Refuge submission to the Online Safety Public Bill Committee
Contact: Jessica Eagelton, Policy and Public Affairs Manager, jessica_eagelton@refuge.org.uk

About Refuge

1. Refuge is the largest specialist provider of gender-based violence services in the country supporting thousands of 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 41 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 broad aims of the Online Safety Bill to introduce regulation of user-to-user online services. Social media and other online platforms are frequently used by perpetrators of domestic abuse to control, monitor and harm survivors, yet many companies are failing to respond. Technology-facilitated domestic abuse – or tech abuse – is an increasingly prevalent form of domestic abuse. More than 1 in 4 women in England and Wales aged 16-74 experience domestic abuse at some point in their lives and of the women and children Refuge supported in 2020-21, 59% experienced abuse involving technology.[1] [2]

3. We welcome the government's ambition to make online spaces safer for women and girls, and the national and international commitments made to 'stem the tide' of online gender-based violence.[3] However, the Bill in its current form will not protect survivors of domestic abuse and other forms of violence against women and girls (VAWG). Despite the response to VAWG being a key priority of government and a growing body of evidence on the gendered nature of online abuse, the Bill does not directly reference women, girls, gender or VAWG, and instead only creates general safety duties[4] The Bill must be strengthened if it is to protect survivors and ensure women and girls are able to participate in online spaces.

4. Refuge welcomed the opportunity to provide oral evidence to the Committee and asks Committee members to consider the proposals outlined below in scrutiny of the Bill.
    a. Mandate Ofcom to develop a VAWG Code of Practice
    b. Include Controlling or Coercive Behaviour in the list of priority illegal offences
    c. Launch a funding package for victims of tech abuse and other forms of online violence against women and girls alongside the Bill

Refuge's tech abuse team and research

[1] ONS (2020), 'Domestic abuse prevalence and trends, England and Wales: year ending March 2020,' https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/domesticabuseprevalenceandtrendsenglandandw ales/yearendingmarch2020
[2] Refuge Annual Report 2020-21, https://www.refuge.org.uk/wp-content/uploads/2021/11/Annual-Report-nosig-Refuge.pdf
[3] G7 Interior and Security Ministers Ministerial Commitments, 'Annex 2: Protecting against online exploitation, violence and abuse.'
[4] See Tackling VAWG Strategy

5. In response to the growing threat of tech abuse, Refuge pioneered a specialist tech abuse service in 2017. The tech abuse team is expertly trained in supporting survivors and responding to complex tech abuse cases. They are the only such team in the country that works across frontline services, and Refuge therefore has unique insights into this form of domestic abuse and the barriers survivors face in seeking protection and justice.

6. Whilst tech abuse can take many forms across a range of devices and platforms, social media is a particularly powerful weapon for perpetrators. Domestic abuse perpetrated on social media platforms features in 35% of issues reported to Refuge's tech team.[5] We have supported survivors who have experienced harassment, stalking, monitoring, threats of violence, intimate image abuse, hacking of accounts, online impersonation and 'doxing' on social media and other platforms such as dating apps and websites.

7. Last year, Refuge conducted market research of over 2,200 UK adults into the broader prevalence of online abuse and the experiences of women and survivors of domestic abuse online. Our findings highlighted the scale, impact and severity of tech abuse on social media, and the inadequate response survivors currently receive from tech companies.

8. **1 in 3 UK women (36%) have experienced online abuse perpetrated on social media** or another online platform at some point in their lives, rising to almost 2 in 3 among young women (62%). The survey findings, published in our report Unsocial Spaces, revealed that 1 in 6 women experienced this abuse from a partner or former partner, equivalent to **almost 2 million women in the UK.**

9. The impact of this abuse is devastating, affecting survivors' mental health, and increasing the risk to their physical safety. Nearly all survivors responding to the survey (95%) said that the abuse had an impact on their mental health, or impacted them in other life-debilitating ways, such as by affecting their businesses and income. 1 in 10 said they felt suicidal because of the abuse. Tech abuse is closely linked to physical safety, in part due to the exploitation of location settings and geo-tagging by perpetrators. Almost 1 in 5 survivors (17%) said they felt afraid of being attacked or subjected to physical violence because of the tech abuse. Tech abuse rarely occurs in isolation, but as part of a pattern of coercive and controlling behaviour. 94% of women experiencing tech abuse on social media also experienced other forms of domestic abuse.[6]

10. Despite the prevalence and impact of tech abuse, survivors frequently experience significant barriers when reporting to social media companies, as the survivor stories below highlight. In Refuge's experience, many of these companies lack an understanding of the nature and different forms of domestic abuse and coercive control and are not sufficiently prioritising the response to VAWG occurring on their platforms. Many survivors are left waiting weeks or months for a response to their reports of harmful content, if a response is received at all. Reporting processes frequently require users to complete an automated form and select a reason the content is harmful from a finite list - domestic abuse is rarely included on these lists. Users must also often report pieces of content individually. This can be retraumatising and time-consuming, given perpetrators frequently send dozens or hundreds of abusive messages or posts. 52% of women responding to our survey said that the platform they experienced online abuse on handled their report badly.[7]

[5] Data for Refuge's tech abuse service
[6] Unsocial Spaces, Refuge, 2021, https://www.refuge.org.uk/wp-content/uploads/2021/10/Unsocial-Spaces-for-web.pdf
[7] Ibid

11. Orisa's story: *"When I was pregnant I was getting threats about my child. A lot of (the messages) were fake accounts – so it was over 40 accounts. I reported it to Snapchat; well I haven't heard anything back to be honest. I reported three times."*

12. Cece's story: *"I was looking how to report it and I found the reporting tool. It was difficult to use – if your options are not there you are restricted. It's ABC. You cannot report anything additional to that. The only exit was closing the account and starting a new one…If there is a report they [online platforms] should not ignore it. I was expecting for them to tell me, we are looking at that, we [are] doing [an] investigation, we will remove their account or whatever. No answer, [they] just ignor[ed] the situation…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. I would say [it's] trauma. On top of that they (the perpetrator) can get away with that – it's incredible."*[8]

13. Due to the unsatisfactory response from online platforms, the actions survivors can take in response to abuse are often restricted to either blocking the perpetrator themselves – which has minimal impact when they can easily create new fake accounts – or coming offline. 38% of survivors responding to our survey felt unsafe or less confident online and Ofcom research has shown that women are significantly less likely to feel that being online allows them to share their opinions and have a voice.[9] [10] This not only silences and isolates women from their networks and limits their ability to participate fully in online life and public debate, but can also escalate risk, as the perpetrator may turn to 'in person' forms of abuse when unable to contact the survivor online.

VAWG Code of Practice

14. In order to address the inadequate response from companies to tech abuse, Refuge recommends that the Bill be amended at Clause 37(3) to mandate Ofcom to develop a dedicated VAWG Code of Practice.

15. Including VAWG in the list of Codes of Practice that Ofcom must produce would be a straightforward and effective change to the Bill, and one which is supported by the Domestic Abuse Commissioner and Victims Commissioner.[11] [12] Without clear guidance to platforms on tackling VAWG perpetrated online, we fear the Bill will fail to ensure services put in place the appropriate measures needed for survivors. A Code would provide recommended measures for companies and share existing best practice more widely on the appropriate prevention and response to VAWG.

16. VAWG warrants a similar level of prioritisation to Codes of Practice already mandated in the Bill, such as those on fraudulent advertising, terrorism and child sexual abuse and exploitation. As of March 2021, VAWG is a strategic policing requirement, alongside terrorism and child sexual abuse and exploitation. The government has also made national and international commitments to tackling online VAWG, such as in the Tackling VAWG Strategy and as part of the UK's Presidency of the G7. Whilst Ofcom has discretion to create further Codes of Practice, their initial priorities will be to develop the Codes and guidance mandated in the Bill. The harms listed in the Bill will take precedence with Ofcom, and with platforms in complying with their duties, meaning VAWG will likely be deprioritised if it is not mandated. A dedicated Code of Practice on

[8] All survivor names have been changed to protect their anonymity
[9] Refuge, Unsocial Spaces, 2021.
[10] Ofcom, Online Nation: 2022 report, 2022.
[11] Domestic Abuse Commissioner, Blog: Commissioner calls for Online Safety Bill to be more robust when it comes to domestic abuse and violence against women and girls, 19 April 2022,
[12] Victims Commissioner, 'The Impact of Online Abuse: Hearing the Victims' Voice', 2022.

VAWG would therefore also send an important message to tech companies about the priority and urgency given by government to tackling violence against women and girls on these platforms.

17. In order to show that a VAWG Code of Practice would be workable and in line with the systems- and risk-based approach of the Bill, we have developed a draft Code with a coalition of experts. The Code provides detailed guidance for tech companies on the nature of online gender-based violence and sets out recommended measures covering topics such as risk assessment, mitigation, safety by design, user tools, moderation, transparency, enforcement of criminal law and victim support. The Code was jointly developed by Refuge, Ending Violence Against Women coalition, Glitch, NSPCC, 5Rights, Carnegie UK, and academics Professor Clare McGlynn and Professor Lorna Woods. If the Bill is amended to mandate a VAWG Code of Practice, we hope that this document could serve as a useful basis for Ofcom's development of a Code.

Inclusion of Controlling or Coercive Behaviour in Schedule 7

18. The list of priority illegal offences currently includes some domestic abuse offences, such as stalking, harassment and disclosure of and threats to disclose intimate images and films. However, there are a number of gaps in the list at Schedule 7 – the most significant being controlling or coercive behaviour. Refuge recommends the list of priority illegal content at Schedule 7 be expanded to include controlling or coercive behaviour (section 76 of Serious Crime Act 2015).

19. Controlling or coercive behaviour is prevalent on social media and carries serious risk of harm. It is one of the most common forms of domestic abuse, and forms part of the definition of domestic abuse as set out in the Domestic Abuse Act 2021. There were 33,954 offences of controlling or coercive behaviour recorded by the police in England and Wales in the year ending March 2021, but this is likely to be an underestimate of the true scale of coercive control, given than only one in five of the women Refuge supports will ever report to the police.[13] Coercive control is also a key indicator for domestic homicide. The most recent analysis of Domestic Homicide Reviews for the Home Office identified coercive control as the most common aggravating factor for domestic homicide, occurring in 65% of cases, with physical stalking the next most common factor identified at 18%.[14]

20. The government's draft statutory guidance to the Domestic Abuse Act 2021 outlines how perpetrators use technology and social media as a means of controlling or coercing victims.[15] In addition, the recently published revised draft statutory guidance on Controlling or Coercive Behaviour also highlights examples of the offence taking place on social media, such as where perpetrators place false or malicious information about a victim on their or others social media.[16] Further examples can include threats to kill, to harm and to share private and personal information about survivors (i.e. contact details), as well as humiliation and degradation of survivors, pile-ons and economic abuse via the targeting of survivors' online businesses or employers social media channels.

21. There are established practical steps companies can take to preventing and removing content which is controlling or coercive. Platforms such as Instagram and TikTok offer user-set filters of harmful comments, which is a well-used and helpful tool for survivors to prevent them from seeing triggering words and phrases. Instagram also offer a feature to

[13] ONS, Domestic abuse prevalence and trends, England and Wales: year ending March 2021, 2021.
[14] Analytics Cambridge and QE Assessments Ltd for the Home Office, 'Key findings from analysis of domestic homicide reviews,' 2022.
[15] See paragraph 59 of Domestic Abuse: Draft Statutory Guidance Framework, 2021.
[16] See paragraphs 26 and 129 of Draft Controlling or Coercive Behaviour Statutory Guidance Framework, 2022.

automatically block the same user if they create a new account, which can be useful where perpetrators seek to create new fake accounts when blocked by a survivor, although this only applies where the perpetrator uses the same details to create further accounts. Behavioural indicators can also be used to identify and prevent controlling or coercive behaviour, such as where a user sends multiple and repeated messages to another user.

New communication offences

22. Refuge supports reform of legislation governing harmful online communications. In our experience, the current legislation is not fit for purpose and does not adequately respond to some forms of tech abuse. The law in this area is often vaguely defined and sometimes poorly understood by law enforcement officers. Refuge has seen very few investigations and prosecutions for offences under the Malicious Communications Act 1988 and Communications Act 2003 when women report the abuse they have experienced to the police.

23. We therefore support the move to focus more on the risk of harm from a particular communication and hope that this will better reflect the realities of domestic abuse. However, we have a number of concerns regarding the new offences proposed in the Bill.

24. The harmful communications offence (clause 150) relies on a limited definition of harm relating to psychological harm. This appears to exclude other forms of harm arising from online communications, such as economic harms and self-harm and suicide. Economic abuse is an increasingly common form of domestic abuse. Refuge research has shown that 1 in 6 (16%) of adults in the UK say they have experienced economic abuse, with 39% reporting experiencing behaviours suggestive of economic abuse.[17] There is also a large and growing evidence base about the links between domestic abuse and suicide. It is estimated that every week 3 victims of domestic abuse die by suicide.[18] In addition, we are concerned about the interpretation of the 'without reasonable excuse' element of the offence. From our experience of supporting survivors, we anticipate perpetrators will argue that they needed to communicate with the survivor because of child contact arrangements, or because they were worried about the survivor's safety. It is also unclear whether some types of harmful communication used by perpetrators would fall within the definition of the offence. For example, where a perpetrator has liked a post which shows the location of a survivor or created a website or online forum to harass the survivor. Finally, we are concerned by the removal of the awareness of risk of harm element of the offence. Including a subjective awareness of risk would lead to a more workable offence that would capture circumstances where evidence of intention is challenging, but where it was clear that a perpetrator was aware their communication could cause harm but were reckless or disinterested in this risk.

25. With regards to the threatening communications offence (clause 152), the context within a communication is sent must also be considered by law enforcement and the courts when interpreting this new offence. Some survivors may receive threats disguised as innocuous messages, such as where perpetrators reference a date or event at which the perpetrator sexually or physically assaulted the survivor. Criminal justice professionals must take into account the context to such communications, which at first glance may not appear threatening. In addition, we recommend that existing offences relating to threats,

[17] Refuge, Know Economic Abuse, 2020.
[18] Walby, S. (2004), The cost of domestic violence, Women and Equality Unit.

such as threats to kill, are used more widely, as they better reflect the seriousness of a threat and therefore attract a more severe sentence.

26. Finally, we welcome the criminalisation of cyberflashing but recommend that the new offence be based on the lack of consent from the survivor, rather than the motivation/s of the perpetrator. Refuge therefore supports Professor Clare McGlynn's proposed amendment to clause 156.

Funding for specialist support services

27. Specialist VAWG organisations provide life-saving support to survivors of online VAWG. Refuge's tech abuse team has supported thousands of women, using their expertise to advocate for survivors, increase their safety and empower them to use technology safely. The service is highly effective in improving outcomes, as well as providing vital awareness-raising by working closely with tech companies and state agencies. Demand for specialist support is growing - between April 2020 and May 2021, there was an average 97% increase in the number of complex tech abuse cases requiring specialist tech support when compared to the first three months of 2020.[19]

28. Despite the prevalence and impact of online VAWG, specialist services largely rely on insecure, fundraised income. To ensure all survivors can access the support they need, government should launch a funding package for victims of tech abuse and online VAWG which ensures specialist services are sustainably funded. This could be achieved by dedicating a specified percentage of fines levied on social media companies for non-compliance with the new regulatory framework. For example, the following proposal is outlined in the VAWG Joint Principles for the Online Safety Bill: 5% of any fines levied by Ofcom to be directed to funding specialist VAWG sector support services, and for 50% of this amount to be specifically ring-fenced for specialist 'by and for' led services supporting Black and minoritised women and girls.[20]

Conclusion

29. The Bill is a vital opportunity to improve protections and safety for survivors of domestic abuse, and to ensure women and girls are free to exercise their rights and freedoms online. To ensure platforms are compelled to tackle domestic abuse and VAWG, Refuge recommends the Bill be amended to:
    a. Mandate Ofcom to develop a VAWG Code of Practice
    b. Include Controlling or Coercive Behaviour in the list of priority illegal offences
    c. Launch a funding package for victims of tech abuse and other forms of online violence against women and girls alongside the Bill

[19] Data for Refuge's tech abuse service.
[20] VAWG Principles for the Online Safety Bill, 2021.