Written evidence submitted by Refuge

Refuge evidence: Digital, Culture, Media and Sport Sub-Committee on Online Harms
and Disinformation: inquiry into online safety and online harms

About Refuge

1. Refuge is the largest specialist provider of gender-based violence services in the country supporting over 7,000 women and children on any given day. Refuge opened the world's first refuge in 1971 in Chiswick, and 50 years later, provides: a national network of 48 refuges, community outreach services, child support services, and acts as independent advocates for those experiencing domestic, sexual, and other gender-based violence. We also run specialist services for survivors of modern slavery, 'honour'-based violence, tech abuse and female genital mutilation. Refuge provides the National Domestic Abuse Helpline which receives hundreds of calls and contacts a day across the Helpline and associated platforms.

Summary

2. Refuge welcomes the opportunity to submit evidence to this inquiry. The Online Safety Bill is a vital opportunity to tackle online domestic abuse – otherwise known as tech abuse – and other forms of online violence against women and girls (VAWG). Domestic abuse takes and ruins lives, affecting more than one in four women (27.6%) aged 16-74 at some point in their lives.[1] Technology is increasingly being weaponised by perpetrators to coerce, control and abuse survivors of domestic abuse, providing perpetrators with ever-growing methods to abuse women. This form of abuse can include:
    - Online harassment
    - Stalking
    - Monitoring, surveillance and spyware
    - Online impersonation, for example creating fake social media accounts posing as the survivor or to contact the survivor
    - Having accounts hacked or controlled
    - Non-consensual intimate image or video sharing,[2] and threats to share intimate images or videos
    - "Doxing" – putting someone's personal details online
    - Tracking apps and devices, for example installed in cars, phones and children's toys

[1] ONS (2020), 'Domestic abuse prevalence and trends, England and Wales: year ending March 2020,' https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/domesticabuseprevalenceandtrendsenglandandwales/yearendingmarch2020

[2] This is also known as so-called "revenge porn" but Refuge does not endorse the use of this term as this implies some wrongdoing on the survivor's part. It also implies the sharing of such images or videos has been done for the purposes of sexual gratification, when frequently this is not the case and the purpose is to coerce, control and humiliate the survivor.

3. Tech abuse perpetrated on online platforms is particularly prevalent, with over a third (34.8%) of issues reported to Refuge's specialist tech abuse team between January 2020 and March 2021 relating to social media. Tech abuse frequently forms part of a pattern of coercive and controlling behaviour and is closely linked to physical, psychological, sexual and economic abuse - 83% of women who experienced threats to share intimate images or videos by their partners or ex-partners also experienced other forms of domestic abuse.[3] Survivors tell us of the significant and often-long term impact of tech abuse on their mental health and physical safety, with many having little choice but to delete their accounts or come offline entirely due to the failures of online platforms to respond to reports of harmful content. This further compounds the isolation and trauma of the tech abuse, shutting women out of online spaces, and for women whose income relies on being online, for example if they own an online business, they are often left suffering financially.

4. Refuge has a dedicated team comprised of specially trained staff that support and empower survivors experiencing tech abuse. The tech abuse team was formed in 2018 in response to the growing threat and devastating impact of tech abuse on survivors, including children. Between April 2020 and May 2021 there has been an average 97% increase in the number of complex tech abuse cases requiring specialist support from Refuge's tech abuse team when compared to the first three months of 2020. The current response from online platforms and the criminal justice system to victims of tech abuse is extremely poor, often leaving survivors with no recourse to protection or justice and effectively enabling perpetrators to continue abuse with impunity. Urgent action is required to safeguard women and girls' safety online and ensure their rights are safeguarded. Refuge welcomes the government's plans to introduce a regulatory framework and duties of care for user-to-user internet services in the Online Safety Bill, but argue that insufficient attention has been paid in the draft Bill to the ways in which such platforms and services are being used to perpetrate tech abuse and other forms of online VAWG. **It is vital the government safeguards women and children from online harms by explicitly recognising, on the face of the Bill, online VAWG as a specific online harm and requiring the regulator to produce a corresponding VAWG code of practice as a matter of urgency, to ensure technology companies and the regulator prioritise the prevention and tackling of these harms.**

5. Tech abuse is not solely limited to online platforms – it can include 'smart' internet-connected devices such as 'smart' doorbells and alarms, cloud-based storage systems, WiFi, cameras and other audiovisual recording devices, and a wide range of increasingly inexpensive and easily accessible tech products. We want to use this opportunity to highlight to the Committee the additional dangers poorly regulated technologies pose to survivors and the upcoming opportunities the government have to protect women from these potential harms, such as the Product Security and Telecommunications Infrastructure Bill which aims to regulate the security of smart products.

---

[3] Refuge (2020), 'The Naked Threat,' https://www.refuge.org.uk/wp-content/uploads/2020/07/The-Naked-Threat-Report.pdf

6. As the largest specialist provider of support services for survivors of domestic abuse and other forms of violence against women and girls, Refuge is in a unique position to represent the views and experiences of survivors. All our positions are developed in collaboration with survivors and our frontline staff. We are currently formulating detailed policy recommendations relating to the Bill and associated codes of practice and would be pleased to share these with the committee at a later date, in the Autumn. At this stage, Refuge makes the following recommendations for the Online Safety Bill:

- **Online VAWG should be explicitly named and recognised on the face of the Bill and given a much more central role**
- **Parliament should require the regulator to draw up a specific code of practice on online VAWG, in consultation with specialist VAWG organisations**
- **The regulator should include recommendations for optimal reporting processes within a VAWG code of practice, in consultation with specialist VAWG organisations**
- **The definition of harm, content that is harmful to adults and content that is harmful to children within the Bill should be expansive enough to include the harms of domestic abuse, including economic harms, which is currently explicitly excluded, and other forms of VAWG**
- **Government should consult with the specialist VAWG sector on the definitions and processes for determining harm**
- **Duties relating to adult's online safety should be more carefully considered and strengthened to align with those on children's safety and illegal content. For example, the duty of care for providers to use systems and processes to minimise illegal content and prevent children from encountering harmful content should be extended to content that is harmful to adults, particularly those experiencing online VAWG**
- **Government and the regulator should work to increase the extent to which companies must consider how their products can be used to perpetrate tech abuse and design this out as far as possible**
- **Tech companies should routinely develop guidance for users experiencing tech abuse setting out actions they can take, which minimises the burden on survivors themselves to keep themselves safe online**
- **Online platforms should be required to work together to prevent perpetrators of tech abuse switching platforms with ease**
- **Technology companies should be required by the regulator to compile and publish annual transparency reports on online harm perpetrated on their platforms and the companies' response to it. This should include reporting on online VAWG and the data should be disaggregated by sex and other protected characteristics.**
- **Government and the regulator to raise awareness of tech abuse via public campaigns and guidance for regulated services**
- **The regulator should develop an appeals mechanism for individual users to bring a complaint when they have exhausted a platform's reporting process**

- **The regulator should have a full range of enforcement powers, including the ability to hold senior management criminally liable from the outset of their role as regulator and to impose take-down notices**
- **The regulator should be independent and allocated sufficient resources to effectively conduct its functions as regulator**
- **Domestic Homicide Reviews should be empowered to make recommendations to technology companies, where relevant, and notify the regulator where tech abuse factors in a domestic homicide and there is concern that technology companies could or should have acted differently**
- **Government should accept, and legislate for, the Law Commission's proposal for a new "harm-based" communications offence to replace the offences within section 127(1) of the Communications Act 2003 and the Malicious Communications Act 1988**
- **Clarity should be provided on the inclusion of platforms and platform features such as one-to-one "voice notes"**

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

Explicit inclusion of VAWG

7. Whilst the Online Harms White Paper made some, albeit limited, references to online VAWG, such as to 'coercive behaviour,' at present there are no references to violence against women and girls in the draft Bill at all. This is of great concern, as without specific reference to domestic abuse and other forms of VAWG the Bill is likely to fail to ensure online platforms pay due attention to these online harms by preventing tech abuse and other online VAWG as much as possible, protecting survivors and holding perpetrators to account. If VAWG is not explicitly included as an online harm on the face of the Bill, while other forms of online harm are (i.e. child sexual exploitation and terrorism), then the regulator will likely not prioritise producing a code of practice for online VAWG and tech abuse, setting out clear expectations and processes for online platforms when it comes to this form of abuse. This will leave survivors having to navigate reporting processes and procedures which are not built with their needs or experiences in mind. In order to fall within the Bill's current remit and the proposed regulatory framework, individual instances of tech abuse would therefore need to be shown to be either illegal content, content that is harmful to children or content that is harmful to adults. Many instances of tech abuse are not clearly unlawful, meaning that survivors would need to demonstrate to platforms that the abuse is harmful to them (an adult), or that the content is illegal, for example as part of a pattern of coercive and controlling behaviour. Given the widespread lack of understanding of the nature and impact of domestic abuse and coercive control in general, let alone tech abuse, this situation is unlikely to lead to the protection that survivors should be entitled to as the decision on whether content is harmful, or even illegal, will be left largely to the platforms themselves to judge. As such, it is critical that online VAWG and tech abuse are included as an explicit harm on the face of the Bill.

8. While there are avenues, albeit poor and reliant on outdated legislation, for pursuing criminal charges for forms of tech abuse that amount to an offence, the routes to resolution through online platforms are arguably even more limited. In our experience social media companies and other online platforms have a limited understanding of domestic abuse and often do not comprehend the context specificity of such abuse when reported on their platforms. For example, harmful communications sent to women supported by Refuge's services have included perpetrators locating survivors after they have fled to a refuge or other secret location and sending them an image of their front door or road name. Whilst a photo of a front door would not be considered harmful in many contexts, this content was clearly sent with the intent to cause distress and fear, and is incredibly harmful to a survivor, both psychologically and physically. These examples would likely not be judged as harmful or in breach of online platforms' community standards without an understanding of the history of domestic abuse and context of coercive control. For instance, a survivor supported by Refuge was stalked online by her ex-partner and his friends and contacted by fake accounts. When she reported this to Facebook they deemed there to be nothing wrong with this behaviour. These failings in content reporting and moderation processes leave women with limited recourse to justice and protection and effectively permit perpetrators to continue the abuse.

9. Many reporting functions are currently not fit for purpose when reporting tech abuse and other online VAWG and feature checkbox-only systems to explain why content is harmful; these checkboxes rarely include options which adequately describe experiencing tech abuse or other forms of online VAWG. A common experience for survivors is to receive dozens or hundreds of abusive, harassing images or communications from a perpetrator via social media. Due to the limitations of current reporting processes, survivors must report each individual piece of content in turn, which is both time-consuming and re-traumatising. For instance, one survivor supported by Refuge experienced online stalking by the perpetrator, his friends and new partners. She was forced to search her ex-partner's profile to find the profiles of these people and then block them individually herself.

10. In addition, social media companies often take weeks to respond to reports of harmful content, and frequently do not respond to reports at all. From our experience working with survivors of tech abuse, the speed at which action is taken to respond to or to remove reported content is a key priority for survivors. When platforms do respond, this at best results in the removal of content rather than more effective steps to prevent online harms, such as the banning of a perpetrator from a platform. A survivor recently told us about her experience of receiving threats on Snapchat: *"When I was pregnant I was getting threats about my child, and that people would kick my child out of me. A lot of (the messages) were fake accounts – 43, so it was 43 accounts. I reported it to Snapchat; well I haven't heard anything back to be honest. I reported three times. I also reported it*

to the police because it became too much. Their advice was to get rid of social media." Refuge's specialist tech team have "trusted flagger" status with many social media sites. In theory this should result in a more rapid response to reports of harmful content and review by human moderators. The reality is the team face lengthy waits for replies – for example, Facebook and Instagram stated they would respond within 48 hours to reports, yet the team frequently find their reports are not responded to for 4-6 weeks before they are then acknowledged. This leaves the survivor open to continued abuse from their perpetrator, with content remaining live for many weeks if not months. Both the criminal justice system and online platforms are failing to sufficiently support and respond to survivors of tech abuse. Therefore, it is vital that online VAWG is explicitly recognised on the face of the Online Safety Bill to ensure online platforms are compelled to prioritise its prevention and response.

Definitions of harm and content that is harmful to adults and children

11. The current definitions in the draft Bill of harm, content that is harmful to adults and content that is harmful to children are insufficient and require a number of improvements, as set out below.

12. Harm is defined in the draft Bill as meaning "physical or psychological harm," or in reference to content that is harmful to children and adults, as content which has a "significant adverse physical or psychological impact." Whilst Refuge supports the inclusion of physical and psychological harms in this proposed definition, the definition specifically excludes harms that flow from the financial impact of the content, which risks excluding some forms of economic abuse. Economic abuse is a common form of domestic abuse which involves a perpetrator restricting a survivor's ability to acquire, use and maintain money or other economic resources. Research by Refuge and The Co-Operative Bank revealed 39% of UK adults had experienced behaviours which suggest they had experienced economic abuse.[4] Survivors supported by Refuge have reported perpetrators targeting their online businesses through their business social media accounts. In one instance, after a survivor had a book published, the perpetrator contacted her publisher and posted malicious lies about her on their public social media pages which had potentially damaging consequences on her income. The exclusion of economic harms from the definition of harm will therefore leave significant gaps in the Bill. We recommend that financial harms are not excluded from the definition of harm or content that is harmful to children and adults, particularly in the context of domestic abuse and other online VAWG.

13. The definition of "content that is harmful to adults" outlined in section 46 of the draft Bill is additionally problematic for a number of reasons:
    - Vague concepts are used within the definition, such as the "reasonable grounds" the service provider must have to believe there is a material risk of the content having an adverse impact. No detail is provided on the definition

[4] Refuge and The Co-Operative Bank (2020), 'Know Economic Abuse,' https://www.refuge.org.uk/wp-content/uploads/2020/10/KnowEconomic-Abuse-Report-2020.pdf

or threshold of reasonable grounds, nor the evidence a provider may have to show to demonstrate how reasonable grounds has been proven, or not.

- Further clarity is required on "priority content that is harmful to adults." The draft Bill states that the government will designate content as priority content at a later date, in consultation with the regulator, but it not clear on what basis content will be deemed as priority. This must be made clarified in the Bill to ensure transparency.
- In reference to the "significant adverse" impact content must have on an adult in order for it to fall within the scope of "content that is harmful to adults," it must be made clear that all domestic abuse has a significant adverse impact on victims. Domestic abuse has devastating consequences, such as to survivors' mental, emotional and physical health, to their social connections, financial situation and housing. For example, survivors of domestic abuse are up to three times as likely to develop mental illness as women who do not experience domestic abuse.[5] Any interpretations of "significant" impacts in the Bill must therefore reflect the serious impact domestic abuse has on survivors.
- The determination of whether content is harmful to adults at present is left to the judgement of the provider of the online platform, as set out in section 46 (3): "(c)ontent is within this subsection if the provider of the service has reasonable grounds to believe that the nature of the content is such that there is a material risk of the content having, or indirectly having, a significant adverse physical or psychological impact on an adult of ordinary sensibilities." This is particularly concerning because in Refuge's experience online platforms frequently do not understand the context of reported tech abuse, as outlined in paragraph 8. Leaving the judgement of risk solely in their hands is therefore a key flaw of this subsection, as it may lead to little change in the experiences of survivors reporting tech abuse to platforms. Given the widespread misunderstanding of domestic abuse, the harms of both domestic abuse and violence against women and girls should be explicitly included within the Bill.
- The inclusion of indirect harms in the definition of content that is harmful to adults and the element of subjectivity introduced within section 46 (6) into the test of an adult of "ordinary sensibilities" is to be welcomed. It is common for perpetrators of domestic abuse to contact the children, family or friends of a survivor, in order to cause harm and distress to the survivor. These indirect communications should rightly fall within the definition of harm. Some women are also disproportionately affected by domestic abuse due to their ethnicity, race, sexuality and / or other identities, and may also experience different forms of online harms. For example, Black and minoritised women are more likely to experience domestic abuse and disabled women are twice as likely to experience it.[6] It is therefore a positive step that the Bill allows for content to

[5] Chandan et al (2019), 'Female survivors of intimate partner violence and risk of depression, anxiety, and serious mental illness,' *The British Journal of Psychiatry*, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B33176643C1858B2D502E584D160F794/S0007125019001247a.pdf/female_survivors_of_intimate_partner_violence_and_risk_of_depression_anxiety_and_serious_mental_illness.pdf

be read by the service provider in "reference to that particular adult, taking into account any of the adult's characteristics." However, this provision should go further to specify that contextual readings of harm should also include online VAWG and the relationship between the perpetrator of abuse and the victim-survivor as this will help platforms identify tech abuse being perpetrated on their platforms.

14. Moreover, recognition of online VAWG on the face of the Bill would also strengthen protections for children, as well as adults. As per the Domestic Abuse Act 2021, children are legally recognised as victims of domestic abuse in their own right, as there is significant evidence that children living within a household where one partner or parent is abusing the other are harmed as a result of that abuse. On any given day, Refuge supports around 3,500 children across our services. Children exposed to domestic abuse are not simply witnesses - 97% of children living with domestic abuse are exposed to the abuse, 62% of these children were directly harmed, 58% were emotionally abused and 28% were physically harmed.[7] Where tech abuse is being perpetrated, whether or not it is directly aimed at the child or the mother, the child is still considered a victim in their own right of that abuse as they will likely experience indirect or direct harm as a result. For example, survivors whose online businesses have been targeted by perpetrators may be financially impacted by this and have reduced funds to care for the children. One of the most effective ways to protect children living with and experiencing domestic abuse is to improve protection for the survivor-parent, to ensure they are safe and free to live their lives and to raise their children. VAWG affects both children and adults, and the Online Safety Bill should reflect this by explicitly naming and recognising online VAWG in the Bill.

Illegal content

15. In relation to tackling illegal user-generated content, the draft Bill specifically refers to only two groups of offences – terrorism and child sexual exploitation and abuse. These appear to form the focus of the illegal content duties within the Bill, and will be the subject of dedicated codes of practice drawn up by the regulator. Refuge urges the government to also specifically include VAWG offences on the face of the Bill to help galvanise service providers to better address and prevent these crimes and oblige the regulator to draw up a specific code of practice as a matter of urgency. VAWG crimes are widespread and pervasive. 15% of all police recorded crimes were domestic-abuse related in the year ending March 2020, and the police receive a domestic-abuse related call every 30 seconds in England and Wales.[8] [9] A large proportion of tech abuse and online VAWG

---

[6] ONS (2020), 'Domestic abuse victim characteristics, England and Wales: year ending March 2020,' https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/domesticabusevictimcharacteristicsenglandandwales/yea rendingmarch2020#ethnicity

[7] SafeLives (2014), 'In plain sight: The evidence from children exposed to domestic abuse,' http://www.safelives.org.uk/sites/default/files/resources/In_plain_sight_the_evidence_from_children_exposed_to_domestic_abuse.pdf

[8] ONS (2020), 'Domestic abuse and the criminal justice system, England and Wales: November 2020'. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/domesticabuseandth

amount to criminal offences. In a Glitch and Ending Violence Against Women coalition (EVAW) survey of the online experiences of women and non-binary individuals in the UK during the pandemic, 20% of white respondents and 17% of Black and minoritised respondents reported stalking or stalking by proxy, whilst 21% of white respondents and 13% of Black and minoritised respondents experienced threats of physical or sexual violence.[10] These crimes are far too prevalent, and have a devastating impact on the victims. Yet they are often not understood by online platforms to be illegal behaviour. Refuge's tech abuse team frequently advocates on behalf of clients to explain to tech companies that behaviours experienced online by the survivor, such as harassment and coercive control, are illegal. As outlined in paragraphs 7-10, the explicit inclusion of online VAWG in the Bill, and the development of a specific code of practice, would help rectify some of these issues by ensuring platforms understand what is meant by tech abuse and other forms of online VAWG, the harm and impact of such behaviour, and where behaviour amounts to a criminal offence thereby prompting a stronger response from platforms.

16. The government's recently published Tackling Violence Against Women and Girls strategy makes clear the ambition to ensure the safety of women and girls across the country, including in online spaces.[11] Whilst the strategy refers to the Online Safety Bill as part of the work the government is undertaking to this end, the strategy focuses on how the Bill will be particularly equipped to protect children from child sexual exploitation and abuse and gives no detail on how the Bill will be utilised to prevent online VAWG and protect survivors. This is unsurprising given the Bill fails to detail how it will specifically address violence against women and girls. However, it does make clear that omitting VAWG from the Bill will be a missed opportunity to support the government's ambition to tackle online crimes and make online spaces for women and girls safer.

17. **Refuge recommends that:**

- **Online VAWG should be explicitly named and recognised on the face of the Bill and given a much more central role**
- **The definition of harm, content that is harmful to adults and content that is harmful to children within the Bill should be expansive enough to include the harms of domestic abuse, including economic harms, which is currently explicitly excluded, and other forms of VAWG**

---

ecriminaljusticesystemenglandandwales/november2020

[9] HMIC (2014), 'Everyone's business: Improving the police response to domestic abuse,' https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/2014/04/improving-the-police-response-to-domestic-abuse.pdf

[10] Glitch UK and End Violence Against Women Coalition (2020), 'The Ripple Effect: COVID-19 and the Epidemic of Online Abuse,' https://www.endviolenceagainstwomen.org.uk/wp-content/uploads/Glitch-and-EVAW-The-Ripple-Effect-Online-abuse-during-COVID-19-Sept-2020.pdf

[11] HM Government (2021), 'Tackling Violence Against Women and Girls,' https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1005630/Tackling_Violence_Against_Women_and_Girls_Strategy-July_2021-FINAL.pdf

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?

18. VAWG should be named as a specific online harm in the Online Safety Bill and given a much more prominent role in the Bill. For further detail on this, please refer to paragraphs 7-10 and 28-31. Domestic abuse and coercive and controlling behaviour both have statutory definitions which may be referred to within definitions of harm to children and adults, as set out in the Domestic Abuse Act 2021 and the Serious Crime Act 2015. The government should also consult with the specialist VAWG sector on the definitions and process for determining harm to children and adults in the Bill, as the contextual harms of domestic abuse must be understood and captured in any such process. As outlined in paragraph 8, online platforms often fail to comprehend tech abuse and deem instances of online VAWG as not in violation of their community standards. Building a better understanding of VAWG into the Bill will help tech companies to better discharge their responsibilities to women and girls using their platforms and products.

19. A dedicated code of practice for VAWG should also be developed by the regulator, in collaboration with the specialist VAWG sector, in order to ensure online platforms take appropriate steps to improve their response to such online harms. The Bill must be amended to prioritise the production of this code of practice, in line with the priority status given to child sexual exploitation and abuse and terrorism. For further detail on Refuge's recommendations for standards to be included in a VAWG code of practice, please see paragraphs 32-33.

20. Without urgent improvements to reporting functions and processes for determining harm, online VAWG will continue to proliferate. Women are already being forced to minimise their presence online, or come offline entirely, thereby reducing their ability to participate in society and perform day-to-day tasks. This is particularly isolating as we conduct more and more of our lives online. Over half (53%) of women supported by Refuge's tech abuse team between July 2020 and March 2021 said the tech abuse had left them feeling unsafe online. One survivor Refuge supported detailed the impact of her former partner monitoring her use of social media, and posting false information and images of her child online as part of a pattern of coercive control and emotional abuse: *"I reported to Facebook saying this is not appropriate and they came back to me saying there is nothing inappropriate there. So from there I used Facebook to the minimum. Zero personal information in my Facebook, I feel restricted about that. I used to be a very positive outgoing person, now I feel like a person who wants to be very invisible. I don't want to share anything. It really makes me emotional too, that's I would say trauma. On top of that they (the perpetrator) can get away with that – it's incredible."*

21. **Refuge recommends that:**

- **Online VAWG is explicitly included on the face of the Bill**

- **Government should consult with the specialist VAWG sector on the definitions and processes for determining harm**
- **Parliament should require the regulator to draw up a specific code of practice on online VAWG, in consultation with specialist VAWG organisations**

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?

22. The Bill should focus much more on safety by design. Safety by design is crucial to reducing the risk of harm to victims of domestic abuse. A better understanding of the potential risks that products present to survivors could lead to the development of safer, more secure products that have their safety in mind. The draft Bill currently places a duty on providers to operate their services "using proportionate systems and processes" designed to minimise the presence of illegal content and to prevent children from encountering harmful content. The same duty must be extended to content that is harmful to adults, specifically those that are experiencing tech abuse being perpetrated on these platforms. The duties of care relating to adults' online safety and safety by design are currently far weaker than those for children's safety and illegal content, only requiring platforms to undertake risk assessments which include examining how the design and operation of the service may reduce or increase risk of harm. Refuge argues that a responsibility should be placed on companies making design choices which would allow or inadvertently encourage online harms to be perpetrated, particularly for products which enable anonymous or untraceable communications. For example, dating apps are almost entirely unregulated and are frequently used to abuse women online; women are also encouraged to meet offline, where the risk of harm escalates. The company benefiting from the profits of a product that, at least in certain circumstances, facilitates VAWG, has a responsibility to its users and should have a duty to appropriately respond and prevent it from occurring in the first place. Both government and the regulator should work to increase the extent to which companies must consider how their products can be used to perpetrate tech abuse and design safer features and functionalities.

23. Service providers should also be required to cooperate with one another to more effectively prevent abuse from escalating. It is very easy for perpetrators to move from one platform or app to another to continue abuse. Refuge supported a client who had experienced abuse on Facebook, Instagram and WhatsApp to report that abuse. Despite Facebook owning all three platforms, the company requested the survivor file new reports with each platform in turn and refused to discuss the WhatsApp issue with her. Another survivor who was stalked and harassed by a man she met on a dating app was able to secure a stalking prevention order against the perpetrator. However, she is unsure whether the perpetrator has been blocked from the dating app, or whether the company has shared details of the perpetrator's behaviour with other dating apps to prevent him targeting other

women. Collaboration among tech companies could help hold perpetrators to account for the abuse, including when perpetrated across a number of platforms, and therefore prevent the perpetrator from causing further harm. The government should consider using the Online Safety Bill to place a duty on services to work together to prevent perpetrators of tech abuse switching platforms with ease.

24. Refuge suggests that platforms should invest in human moderators as part of their reporting processes. Staff trained in online VAWG and in providing holistic support to users experiencing online abuse would be better able to recognise tech abuse and the contextual elements of harm than an algorithmic process. This would lead to more appropriate actions being taken by platforms when they identify tech abuse or when responding to a report from a user. Investment in technologies which enable the online platform to recognise when one user has set up multiple accounts, such as by identifying where one IP address has been used to create numerous accounts, may also be useful. This could help prevent the creation of new and fake accounts with ease to perpetrate abuse.

25. Tech companies should be encouraged to routinely develop user guidance which clearly sets out actions that can be taken if their products are being used to harm or abuse users. Refuge has developed resources to provide women with support in securing their devices and using technology safely and has recently launched a new tech safety website (refugetechsafety.org). These resources include a series of step-by-step support guides for a range of devices and social media platforms, and an interactive chatbot with video guides in multiple languages. Given the vast resources available to many social media platforms, these platforms should be able to develop similar resources for their users.

26. One of the most urgent improvements needed to online platform design is to reporting systems and processes. A dedicated VAWG code of practice should include recommended standards for optimal reporting processes for platforms which recognises the specific circumstances survivors are often in, ensuring a survivor needs-led response which does not place a disproportionate burden on the survivor. For further detail on Refuge's recommendations on standards for reporting systems, please see paragraphs 32-33 in our response to the following question on key omissions to the draft Bill.

27. **Refuge recommends that:**

- **Government and the regulator should work to increase the extent to which companies must consider how their products can be used to perpetrate tech abuse and design this out as far as possible**
- **The duty of care for providers to use systems and processes to minimise illegal content and prevent children from encountering harmful content should be extended to content that is harmful to adults, particularly those experiencing online VAWG**
- **Tech companies should routinely develop guidance for users experiencing tech abuse setting out actions they can take, which**

minimises the burden on survivors themselves to keep themselves safe online

- **Online platforms should be required to work together to prevent perpetrators of tech abuse switching platforms with ease**
- **The regulator should include recommendations for optimal reporting processes within a VAWG code of practice, in consultation with specialist VAWG organisations**

<u>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?</u>

Explicit inclusion of VAWG

28. The key and glaring omission to the draft Bill is its failure to include specific provisions relating to violence against women and girls occurring in online spaces. No reference is made to women, domestic abuse, or any other form of VAWG in the draft Bill. This is despite the government highlighting the Online Safety Bill as the key mechanism for ensuring women and girls are safe online in the recently published Tackling VAWG Strategy. It is critical that online VAWG is included in the Bill as a key focus for tech companies to address, alongside a requirement on the regulator to develop a code of practice, in consultation with the VAWG specialist sector, setting out steps for companies to comply with regarding tech abuse perpetrated on their platforms. Refuge supports the importance placed upon tackling child sexual exploitation and abuse and terrorism in the draft Bill, and argues that the prevalence and impact of online VAWG, and the current failure of platforms to adequately respond to these harms, warrants a similar level of prioritization. According to the Crime Survey of England and Wales more than one in four women in England and Wales aged 16-74 experience domestic abuse at some point in their lives, and an average of two women are killed every week by their partner or ex-partner – a statistic which has not changed in decades.[12] [13] In Refuge's experience domestic abuse is increasingly involving technology. This trend is likely to continue as more sophisticated platforms are developed and cheaper devices come to market. During the first national lockdown for COVID-19, the number of clients supported by Refuge's specialist tech team rose by 46%, compared to the three months before that (April – June 2020 compared to January – March 2020). A survey by Glitch and EVAW found that approximately 46% of women had experienced online abuse since March 2020, with most of the abuse taking place on mainstream social media platforms.[14] The women Refuge supports who have

[12] ONS (2020), 'Domestic abuse prevalence and trends, England and Wales: year ending March 2020.' https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/homicideinenglandandwales/latest#how-werevictims-and-suspects-related

[13] ONS (2020), 'Homicide in England and Wales: year ending March 2019'. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/homicideinenglandandwales/latest#how-werevictims-and-suspects-related

[14] Glitch UK and End Violence Against Women Coalition (2020), 'The Ripple Effect: COVID-19 and

experienced tech abuse tell us of its devastating impact on their mental health and safety. 19% of the clients supported by the tech abuse team between July 2020 and March 2021 said that their location had been compromised as a result of that abuse, and 30% said the impact of the abuse had left them unable to use their devices, isolating them from their family, friends and supportive networks at a time of crisis. The damaging impacts of tech abuse, and its increasing prevalence, must be reflected in the Bill by explicit reference to online VAWG. A survivor supported by Refuge spoke about the impact of online harassment, threats and non-consensual sharing of intimate images by a partner: *"Even when I was in a refuge he was still using technology, manipulating me through social media, threatening to go where I live and threatening to hurt me. Obviously it impacts me a lot; it's very traumatising, because it just shows how controlling and obsessive these abusers are. It puts me off going on my phone. It's just too much to deal with; it impacts my mental health a lot. I don't want to put up with using social media anymore. I still have to go on it sometimes because I have to stay in contact with my family."*

29. Online VAWG also has significant repercussions on women's access to the internet. The general public spends an increasing amount of time online, reaching record levels during the height of the pandemic when UK adults spent more than a quarter of their waking day online.[15] We are becoming ever more reliant on the internet to live our daily lives, for example to access bank accounts, order food deliveries and book and attend medical appointments. Yet survivors of tech abuse are being forced to minimize their participation in online life, owing to the failures of online platforms to adequately respond to tech abuse. Refuge works to help empower women experiencing tech abuse and to ensure they do not have to censor themselves online, but undeniably the scale and pervasiveness of tech abuse is silencing women.

30. The criminal justice system too contributes to these failures, by placing the onus on survivors to change their behaviour, with police officers frequently recommending survivors come offline, rather than focusing on pursuing perpetrators of online offences. This has implications for survivors' rights to freedom of expression as they minimise their participation in online public life, as well as many other consequences such as limiting their ability to perform day-to-day online tasks. Almost one in five women who had experienced threats to share intimate images or videos left the house less and/or used social media less as a result of the threats.[16] Research by Plan International has found that 43% of girls admitted holding back their opinions on social media for fear of being criticised, and research by Glitch and EVAW also revealed that after facing online abuse, 48% of Black and minoritised respondents and 41% of white respondents reported spending less time online.[17] [18] The focus of government efforts in this

---

the Epidemic of Online Abuse,' https://www.endviolenceagainstwomen.org.uk/wp-content/uploads/Glitch-and-EVAW-The-Ripple-Effect-Online-abuse-during-COVID-19-Sept-2020.pdf

[15] Ofcom (2020), 'Online Nation 2021 report,' https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2020/uk-internet-use-surges

[16] Refuge (2020), 'The Naked Threat.'

[17] "Almost half of girls aged 11-18 have experienced harassment or bullying online," Plan International, 14 August 2017, https://plan-uk.org/media-centre/almost-half-of-girls-aged-11-18-have-

area should be on holding perpetrators of tech abuse and other forms of online VAWG and the platforms which facilitate this abuse to account, rather than encouraging women to adapt their online behaviour in order to reduce the abuse perpetrated against them.

31. In response to arguments that the inclusion of legal but harmful content within the Bill represents a threat to freedom of expression, Refuge argues that a balance can be found and that the rights of women and girls, including to free expression, must be centred. To suggest that there is a zero-sum tradeoff between the right to free expression and increasing the safety of women and girls online by ensuring online VAWG is adequately prioritised is a false dichotomy, and one that entirely ignores the right to free expression of women and girls in this country. We support the retention of legal harmful content within the Bill in order for women and girls to be free from harassment and abuse in online spaces, and exercise their rights to freedom of expression.

VAWG code of practice

32. A further omission from the draft Bill is the requirement for the regulator to draw up a specific code of practice on online VAWG, in consultation with specialist organisations. This should be a matter of priority for the regulator given tech abuse's prevalence and impact as detailed in previous sections. On any given day Refuge supports over 7,000 women and children and in our experience social media companies are failing to respond to, or even acknowledge, reports of online harms, as outlined in paragraphs 7-10. Reporting mechanisms need to be as efficient and speedy as possible, and should be able to take into account the context of reported abuse, rather than simply taking content at face value. A system whereby victims of online abuse can provide the profile name or a link to the account of their abuser would also be more efficient, trauma-informed and user-focused than current systems which require users to report individual pieces of content.

33. The current duties of care in the draft Bill for services to use systems and processes for users to easily report content which they consider to be illegal, or harmful to children or adults, and to operate a transparent complaints procedure which is easy to access and use, are welcome. A specific VAWG code of practice must make clear, however, that reporting systems must meet a minimum set of standards regarding the following issues:
    - Requirements to make the reporting procedure as quick and efficient as possible, which includes ensuring survivors are not required to report every single abusive piece of content
    - Details on the speed at which the platform responds to reports of harmful content, which must reflect the seriousness of online VAWG

---

experienced-harassment-or-bullying-online

[18] Glitch UK and End Violence Against Women Coalition (2020), 'The Ripple Effect: COVID-19 and the Epidemic of Online Abuse.'

- Requirements for platforms to have clear policies and procedures to deal with threats to inflict harm
- Requirements to provide law enforcement with the specific data they require to investigate and prosecute perpetrators – there are currently barriers to obtaining relevant evidence from social media platforms of tech abuse perpetrated on their sites
- Platforms to set up systems which can take into account the context of reporting abuse when responding to reports
- Duties regarding cooperation with other platforms to ensure that perpetrators can be more easily identified and removed from platforms

Access to specialist support services

34. Refuge is unique in having a dedicated tech abuse team, and the team has provided holistic support to thousands of women, which results in improved outcomes for survivors. The level of advocacy and specialist knowledge required to support clients is substantial, often requiring weeks of work to elicit responses from social media companies or the police. In addition, the team has to build relationships with social media platforms in order to develop "trusted flagger" status which theoretically allows them access to speedier reporting processes, but which in practice still requires lengthy waits before action is taken. Specialist VAWG organisations are severely underfunded and face an insecure funding landscape and historic funding cuts. Since 2011, Refuge has experienced cuts to 80% of its services. In order to ensure survivors of tech abuse and other forms of online VAWG have access to the specialist, independent support they need, financial provision for support must be guaranteed in the Bill. A funding package for victims of online VAWG should be launched alongside the Bill. This could be achieved by allocating 5% of any fines levied by the regulator to funding support services, with 50% of this amount specifically ring-fenced for specialist 'by and for' led services supporting Black and minoritised women and girls, as suggested by the Joint VAWG Sector submission to the Committee.

Annual reporting and data collection

35. The Bill requires online platforms to produce annual transparency reports on the incidence of illegal and harmful content, the reporting systems available to users and the steps that the platform has taken to comply with duties of care, as well as other information requested by the regulator. As part of the annual reporting process, companies should be required to specifically report on steps they have taken to reduce online VAWG and also to provide data on the types of online harms perpetrated on their platforms. This data should be disaggregated for sex, ethnicity, age and other protected characteristics, as well as the relationship between the victim and perpetrator of the abuse, where known. The collection of this data would help highlight flaws in reporting systems, allowing the regulator to act where there is consistent poor practice, as well as helping the regulator to identify any new emerging harms. All transparency reports should be made publicly available. The regulator should also be required to undertake research with users of online platforms who have experienced online VAWG in order to

understand their experiences and make recommendations to platforms on how to improve practice.

Role of the regulator

36. Refuge also recommends that the Bill should set out further roles for the government and the regulator in raising awareness of tech abuse. The regulator will be well placed to provide information and guidance to regulated services about the ways in which products can be used to perpetrate VAWG, and the impact this has on survivors. The government should also play a role in funding and launching public awareness raising campaigns. The focus of such campaigns should be on communicating that perpetrating online harms is unacceptable and is in many cases a criminal offence, rather than on how victims of tech abuse should change their behaviour for their safety. The campaigns should also encourage the public to report online harms or crimes they witness. Caution will be required with campaign messaging so as not to inadvertently educate perpetrators on new methods to abuse. The government should always develop such campaigns in partnership with specialist VAWG organisations.

37. An additional omission from the draft Bill relates to an appeals mechanism for individual users. Whilst the inclusion of a super-complaints procedure is to be welcomed, as this could enable specialist organisations such as Refuge (if accepted as a designated body) to challenge systemic problems not being dealt with by platforms and help complement the regulator's work, there is a clear need for a system for individual victims of tech abuse to seek redress. A mechanism should be developed for survivors to bring a complaint to the regulator as an individual when they have exhausted a platform's reporting process. The draft Bill currently allows tech companies to appeal the regulator's decisions (see sections 104-105 of the Bill) and for users to report their concerns to the regulator, but the regulator will not investigate individual cases of alleged non-compliance. This leaves a huge gap in enforceability. As mentioned elsewhere in this submission, many online platforms are frequently failing to investigate and respond to reports of harmful content, leaving victims with little recourse to justice. A system for individual users to seek redress via the regulator should be established. In addition, the regulator should have the power and resources to proactively investigate systemic issues, rather than being reliant on receiving a super-compliant to take action. The super-complaints process will also be more effective if the Bill explicitly names VAWG as an online harm, and if complaints can be brought against single providers regardless of their user base.

Policing and criminal justice

38. Many forms of tech abuse amount to a criminal offence, including harassment, coercive and controlling behaviour, stalking, the non-consensual sharing of intimate images/videos, and threats to share such images/videos, which has recently been criminalised in the Domestic Abuse Act 2021 following a Refuge campaign. However, too often there are failures by the police and Crown Prosecution Service to investigate and charge these crimes. Countless reports

and reviews by independent inspectorates and by law enforcement agencies themselves have illustrated the systemic failures of the criminal justice system to protect women and girls.[19] In England and Wales, from the year ending March 2015 to the year ending March 2020, referrals from the police to the CPS for domestic abuse-related crimes fell by 40%, and convictions fell by 37% from 2016 to 2020.[20] In Refuge's experience, the police and criminal justice system handle the online "versions" of these crimes even more poorly. Survivors tell us they have been advised by the police to come offline as a solution to the abuse. It is unacceptable that the policing response to online abuse of women and girls is for the victims to remove themselves from these online spaces, rather than pursuing the perpetrators. This not only serves to further isolate survivors, but also risks escalating the abuse, as perpetrators move to pursuing "in person" forms of abuse because perpetrating online abuse is no longer an option.

39. The recent Law Commission review of the criminal law governing harmful communications, namely the Malicious Communications Act 1988 and the Communications Act 2003, found that legislation had not kept pace with technological changes, was ambiguous and unclear, and that the criminality threshold is often set too low when applied to online spaces.[21] Refuge strongly supports the Commission's proposal for a new "harm-based" communications offence and urges the government to adopt this proposal. We suggest the Online Safety Bill may be a suitable legislative vehicle to do so.

40. Tech abuse is closely connected to women's safety. Refuge has been involved in the quality assurance of Domestic Homicide Reviews (DHRs) for around a decade, and frequently sees tech abuse raised in these reviews. DHRs are multi-agency investigations of the circumstances of domestic homicides of persons aged 16 and over whose death has, or appears to have, resulted from the abuse of an intimate partner or family member. The reviews make recommendations to agencies and public bodies in order to deliver improvements to the safeguarding of victims and to prevent future domestic homicides. Where tech abuse has played a role in a domestic homicide, DHRs should be able to make recommendations to the police and other statutory services and agencies, as well as technology companies where their platform or product has factored in the homicide. The regulator must also be notified where there is concern that online platforms could or should have acted differently, in order to support their

---

[19] For example, see: College of Policing, Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) and Independent Office for Police Conduct (20211), 'A duty to protect: Police use of protective measures in cases involving violence against women and girls,' and HMICFRS (2021), 'Interim report: Inspection into how effectively the police engage with women and girls'

[20] Calculated using CPS (2020), 'CPS data summary Quarter 4 2019-2020,' https://www.cps.gov.uk/publication/cps-data-summary-quarter-4-2019-2020 and the data published alongside the CPS VAWG Report 2018-19, available for download here: https://www.cps.gov.uk/cps/news/annual-violence-against-women-and-girls-report-published-0

[21] Law Commission (2021), 'Modernising Communications Offences,' https://www.lawcom.gov.uk/project/reform-of-the-communications-offences/

monitoring of services and role as regulator. Learnings should also feed into the codes of practice and duties of care placed on social media companies in the Bill to help improve practice where their platforms have played a role in a domestic homicide.

41. **Refuge recommends that:**

- **Online VAWG as a specific online harm should be explicitly named and given a much more central role in the Online Safety Bill**
- **Parliament should require the regulator to draw up a specific code of practice on online VAWG, in consultation with specialist organisations**
- **Technology companies should be required by the regulator to compile and publish annual transparency reports on online harm perpetrated on their platforms and the companies' response to it. This should include reporting on online VAWG and the data should be disaggregated by sex and other protected characteristics.**
- **Government and the regulator to raise awareness of tech abuse via public campaigns and guidance for regulated services**
- **The regulator should develop an appeals mechanism for individual users to bring a complaint when they have exhausted a platform's reporting process**
- **Domestic Homicide Reviews should be empowered to make recommendations to technology companies, where relevant, and notify the regulator where tech abuse factors in a domestic homicide and there is concern that technology companies could or should have acted differently**
- **Government should accept, and legislate for, the Law Commission's proposal for a new "harm-based" communications offence to replace the offences within section 127(1) of the Communications Act 2003 and the Malicious Communications Act 1988**

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?

42. The duties relating to adults' online safety and content that is harmful to adults should be more carefully considered if the Bill is to achieve the goal of addressing online VAWG. Duties relating to adults' safety must be strengthened and brought in line with those relating to children's online safety and illegal content; otherwise they will do little to protect women. For example, duties to protect adults' online safety, to carry out adult risk assessments and to provide additional reporting processes only apply to service providers which fall into Category 1. It is currently unclear which online platforms will be in Category 1, as the Secretary of State and regulator will designate this at a later stage based on number of users and functionalities, but it may be assumed that only the larger social media sites will be included in this classification. This could potentially lead to a two-tier system of regulation, whereby medium and smaller-sized platforms are left more open to a higher risk of online harms occurring on their sites. Perpetrators of domestic

abuse do not discriminate between platforms when pursuing a survivor. It is Refuge's experience that perpetrators will find any means to contact, abuse and control victims. Our frontline services have supported women who have experienced abuse across a broad range of platforms, from the largest social media sites, to smaller platforms such as dating apps for single Muslims. In one example, a perpetrator transferred small amounts of money to a survivor on PayPal in order to send abusive messages alongside the transfer. All online platforms should have responsibilities towards their adult users.

43. A key area for further consideration before the final Bill is put to Parliament is the resourcing and enforcement powers of the regulator. In Refuge's response to the Online Harms White Paper consultation, we supported the establishment of a new public body as the regulator, in order to ensure the regulator could develop expertise in the wide range of online harms and the enormous damage they have, and adequately enforce the duties of care and regulatory framework. Refuge endorses the regulator having a strong range of powers to increase the likelihood that companies pay due regard to their duties of care and cooperate with the regulator. The adequacy of the regulator's current enforcement powers in the draft Bill is of concern. For example, provisions to impose criminal sanctions against senior executives of tech companies are kept in reserve, and may only come into effect with the introduction of secondary legislation and a consequent two-year wait until the sanctions are enforceable. Criminal sanctions are also only applicable for non-compliance with information notices, suggesting they may not be brought forward for all breaches of duties of care. The regulator should have powers to hold senior executives liable from the start of their role as regulator. In addition, the regulator should also have powers to issue take-down notices to online platforms, requiring them to remove content. A full suite of enforcement powers is necessary as financial penalties alone may not be effective in holding platforms to account for breaches of regulation, particularly given the vast resources of larger tech companies. Further thought should also be given as to whether companies which repeatedly and brazenly fail to uphold their duties of care and to meet the codes of practice are permitted to "buy" their way out of regulation by paying penalty fees, rather than face criminal sanctions. Ultimately, the success of the new regulatory framework will depend on the regulator having the necessary powers and resourcing to effectively enforce it. It is currently unclear what resourcing will be allocated to the regulator to undertake their new role. Refuge argues the body will require significant resources to enforce the regulations, as they will be challenging some of the largest and most powerful tech companies in the world.

44. Finally, clarity should be provided as to the inclusion, or exemption, from the regulatory framework of certain features of platforms facilitating user-generated content. Refuge has supported women who have experienced abuse through features on social media sites such as voice messages on Instagram. It is not fully clear if features like one-to-one "voice notes" on WhatsApp and Instagram, or indeed WhatsApp as a platform in its entirety, are within scope of the regulations. Similarly to the categorisation of service providers as Category 1 or

Category 2A/2B, if such features are not included in the Bill's scope, there is a risk that a two-tier system of regulation may emerge. This would not be reflective of the ways in which survivors experience online abuse, and would require them to artificially separate aspects of their experiences based on the different functionalities of platforms.

45. **Refuge recommends that:**

- **Duties relating to adult's online safety should be more carefully considered and strengthened to align with those on children's safety and illegal content**
- **The regulator should have a full range of enforcement powers, including the ability to hold senior management criminally liable from the outset of their role as regulator and to impose take-down notices**
- **The regulator should be independent and allocated sufficient resources to effectively conduct its functions as regulator**
- **Clarity should be provided on the inclusion of platforms and platform features such as one-to-one "voice notes"**

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

46. This falls beyond the scope of Refuge's expertise. However, we recommend that when examining international efforts to regulate big tech, the government should include as a key indicator of success whether policies and interventions have resulted in a better response to and prevention of online VAWG and survivor satisfaction with the procedures and policies available.

Conclusion

47. Online violence against women and girls is an endemic, hugely damaging issue which must be addressed. The Online Safety Bill is a crucial opportunity to do so. Tech abuse and other forms of online VAWG are incredibly widespread, and women and girls are experiencing these harms in online spaces every day. As outlined in paragraphs 28-30 the impact of tech abuse and online VAWG on mental and physical health is immense, and risks shutting women out of online spaces entirely. Urgent action is needed to ensure women and girls are free to enjoy online spaces. The government's Tackling VAWG Strategy highlights the Bill as a key tool in responding to online VAWG, yet without explicit reference to online VAWG on the face of the Bill, it is difficult to see how this will be achieved in practise. As evidenced throughout our submission, it is clear that social media companies and other online platforms, and the criminal justice system are failing to protect survivors of tech abuse, and Refuge argues that without adequate focus on online VAWG in the Bill, women and girls will see little change in their experiences of online abuse.

48. The Bill has the potential to significantly improve the safety of survivors of domestic abuse and expand their routes to justice and protection. To achieve

this, it is vital the government safeguard women and children from online harms by building an online VAWG strand into the Bill and a corresponding VAWG code of practice to ensure technology companies and the new regulator prioritise the prevention and tackling of these harms.