is unclear how it will achieve that in its current form. We are encouraged that intersectionality is in a sense included in section 21 6b (through "combined characteristics") of the Bill, though without a gendered lens, this does not go far enough and we are yet to understand how the UK Government intends to implement it in practice.

Currently, there is no provision in the draft Bill around anonymity. Following a lively debate on anonymity in the House of Commons earlier this year, we believe there is considerable political interest in anonymity in relation to online abuse and therefore find it unlikely that its inclusion will not be debated during the Bill's progress through parliament. Social media companies should enforce a zero-tolerance culture to online abuse to deter those creating accounts solely to abuse and sow discord. Sadly, many of the perpetrators of online abuse hide behind anonymous accounts.

While often discussed as a cause of online abuse, anonymity serves a legitimate purpose for those who do not abuse the privilege of being anonymous online. As many MPs expressed in the anonymity debate, anonymity can be an essential tool for whistle-blowers, activists and members of marginalised groups. Likewise, some people use anonymity to create content that is far from harmful. We do not advocate a total ban of anonymous accounts, though we believe that a balance needs to be struck between bad actors who use anonymous accounts to be abusive online and the rights of those abused online to control the content they see online. Anonymity should not impede the accountability and traceability of perpetrators of online abuse, particularly those perpetrating illegal harms, nor should regulation change damage the anonymity of legitimate good actors using pseudonyms online.

Due to the lack of consequences for poor online behaviour, there is a feeling of immunity afforded to those creating and using anonymous accounts online and people are emboldened to behave in ways they would not behave in public offline. Platforms which allow for anonymity (e.g. Twitter and YouTube) face high levels of online abuse. This suggests that these platforms need to review their processes to verify accounts better and put in place measures to protect their users from abuse and harassment from anonymous accounts, for example by putting in place filters and mechanisms that allow people to interact or only see content from verified accounts.

Anonymity should not be used as an excuse to not address the real issues at hand, including the need for digital citizenship education for people of all ages, that includes our online responsibilities but is also inclusive and progressive. While platforms differ when it comes to those that seemingly allow anonymity and those that do not, Twitter - considered a site that allows anonymous users - stated that following the football Euros final, it removed 1,622 tweets in the 24 hours after the final, and of the accounts that it permanently suspended, 99% of these users were 'not anonymous'. In a statement, Twitter deemed that identity verification, in this case, would have been unlikely to have prevented such abuse. Facebook has tried to eliminate anonymity on its site and our report, *The Ripple Effect* found that our survey participants experienced 27% of overall abuse on Facebook, compared to 65% on Twitter, suggesting that the ban on anonymity more widely would not stop online abuse.

Freedom of expression has become a smoke screen for perpetrators of online violence. Freedom of expression and online abuse are not in opposition with each other. Rather, ending and mitigating online abuse is an integral part of supporting freedom of expression of those that are frequently and disproportionately silenced online.

In our view, the current narrative around freedom of expression online has created a false trade-off between 'free speech' and online violence. Online abuse disproportionately affects women and in

particular Black women and other racialised women. Since we started our work at Glitch in 2017, we have documented the scale of abuse and online violence targeting women and girls in the UK, as well as marginalised communities and have seen how this abuse undermines free speech by attempting to silence marginalised communities and women and persons of colour who are involved in public life.

A major tension point is that as a global society, we have not drawn up the rules or social norms online for the line between political accountability and online abuse. While some offline perpetrators of abuse towards public figures cross the line of what is widely considered socially acceptable, the majority of people would not perpetuate this level of violence towards public figures in the offline world, partly because good bystanders would likely intervene, in addition to the in-built security provisions.

Social norms of this kind are less clear in the online space. In the UK's education systems, there is a deficit in political education, and curricula that are in dire need of being decolonised. We must teach young people about racism, sexism and other forms of systemic oppression, or we cannot expect good online digital citizens.

Q5: Are there any contested inclusions, tensions or contradictions in the draft Bill that need to be more carefully considered before the final Bill is put to Parliament?

There are campaigners who argue that the 'legal but harmful' provision should be removed from the Bill and that, for example, the racist abuse experienced by England's footballers after the Euro final that is not currently illegal should be criminalised. We do not support this belief. When talking about gender-based online abuse, the vast majority of online abuse against women falls into the 'legal but harmful' category. We believe that the removal of the 'legal but harmful' regulations in the Bill would weaken the legislation with regards to ending online violence against women.

We also advocate for digital citizenship education, aiming to change behaviour of individual internet users by upskilling them to understand that the online space is as real as the offline space. We do not wish to create a pipeline for perpetrators of online abuse to be given custodial sentences, particularly as we acknowledge that good online behaviour was never taught, and therefore the educational piece to encourage better behaviour online has not been widely delivered in the UK. We also support systemic changes to the way that platforms run their services, which currently reward, rather than punish online abuse.

Freedom of expression is not the freedom to abuse, or commit hate speech online or offline, and we should be careful about framing 'freedom of expression' and 'harassment' in opposition to one another. Without safeguards against harassment or hate speech, freedom of expression is undermined, and diverse political representation is stifled. We do recognise that there are difficult legal questions to answer in relation to, for example, what constitutes 'gross offensiveness' online but these questions should not distract from the problem at hand: the sheer scale of online abuse targeting women and girls, and marginalised communities in the UK and across the world.

While we believe that there is an opportunity to adopt the recommendations of the Law Commission's recent reviews on online harms and hate crime into the Bill, where appropriate, the advice of experts in the field should be heard to ensure that this is done in the most appropriate and effective way. For example, we support Professor Clare McGlynn's argument that the Law Commission's recommendation regarding image-based abuse should not focus on the motivation of the perpetrator to cause harm, but rather recognise the threat and invasion of privacy for the victim.

It is imperative that the Online Safety Bill is appropriately aligned with the Home Office's Tackling Violence Against Women Strategy and also works alongside the UK Government's commitments to the ratification of the Istanbul Convention and the Convention on the Elimination of all forms of Discrimination Against Women (CEDAW).

Q6: What are the lessons that the Government should learn when directly comparing the draft Bill to existing and proposed legislation around the world?

After twenty years of platform self-regulation, this is an important moment in global internet policies. When considering the global legislative landscape around online abuse, it is important to consider both good and promising practices as well as bad practices, to learn to create strong legislation. As the Digital Services Act is being developed at a similar time as the Online Safety Bill, there is an opportunity for the UK Government to benefit from the current and future debates around the Digital Services Act, and vice versa. There have also been strong calls in 2021 for further interventions at an EU level to combat gender-based violence/cyber violence.

While several countries have passed legalisation in this area already, some legislative developments abandon a gender-neutral stance by acknowledging that women are disproportionately affected by online abuse and that online abuse is part of a continuum of violence against women that it is in the best interest of the State to mitigate, minimise and work towards ending. For example, the e-Safety Commission in Australia is the world's first government agency committed to keeping its citizens safer online, and has a programme - Women in the Spotlight - to specifically elevate and protect women's voices online. The Commission is also becoming increasingly intersectional in its approach, with 'diverse groups' recognised as part of at-risk groups online, i.e. Aboriginal and Torres Strait Islander people; culturally and linguistically diverse people; people living with disabilities; lesbian, gay, bi, trans, intersex and queer people; as well as women, older Australians, children and young people.

There are also existing frameworks and conventions the UK Government has signed up to and could utilise to strengthen this policy area. For example, now that the Domestic Abuse Act has passed, we urge the UK Government to ratify the Istanbul Convention, as well as incorporating the Convention on the Elimination of All Forms of Discrimination against Women into domestic law. While the UK Government has signed up to both of these important frameworks, the lack of implementation to date has meant that less progress has been made in terms of ending violence against women and discrimination against women than if these were fully ratified and fully incorporated into UK law.

We also believe that the recommendations of the Law Commission with regards to hate crime and online violence against women and marginalised people should be included in the Online Safety Bill to ensure these policy recommendations are legislated as soon as possible, with advice from experts in each specific field.