Written evidence submitted by Refuge (COR0157)

About Refuge

Refuge is the largest specialist provider of gender-based violence services in the country supporting over 6,500 women and children on any given day. Refuge opened the world's first refuge in 1971 in Chiswick, and 49 years later, provides: a national network of 47 refuges, community outreach services, child support services, and acts as independent advocates for those experiencing domestic, sexual, and gender-based violence. We also run specialist services for survivors of modern slavery, tech abuse, 'honour'-based violence, and female genital mutilation. Refuge provides the National Domestic Abuse Helpline which receives hundreds of calls a day.

Refuge welcomes the opportunity to submit evidence to the Home Affairs Committee on Online Harms during the Covid-19 pandemic.

Tech abuse and online harms

1. Refuge has a specialist tech abuse service, consisting of a manager, eight tech leads and a network of tech champions, to support survivors and ensure that all of our specialist services and staff continue to adapt to and learn the ways in which perpetrators use technology to inflict abuse. Over 250 members of Refuge staff have been trained on tech abuse. To date, more than 4,500 survivors experiencing domestic abuse and other forms of gender-based violence have reported tech abuse to Refuge staff and have subsequently received specialist support around tech safety planning, with hundreds of complex cases being managed by our specialist tech team. Women are reporting a wide range of abuse including online stalking, harassment, image-based abuse, abuse of online banking and other accounts, abuse on social media, tracking devices and gaslighting.

2. Tech abuse very rarely exists in isolation, but is commonly part of a pattern of coercive and controlling behaviour and is closely connected with physical, sexual, economic and psychological abuse. An analysis of case files in which survivors had experienced tech abuse shows the following:

- 68% of tech abuse survivors were trying to separate and said perpetrators controlled everything
- 68% of tech abuse survivors were assessed as high-risk of being seriously physically harmed
- 95% had also been psychologically abused
- 73% had also been physically abused
- 42% had also been economically abused
- 33% of survivors had also been sexually abused
- 46% of survivors reported that their partner threatened he would eventually kill her and she believed him
- 18% survivors had attempted suicide due to the abuse that they suffered

The nature, prevalence and scale of online harms during the Covid-19 period

3. Evidence from around the world has shown that violence against women and girls (VAWG) increases following the imposition of lockdown measures introduced to reduce the spread of Covid-19 in the community. Evidence from China showed a three-fold increase in domestic abuse following the introduction of lockdown. France, Italy, Brazil, Cyprus, Spain, and the US have all reported rises in domestic abuse as a result of measures confining families to their homes.[1] Additionally, Refuge's own data shows that average calls and contacts to the National Domestic Abuse Helpline have increased by 50% compared to pre-lockdown averages. Traffic to the National Domestic Abuse Helpline website has increased by over 300% over the same period.

4. Online harms, including harassment, threats, image-based abuse, doxxing (putting someone's personal information such as home address and phone number online) and spoofing and other forms of impersonation (for example creating fake social media accounts, sending messages or pictures posing as the survivor) are commonly carried out as part of a pattern of domestic abuse and coercive control. Domestic abuse and other forms of VAWG therefore ought to be central when looking at online harms and developing responses.

5. Since the Covid-19 pandemic Refuge has seen a significant increase in referrals to our specialist tech abuse team. Malicious communications and harassment, monitoring and surveillance via hacked online accounts and threats to share intimate images are amongst the most common forms of tech abuse at this time. The Revenge Porn Helpline has also reported a significant rise in calls over the Covid-19 period, with over half of cases clearly part of a pattern domestic abuse[2].

6. Tech abuse has a significant and often long-term impact on the lives of survivors. Many of the women Refuge works with said tech abuse felt constant, suffocating and that there was no escape no matter what they did. Many women we support feel that they have no choice but to delete all social media accounts and reduce their use of the internet as much as possible. Unsurprisingly, they report that this can make them feel silenced, isolated, left out and make ordinary day-to-day tasks more difficult. Forms of tech abuse, like hacking and monitoring, can enable perpetrators to find out where women are living, working or socialising and risk women's physical safety. Threats to share intimate images can have a huge impact, with women pressurised by perpetrators do various things including share their location, meet up with the perpetrator and allow access to children. In Refuge's experience online harms and tech abuse have an enormous impact on both physical safety and psychological wellbeing.

Steps that could be taken to mitigate these concerns

7. Refuge advocates law, policy and practice change in order to improve the response to tech abuse. This should include improvements to the criminal justice system as well as regulation and accountability for tech companies.

---

[1] Guardian (2020). 'Lockdowns around the world bring rise in domestic violence'. https://www.theguardian.com/society/2020/mar/28/lockdowns-world-rise-domestic-violence

[2] BBC (2020) 'Coronavirus: Revenge Porn surge hits helpline' https://www.bbc.co.uk/news/stories-52413994

8. Reform to the criminal law is urgently needed. A particular problem identified by our specialist tech team is that threatening to share intimate images is not adequately covered by the criminal law. Whilst actual disclosure of a private sexual photograph or film is a crime under the Criminal Justice and Courts Act 2015 (known colloquially as the 'revenge porn' offence), threats to share are not. In Refuge's experience, when the survivors we support approach the police about these threats, they are told to wait until the images have been shared by the perpetrator and then come back, as only then is it a police issue. This is unacceptable and fails to recognise the coercive control used by perpetrators who threaten to expose these images.

9. Refuge welcomes the Law Commission's work on image-based abuse and malicious communications. However we note that this work is at an early stage and reform to the law is not guaranteed. Due the prevalence and impact of threats to share intimate images without consent we are calling on the Government to address this gap in the law in the Domestic Abuse Bill. This can be achieved by amending section 33 of the Criminal Justice and Courts Act 2015 to extend the offence to include threats. Such action would mirror the criminal law in Scotland, where both threats to share intimate images and the sharing of intimate images are clearly criminalised.

10. Recommendation: the Domestic Abuse Bill is amended to extend the criminal law on sharing intimate images without consent to include threats to share intimate images.

11. Action is needed to improve the policing response to crimes committed online and via technology. Whilst change to the criminal law is necessary, a significant amount of the behaviour which makes up tech abuse and online harm is already criminalised. Despite this, in our experience, there are very low levels of police investigation, arrests and prosecutions of these crimes. In addition, the police response can vary significantly between forces and between different officers within forces. Whilst some of our clients have had a good police response in regard to tech abuse, the overall picture is that online crimes are not treated with the same seriousness as other domestic abuse related crimes, despite the significant harm they can cause. It is therefore crucial that police receive training on the impact of tech abuse as a form of VAWG and ensure that online offending isn't treated as less serious, or unconnected to, crime committed offline.

12. In our experience, a lack of resources to capture and analyse digital evidence can lead to delays in a criminal justice response and can be a factor in crime committed by technology not being pursed robustly. Additional investment in police capacity to respond to and investigate online crime is therefore required.

13. Recommendation: training on tech abuse as a form of VAWG and additional resources for the response and investigation of crimes committed online are needed in order to improve the police response

<u>The Government's Online Harms proposals</u>

14. Refuge supports broadly the Government's efforts to begin to tackle the scourge of online harm with a statutory duty of care and a new regulator. However, we are disappointed by the lack of focus on the extent to which particular forms of online

harm disproportionately impact and act to abuse and silence women, as well as sexual and ethnic minorities and women with disabilities. We do not believe that sufficient attention and focus has been paid to the way technology is routinely used to perpetrate domestic abuse and other forms of VAWG and the link between tech abuse and physical safety. In particular, the lack of commitment to develop a specific code of practice on VAWG is a significant omission.

15. Refuge strongly argues that online VAWG/tech abuse is recognised as a specific form of online harm and that a code of practice for VAWG perpetrated online should be developed by the regulator as a matter of priority. Refuge recommends that the code considers and sets standards regarding the following issues:

1. Requirements to make the reporting procedure as quick and efficient as possible. Refuge has worked with many women who have been subject to a campaign of online abuse by their former partner, involving hundreds of abusive images and communication on a single platform. In many of these cases survivors must individually send links to every piece of abusive contact - a traumatic and time-consuming process. A robust code of practice should require relevant organisations to require limited information, for example the profile name and link of an abuser which the organisation then investigates and removes all abusive content.
2. Details on the speed at which the organisation acts. From our experience working with survivors of tech abuse, we know that the speed at which action is taken to respond to or remove abusive content is a key priority for survivors. The code of practice should detail the importance of speed and clear communication with survivors about the timeframe in which they can expect organisations to act. The regulator should then take a robust response to organisations which frequently fail to act promptly to protect survivors, remove content and delete or restrict the accounts of abusers.
3. Requirements for organisations to have clear policies and procedures to deal with threats to inflict harm or abuse. A key problem with the current system is that survivors have little recourse when someone threatens to harm them online, for example disclose sexual images without consent. At present, survivors have to wait until the perpetrator shares the images before they can do anything, which can be extremely traumatic. Whilst responding to threats to harm online is not straightforward (and also requires a change in the criminal law, above), it is a crucial issue that should be carefully considered as this policy area develops further.
4. Requirements to provide law enforcement agencies with the data they require to investigate and prosecute perpetrators. The majority of online harms and examples of tech abuse raised in this consultation response are crimes. Despite this, in our experience, there are very low levels of police investigation, arrests and prosecutions of these crimes. A major barrier to this is the difficulty in obtaining the relevant evidence of tech abuse from the platforms on which it is perpetrated. There is significant potential for the regulator to work with technology companies and the agencies supporting survivors to develop clear guidelines on how companies should cooperate with the police and survivors wishing to report crimes committed via their platforms to the police.

5. A VAWG code of practice should require companies set up systems which can take into account the context of reported abuse when responding to reports and removing abusive content. For example, Refuge has worked with many survivors who are abused via the non-consensual sharing of images which show them in a way which attracts potential condemnation and abuse in their communities – for example, by sharing a picture showing their hair when they always wear a hijab in public. Currently, survivors experience enormous difficulties in having this kind of highly abusive content removed, as it is not classed as a sexual image under the policies of many of the main social media companies.

16. Recommendation: the Government require a VAWG code of practice to be drawn up by the regulator as part of its Online Harms proposals

May 2020