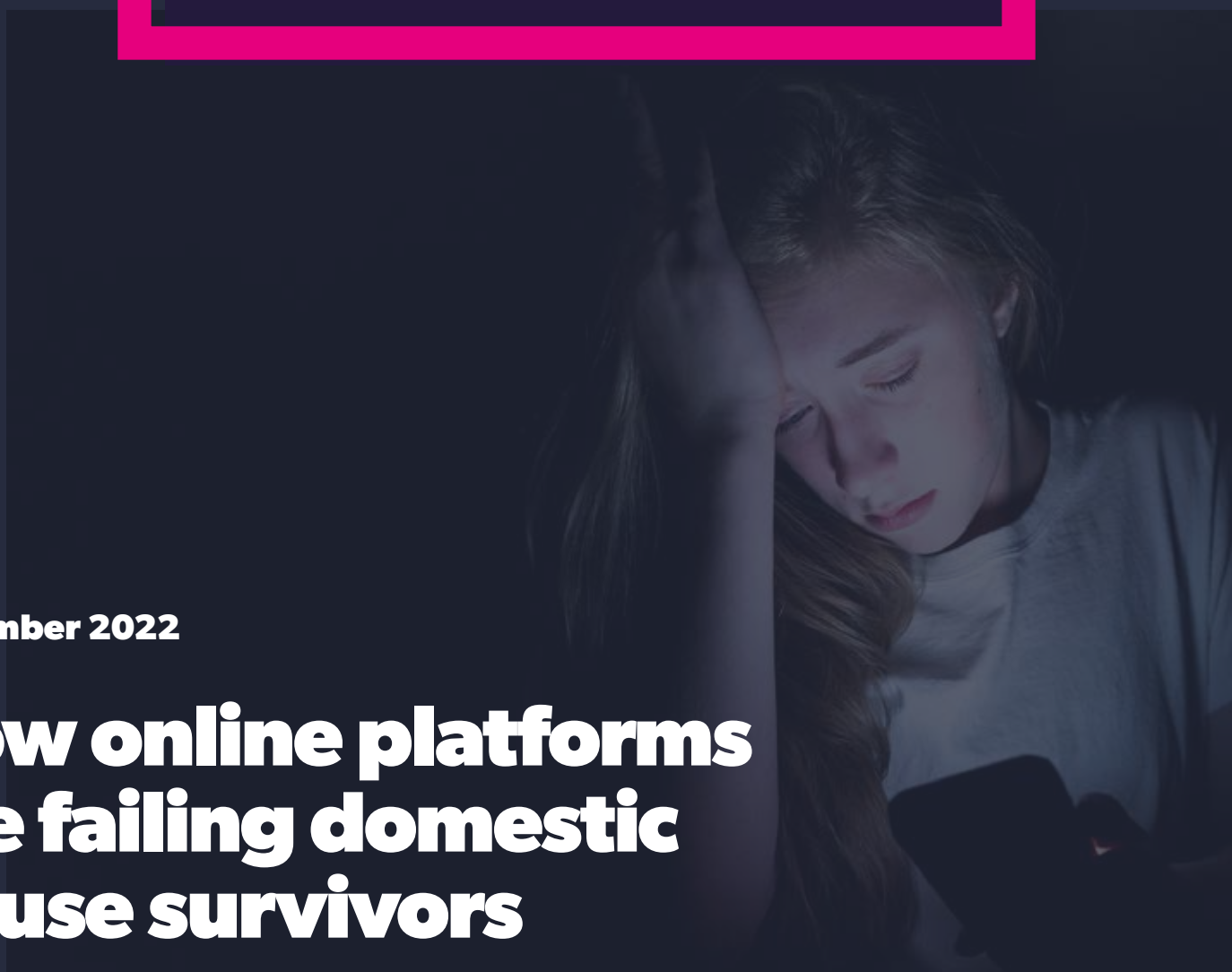
Refuge

For women and children.
Against domestic violence.

MARKED AS UNSAFE



November 2022

How online platforms are failing domestic abuse survivors

Summary

How online spaces are failing domestic abuse survivors

Advances in technology have changed the landscape of domestic abuse and handed new tools to perpetrators. Last year, Refuge commissioned research which, for the first time, revealed the scale, nature and impact of online abuse and harassment as a tool of domestic abuse. This report comes one year on from our Unsocial Spaces research, and offers a spotlight on content reporting and moderation, a key issue for survivors. Unsocial Spaces, available at: https://refuge.org.uk/what-is-domestic-abuse/law-and-policy/

Refuge has unique insight into survivors' experiences of reporting technology-facilitated domestic abuse – or 'tech abuse' – to social media companies. Our pioneering tech abuse team provides specialist support to women and children experiencing complex forms of tech abuse. It is the only such team working across frontline domestic abuse services in the country, and demand for the service is high. Between 2018 and 2022, the number of clients supported by the tech abuse team rose by 258%. [1]

Abuse and harassment on social media is one of the most commonly reported forms of tech abuse seen by Refuge's tech abuse team.[2] The team has developed relationships with many technology companies and has been recognised as a Trusted Partner by several major social media platforms. Trusted Partner programmes enable charities and researchers to communicate directly with safety teams at social media companies, to report abusive content and, in theory, to receive a more rapid response from the platform.

Despite the creation of these programmes, survivors still face significant issues when reporting domestic abuse related content to social media companies. These problems are exacerbated for those reporting without the support of a specialist domestic abuse support service.

To examine this topic, we interviewed 17 survivors supported by Refuge to hear in more detail about their experiences of reporting tech abuse content to social media companies. The interviews were conducted from the end of July to early September 2022. In addition, we conducted an online survey in September 2022, which 89 survivors of domestic abuse responded to, of whom 37 reported tech abuse to social media platforms.

Throughout this report are the stories of women who have experienced tech abuse on social media.[3] We are extremely grateful to the survivors who have shared their experiences with us and who have consented to their stories being shared in this report.

Our findings reinforce the conclusions of our Unsocial Spaces research and the experiences of the tech abuse team – namely, that many major social media platforms are consistently and utterly failing to support survivors of domestic abuse.

Paula* was referred to Refuge's tech abuse team after suffering extensive stalking and abuse from her ex-partner and his family and friends. She had been trying to report the abuse perpetrated on Facebook to the police, which had escalated to physical and sexual abuse. The police lost evidence which meant her case could not be sent to trial and her abuser and his family and friends walked free.

This encouraged Paula's ex-partner to accuse her of lying about the domestic abuse. He made public statements across many social media sites stating that she was a liar and encouraging others to abuse her.

Paula had to move because of the abuse and stalking – she received constant threats every day. Direct threats to harm were made and her name and address were publicly shared from the abuser's account (also known as 'doxing'). Refuge supported Paula to submit evidence of the abuse through the Trusted Partner channel because it clearly breached community standards.

Facebook were contacted six times about the threats and abusive content before a response was received. The platform eventually said that they would remove the posts – but this took four months. Facebook refused to close the abusive accounts, and Paula felt very let down by the platform's response.

In the end, Paula changed her social media account details, with extensive support on online safety from Refuge's tech team.

**All survivor names have been changed to protect their anonymity*

Refuge's experience is that domestic abuse and violence against women and girls (VAWG) is often under-prioritised and misunderstood by social media platforms. Generic approaches to moderating online harms are applied to domestic abuse related content, and these often fail to comprehend the gravity and severity of domestic abuse. For example, platforms frequently misunderstand the link between tech abuse and other forms of domestic abuse, and how tech abuse often escalates to, or is being perpetrated alongside, physical and sexual abuse. In addition, many do not understand that incidences of abuse are, in a domestic abuse context, almost always part of a wider pattern of abusive behaviour.

• 95% of survivors responding to the survey said they were not satisfied with the support they received from the social media company.

• Over half (53%) of survivors interviewed did not receive a response from the platform to their report. Only 29% received a response.

• Facebook, Instagram and WhatsApp – all platforms owned by Meta – are the most commonly used platforms to perpetrate abuse, as reported by the survivors we interviewed.

• After their experience of reporting content, 2 in 5 (41%) of the interviewed survivors said they were unlikely to report again. This is likely due to the myriad barriers survivors faced when reporting, such as the distress caused from lengthy waiting times.

Some companies do not explicitly reference domestic abuse in their community standards, which set out a platform's rules for what content can and cannot be posted. Platforms need to better understand the context of domestic abuse content, the risk to survivors' safety and the potential for abuse to escalate.

Urgent action is needed to ensure platforms take effective steps to respond to domestic abuse survivors. The Online Safety Bill is a crucial opportunity to improve protections for survivors, by regulating social media and introducing duties of care to users. 94% of interviewed survivors agreed that social media platforms should be regulated for users' safety. However, the legislation as drafted currently does not go far enough. To truly transform support for survivors, the Bill must be amended to clearly prioritise domestic abuse and other forms of VAWG.

Refuge urges the government to make two simple changes to the Bill to ensure the legislation delivers for survivors of domestic abuse:

- **Mandate Ofcom, as the regulator, to produce a violence against women and girls Code of Practice.** All survivors interviewed agreed that specific guidance should be given to platforms on tackling domestic abuse and VAWG.
- **Include controlling or coercive behaviour (section 76 of the Serious Crime Act 2015) in the list of priority offences in the Bill.** This will require companies to both prevent and address coercive control, a common form of domestic abuse, from occurring on their platforms.

[1] Refuge internal data for April 2018 (Q1 2018-19) to April 2022 (Q1 2022-23)
[2] Social media is the third most frequently reported issue to our tech team, not including 'other' issues
[3] All survivor names have been changed to protect their anonymity

Refuge is increasingly seeing technology play a key role in the ways in which abusers perpetrate domestic abuse..

1 in 4 women in England and Wales experience domestic abuse at some point in their lives, and the majority of women Refuge supports are now seeing technology used against them as part of this abuse.

Refuge's Tech Abuse Team provides specialist support to survivors experiencing this insidious form of abuse and commonly hears from women who have faced the same frustrating barriers, failed by social media companies when they have turned to them for support. Demand for our specialist support service is soaring.

Survivors are currently experiencing huge problems when they report online abuse and harassment to social media platforms. Often there are long waits for responses which can be distressing, and during which time abuse continues and can escalate, forcing women to feel they have no option but to come offline. Other times social media companies respond to say the content flagged does not breach the platform's community standards, when the content is clearly abusive, harassing or intimidating.

No woman should be forced offline because social media companies are failing to address abuse perpetrated on their platforms. Domestic abuse is a crime, and the lack of legislation and regulation of online spaces is endangering women and girls.

- Emma Pickering, Manager of Refuge's technology-facilitated abuse team

The number of survivors supported by Refuge's tech team rose by 258% between 2018 and 2022

Abuse and harassment on social media is one of the most frequently reported issues to Refuge's tech team

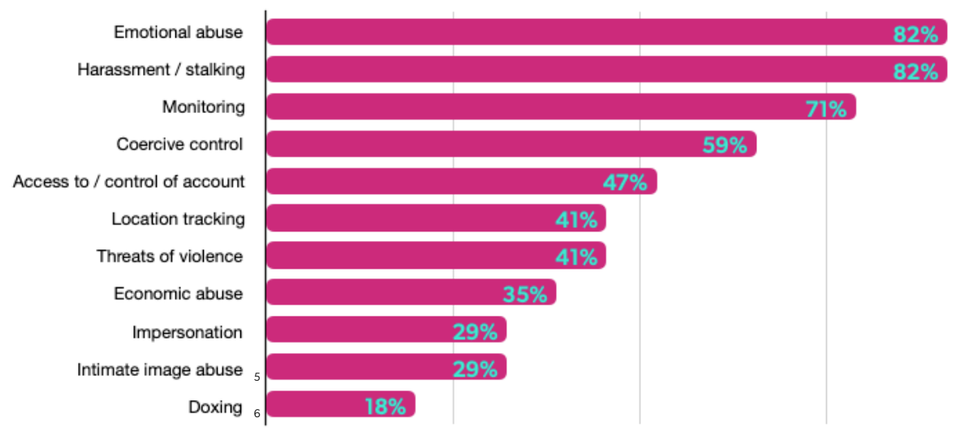
Types of domestic abuse on social media

For perpetrators, social media can be a powerful weapon, and tech abuse takes many different forms on these platforms. New forms of abuse continue to emerge with technological advances. For example, deepfakes - edited or fake images or videos, often intimate - are becoming increasingly realistic and more readily available.

For most of the survivors we interviewed (65%), the perpetrator of abuse on social media was their former partner. A quarter (24%) experienced abuse from their current partner. The large proportion of survivors who experienced abuse from a former partner illustrates how technology has allowed abusers to continue to harass survivors after separation, often at distance, great volume and for many months or years.

Many perpetrators enlist the support of others in the abuse - 35% of survivors we interviewed reported that the friends of family of their partner or former partner conducted abuse.

Survivors reported experiencing many forms of domestic abuse on social media: [4]



[4] Data from the 17 survivor interviews.
[5] For example, the sharing of intimate images or videos without consent, or threats to share. This can cause significant psychological and physical harm and social isolation to the individual depicted. For some groups of Black and minoritised women, such as South Asian women, the sharing of intimate images or videos risks stigma within their community and so-called 'honour-based' abuse. The definition of 'intimate' is often dependent on personal circumstances, including cultural and religious beliefs and attire.
[6] The online publication of private or identifying information about another individual, such as their name, home address or contact details, without their permission.

I don't feel any (platforms) are safe for women and girls.

Survivor of domestic abuse

The impact of tech abuse is significant. The toll of constant abuse, compounded by the frequent failure of platforms to act, has a severe effect on survivors' mental wellbeing. There is also an impact on women's physical safety, particularly where perpetrators have used social media to determine survivors' locations, or where there is a risk of so-called 'honour-based' violence - for example, following the sharing of a survivor's intimate images by the abuser, as shown in Mariam's story.

Survivors who rely on social media for their work and to promote their businesses also report that abusers target these channels to impact their economic livelihoods. Some survivors supported by Refuge have lost their jobs, business contracts and have had to move because of the abuse they have experienced online. Many more have been forced to come offline almost entirely, due to the lack of support from platforms to remain online safely.

Domestic abuse is perpetrated across a wide range of social media platforms, and often abusers will utilise several different platforms at the same time. Among the survivors we interviewed, the majority experienced abuse on a Meta-owned platform – 71% on Facebook, 53% on WhatsApp, and 41% on Instagram. Other common platforms included Twitter (18%), YouTube (18%), Snapchat (12%), and a dating website or app (24%).

When asked which platform they thought was safest for women and girls, most survivors said that none of the platforms were safe.

Community standards

Many platforms set out in their community standards what content is and is not permitted on their sites. Whilst some platforms do not include domestic abuse specifically in their standards – including Twitter, Snapchat, Instagram, TikTok and WhatsApp – many do include the abusive behaviours experienced by the survivors we spoke with.

For example, Twitter's rules clearly outline that users may not threaten violence, or engage in the targeted harassment, of an individual, or incite other people to do so. Facebook's community standards prohibit the use of threats that could lead to death, statements of intent to commit violence, attacking someone based on their status as a victim of domestic abuse, repeatedly contacting someone in an unwanted manner, and sharing or threatening to share non-consensual intimate imagery. Instagram state that serious threats of harm to personal safety are not allowed, and that they have a zero tolerance policy to threatening to post intimate images of others. Despite the clear statements from many platforms that these behaviours will be enforced in line with guidelines, it is evident that they are still frequently occurring, and platforms are failing to respond.

Mariam's ex-partner had been sharing her intimate images and videos online without her consent. As a result, members of Mariam's community made derogatory comments about her on Facebook, saying that she was a disgrace and brought shame upon her community, placing Mariam and her family members at risk of so-called 'honour-based' abuse.

Mariam was supported by Refuge's tech abuse team to report the abusive comments to Facebook; however, Facebook said the comments did not meet the threshold for action and that they would not remove the content. Mariam's ex-partner is still sharing her intimate images and videos on WhatsApp, which has been reported and she is awaiting a response from the platform.

Mariam feels very let down by the reporting experience, and her mental health has deteriorated.

Anastasia's ex-partner hacked into her Instagram account and locked her out of her account. Whilst in her account he uploaded intimate images of her, and then set her account as public, so her posts could be seen by anyone.

Anastasia's family tried to report the content and the hacked account but received no response from Instagram. Anastasia tried many times to regain access to the account, but was unsuccessful.

Refuge's tech team reported the content through the Trusted Partner channel and requested the immediate removal of the content. The platform responded with an automated reply which stated that because of Covid there would be a delay in responding. The platform had committed to reports being responded to within 48 hours. The tech team followed up on the report, but it took two weeks to get a response. The images were eventually removed but Anastasia suffered extreme distress during this time.

Adele was referred to Refuge's tech team after sharing concerns that accounts advertising sex workers and illegal drugs appeared on multiple platforms in the name of her child. This included dating sites and Telegram.

Adele describes her ex-partner as very tech savvy. He set up all her technology including devices, accounts, and business sites. Adele believes he still has control of her tech.

Adele reported the Telegram profile in her daughter's name. The tech team were unable to make the report themselves as a contact for the social media company could not be located. Adele also reported to the police and was advised without an IP address there would be nothing they could do.

The long wait for a reply

Survivors often tell us that their key priority when experiencing tech abuse on social media is for action to be taken quickly by platforms, for example, to promptly remove intimate images shared by the abuser. However, many survivors are left waiting weeks, months or even years for a reply from platforms after reporting tech abuse content.

Under a third of the survivors (29%) we interviewed received a response from the platform. 18% were uncertain if they received a response. Over half (53%) did not receive a reply. Similarly, 54% of survey respondents who lodged a report did not receive a response, further emphasising the poor response rate to domestic abuse-related content.

Of the small number of survivors we interviewed who did receive a response from the platform, none received a final response from the platform within 24 hours. 60% said they had to wait more than 3 days for a response, and 40% waited longer than a week.[7]

Whilst this provides a snapshot of waiting times, Refuge's tech abuse team confirms that many survivors are left waiting longer. In one instance, it took two years for a platform to remove illegal content, despite multiple agencies reporting the content and contacting the platform.

41% of interviewed survivors reported content more than three times, suggesting survivors are trying repeatedly to illicit a response from platforms. Many survivors supported by Refuge also tell us that their family and friends repeatedly report the content as well, and often receive no response.

Trusted Partner channels can be helpful in expediting reports of abusive content. However, waiting times can still be long through these processes. Some platforms, such as Snapchat, do not provide contact details or transparent information about where users can find support. This prevents survivors and support services from flagging abusive content. In addition, companies cannot exclusively rely on Trusted Partner channels, and on external agencies, as a sole provider of flagging content. For survivors who do not have access to specialist support services and to Trusted Partner programmes, waiting times can be even longer.

[7] The base size for this data is smaller (n=5), due to the small number of survivors who received a response from a platform.

Failing to act: the response from platforms

For survivors who do eventually receive a reply from platforms, many tell our tech abuse team that they are disappointed with the response or action, or indeed lack of action, taken by platforms. Whilst some platforms are taking positive steps to address violence against women and girls, the primary finding from our survey and interviews is of survivor dissatisfaction at the response and support available from platforms.

95% of survivors answering the survey said they were not satisfied with the support they received from the social media company they reported domestic abuse content to. Half of the survivors we interviewed (47%) said that they found the process of reporting abuse difficult, with 29% stating that the process was very difficult.

In many instances, the platform took limited or no action in response to the report. Over half of survey respondents who received a response from a platform (53%) told us the company said the content they reported did not breach the platform's safety guidelines. 35% said the company did nothing in response to their report. In other instances, survivors supported by Refuge have been informed that the content they have reported has been 'lost', so no further action can be taken. A small number of survey respondents said the company responded more positively, by either removing the post or content reported by the survivor (12%) or closing the perpetrator's account permanently (12%). [8]

"No change, the post was left up. I only had the option to report the person, not the image, and there was a technicality because they shared it rather than posted it."

Survivor of domestic abuse

A common response from platforms seen by the tech abuse team is that the content does not breach community standards, despite it clearly being abusive. Assuring platforms that reported content is indeed domestic abuse takes up a significant proportion of Refuge's tech abuse team time and extensive support is needed for survivors challenging platform decisions.

"Instagram told me the fake profile did not break any rules and did not remove it"

Survivor of domestic abuse

Among the small number of survivors we spoke to in interviews who had received a response, 40% were asked to provide further evidence following their original report. Often platforms require users, on reporting, to select from a finite list the reason why the content is abusive or inappropriate. Domestic abuse is rarely included in these lists, likely causing further delays in the moderation process. Some survivors recommended that platforms review these lists and enable users to provide additional context at the first point of reporting.

In Refuge's experience, generic content reporting systems often do not work for tech-facilitated domestic abuse. Other forms of cybercrime can often be more easily reported – for example where they are included in lists of reasons why content may be abusive – but there appears to be a lack of consideration of domestic abuse. Platforms often fail to understand or acknowledge the risk of tech abuse escalating to, or happening alongside, 'offline' abuse and violence.

Social media companies also frequently miss the context of domestic abuse. Moderators view content in simplistic terms without a wider understanding of the power dynamics and nuances of domestic abuse. As one survivor explains:

'It's too black and white, and abuse is not black and white.'

An example of this overly simplistic approach can be seen in how platforms respond to perpetrators, and in particular to fake accounts created by them. Perpetrators will go to great lengths to abuse and control the survivors, including recruiting others in the harassment, creating multiple fake accounts, and deflecting blame onto the survivor. Fake accounts are a powerful tool for perpetrators, as they can be created quickly and easily, and action is rarely taken to clamp down on their use. Platforms frequently refuse to act on fake accounts when reported and state that they have no ability to find out who the perpetrator is. Banning all anonymous accounts is not a viable solution, particularly given many survivors rely on anonymity or pseudonyms for their safety and to maintain an online presence. Instead, robust action should be taken against fake accounts reported for abusive behaviour, and measures to identify perpetrators by using IP addresses could be considered.

Carmen was being harassed online by her ex-partner. She blocked him, but he just created new accounts to continue harassing her. Carmen was supported by Refuge's tech team to secure her accounts. She was then supported to gather evidence of all the fake accounts and the content of the messages and abuse - in total there were over 120 fake accounts created by her ex-partner in a few weeks.

Carmen was determined not to come offline as she felt her ex-partner would see this as a victory, and he would then likely escalate to in-person harassment.

The fake accounts were reported to Facebook, who said that because most of the accounts were no longer active the issue was seen as resolved, and that they were unable to find the other accounts that were still live and being used to harass Carmen. This was challenged by Refuge's tech team. Facebook refused to remove posts which had been reported to the police. In addition, Facebook appeared to provide little help to the police with their investigation, claiming that they could not prove the posts had been from her ex-partner.

Carmen felt like she had no choice but to create a new account with a different name to try to prevent her ex-partner finding find her online.

Lois was referred to Refuge's tech abuse team as her ex-partner was harassing her on multiple social media platforms. The ex-partner had also recruited his friends and family to harass her on social media.

Lois needed to have a presence on social media due to her work – her ex-partner had told her he knew the most impactful way to ruin her was to destroy her reputation online. The perpetrator and his family and friends posted online that she was engaging in sex work, had sexually transmitted infections, was untrustworthy and would lie and steal from others. The harassment and abuse impacted Lois' business and she lost a number of contracts.

Lois felt hopeless as she had tried to report, block, and flag the content with the platforms but did not receive a helpful response, only an automated response to say that the reports did not breach the community standards.

The tech team reported the content through Trusted Partner channels. The response was delayed, and the team had to report the content on multiple occasions to get a response. The reports took six months to finally be acknowledged, but the platforms did not resolve the issue. Lois had to pursue the ex-partner through civil court to stop him from harassing her.

Lois felt let down by the platforms as it was clear that she was experiencing was abuse and harassment and she was frustrated that they could not see this, respond to her, and provide support.

[8] The base size for this data is smaller (n=5), due to the small number of survivors who received a response from a platform.

Impact of the reporting process

We asked the survivors interviewed how the response, or lack of response, from the platform made them feel, and what impact this had on them.

Survivors reported significant consequences for their mental wellbeing. Many said they felt disappointed, frustrated and vulnerable as a result of the failures of the reporting and moderating processes. Survivors want content to be removed as quickly as possible and waiting weeks or months for a response, or for action to be taken, often exacerbates the trauma they are experiencing.

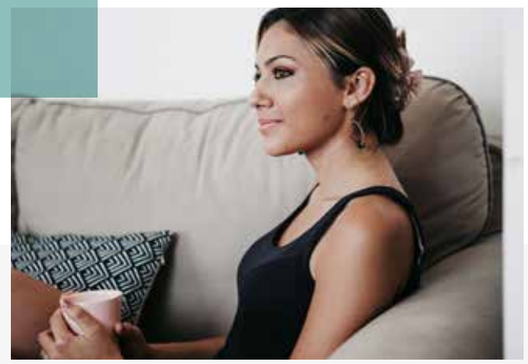
"Very frustrated and let down."

"It's all so overwhelming that you don't have it in you any more to fight against it."

"I had problems with anxiety as there were things written on social media which were not true about private matters of my life, and I had the feeling that there was nothing I could do."

"When you can't trust tech, you feel isolated in this world."

Because of the failure of platforms to take robust action on tech abuse, many perpetrators are able to continue to abuse with impunity. Survivors spoke of how platforms facilitated domestic abuse and of their frustration at the lack of sanctions or repercussions for abusers. Where platforms had deemed content as not in breach of community standards, survivors were left questioning the abuse they had experienced, contributing to gaslighting narratives.



"Even when he's not physically with me it feels like there's always the chance he could have gotten into an online space to watch me."

"I feel that it's too easy to get away with what he's been trying to do to me online. All of his attempts to get to me in online spaces just go without punishment."

"You start to think, 'Am I the crazy one?' because it doesn't feel like anyone takes this kind of abuse seriously."

Survivors also reported an impact on their access to social media and other online spaces. Our Unsocial Spaces research found that 38% of survivors of tech abuse on social media felt less safe or confident online.[9] Many find that they have little choice but to come offline, due to the poor response from platforms to protect them online.

Survivors tell us they want more support to stay online safely – whilst platforms often provide online guides, these are often not fully accessible or able to provide situation-specific advice.

"I felt like I had to be hiding. I couldn't share aspects of my life."

"All of my friends and family use Facebook Messenger, and during the pandemic it was my lifeline. When it was taken away it was horrible, I was angry at first but lost hope and became very low."

"I don't use social media in the same way. I still message people on there but it never felt the same again, it never felt really safe."

"I've come away from everything I can in the online world. I don't do social media, but I do still need accounts like Microsoft to engage with professionals. I tried really hard to keep online to stay in touch with others. I tried to create new profiles, but he constantly managed to find them. I eventually just gave up."

The response, or lack of response, to domestic abuse content also affects the chances of survivors reporting again in future.

After their experience of reporting content, 41% of interviewed survivors said they were unlikely to report content again. Fewer than 1 in 5 survivors (18%) said they would be very likely to report again in future. This means survivors have even fewer routes to protection online and may choose to 'put up with' any future abuse, likely resulting in perpetrators avoiding consequencies.

[9]Refuge (2021), Unsocial Spaces, available at: https://refuge.org.uk/what-is-domestic-abuse/law-and-policy/

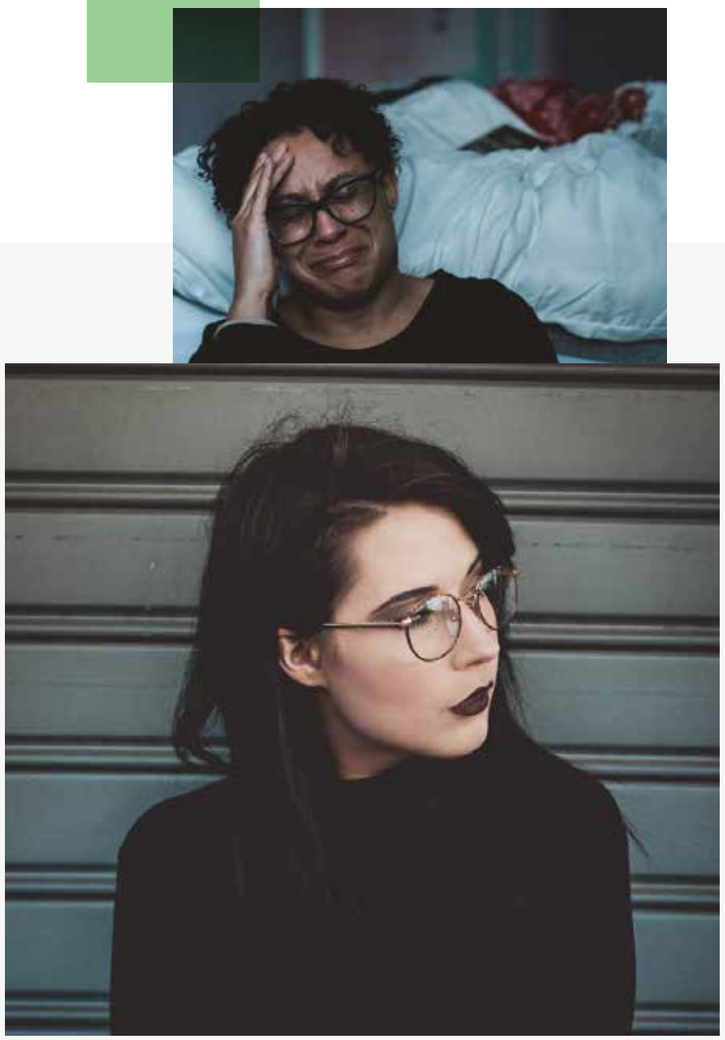
Understanding digital coercive control

One of the most common forms of domestic abuse is coercive control, whereby perpetrators seek to isolate and frighten survivors, to regulate their everyday behaviour and to make them subordinate. Coercive control is a crime which causes severe harm. It is also a key indicator for domestic homicide - in a review of cases where victims had been killed by their current or former partner, research has found that more than half had experienced coercive and controlling behaviour from the perpetrator.[10] [11] 34,000 offences of controlling or coercive behaviour are recorded by the police every year, although this is just the tip of the iceberg as only around 1 in 5 survivors report the abuse they are experiencing to the police.[12]

Increasingly abusers are turning to social media to coerce and control. 59% of the survivors we interviewed said they had experienced coercive control via social media. Further research conducted by Refuge also illustrates the high prevalence of this type of domestic abuse among young women – a third (30%) of young women say they have experienced controlling or coercive behaviour in a relationship, rising to over half (51%) when presented with a list of potentially controlling or coercive behaviour. One of the most commonly experienced forms of coercive control reported by young women is having their social media accounts monitored by a partner or former partner (26%). [13]

Other examples of coercive control on social media can include:

- Making threats, including to kill, harm, and to share private information publicly such as contact details (doxing)
- Humiliation and degradation
- Spreading malicious lies
- Monitoring and controlling online activity
- Control of finances, for example by targeting survivors' businesses or employers online
- Isolating survivors from their family and friends, for example by stopping the survivor from using their online accounts, or falsely posing as the survivor and responding in their place through hacking or the creation of fake accounts



Coercive and controlling behaviour has been an offence since 2015. Despite its prevalence, severity, and the existence of government guidance outlining how perpetrators use social media to coerce and control survivors, coercive control is generally poorly understood by technology companies.[14] Refuge's tech team has to advocate strongly for survivors to explain coercive control to platforms.

What needs to change?

We urgently need robust regulation of companies and social media which centres domestic abuse and other forms of VAWG.

The Online Safety Bill currently proposes to address violence against women and girls via generic, non-VAWG specific, changes to platforms' systems, including content reporting. However, as outlined throughout this report, domestic abuse is frequently not understood or prioritised by social media platforms, and generic approaches to moderating online harms often fail to comprehend the gravity and severity of domestic abuse. In addition, some domestic abuse offences are included within the current list of priority offences in the Bill, which platforms must both prevent and respond to. However, this list is incomplete and crucially leaves out coercive control

The Bill's current provisions will not go far enough to revolutionise the support and protection provided to survivors of tech abuse and make the internet a safer place for women. Two simple changes to the Bill will help ensure content reporting, and other systems, are better able to respond to survivors' needs:

- Mandate Ofcom to produce a VAWG Code of Practice
- Include controlling or coercive behaviour in the list of priority offences

VAWG Code of Practice

Together with a coalition of charities, academics and campaigners, Refuge firmly believes there is an unmissable opportunity to incorporate a dedicated Code of Practice on online VAWG in the Bill. Specific guidance to platforms on identifying and tackling VAWG is crucial to transforming their response to VAWG. All survivors interviewed agreed that specific guidance should be given to platforms on tackling domestic abuse and VAWG.

Whilst Ofcom has discretion to create further Codes of Practice, the new regulator has limited capacity and will likely have to prioritise drafting Codes that are 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 be deprioritised if it is not included in the Bill. A non-mandated VAWG Code would be many years away.

Incorporating a VAWG Code in the Bill would also reflect the government's commitment to tackling VAWG and the disproportionate impact of online abuse on women and girls. VAWG is a strategic policing requirement, as is terrorism and child sexual abuse and exploitation, both of which are mandated Codes.

A Code would include detail on suggested improvements platforms should make to reporting and moderating processes – including making the process as quick and efficient as possible. Survivors of tech abuse frequently say that their key priority is for a swift response from the tech platform, to quickly remove content, rather than, or alongside, a criminal justice response. A fast and effective response from social media platforms could make all the difference to survivors and enable them to stay online without fear of harassment. At a minimum, social media companies should be required to:

- Acknowledge reports within 24 hours. Serious offences should be actioned in 24-48 hours maximum, and within 3-4 working days for less serious offences.
- Set up systems which can take into account the context of reporting abuse when responding to reports, for example by investing in and training content moderation staff instead of over-relying on AI and algorithmic solutions.
- Provide law enforcement with data and evidence to investigate and prosecute perpetrators.
- Increase sanctions for perpetrators on platforms, in consultation with the survivor and in tandem with measures to address fake accounts set up by abusers.

Together with a coalition of experts - including The End Violence Against Women Coalition, NSPCC, Glitch, Carnegie UK, 5Rights Foundation and Professors Clare McGlynn and Lorna Woods - Refuge has developed a ready-for-use Code of Practice on Violence Against Women and Girls which could be adopted by Ofcom: https://bit.ly/3CcmANW

END VIOLENCE AGAINST WOMEN
GLITCH
5RIGHTS FOUNDATION
collective wellbeing Carnegie UK
Refuge
For women and children. Against domestic violence.
NSPCC

[10] Prepared for the Home Office by Analytics Cambridge and QE Assessments Ltd (2021), 'Key findings from analysis of domestic homicide reviews.'
[11] Professor Khatidja Chantler (2022), Manchester Metropolitan University, HALT Project.
[12] ONS (2021), 'Domestic abuse prevalence and trends, England and Wales: year ending March 2021.' and ONS (2018), 'Domestic abuse in England and Wales: year ending March 2018

Registered charity number 277424

[13] Opinium survey for Refuge of 1,010 16 to 19 year olds in August 2022, further detail available.
[14] For example, see: Home Office (2022), 'Domestic Abuse Statutory Guidance.' and Home Office (2022), 'Draft Controlling or Coercive Behaviour Statutory Guidance Framework.'

Coercive control in the list of priority offences

To ensure social media platforms prioritise, respond appropriately to and take steps to prevent this crime, Refuge recommends controlling or coercive behaviour (section 76 of the Serious Crime Act 2015) is included in the list of priority illegal content in the Online Safety Bill.

Some currently available tools can be used to prevent and address coercive control. For example, safety tools which enable users to filter harmful comments on Instagram and TikTok are well used by survivors to prevent them seeing abusive content shared by abusers. Instagram also offer a feature which automatically blocks new accounts linked to existing abusive accounts if the same log-in details are used by the perpetrator. The tech industry should work with the specialist VAWG sector to develop further technology to help identify, prevent and respond to coercive and controlling behaviour and other forms of domestic abuse.

"[Platforms need to] understand the very real-life implications of online abuse on health and wellbeing and recognise that online abuse can regularly lead to very damaging consequences."

"They [platforms] need to review their default options to report to ensure they cover all things and need to give you the chance to type context about the report."

"Respond in a timely manner, let us know what action is being taken, or why action can't be taken."

Survivor of domestic abuse

"Support women to understand what is going on. Provide a helpline - I don't understand technology so it would have really helped to have spoken with someone directly not going through an automatic process."

Conclusion

This snapshot report clearly illustrates how survivors of domestic abuse are repeatedly let down by social media companies and put at risk of potential further harm and abuse.

The findings from the interviews and survey demonstrate a pressing need to improve content reporting systems and the support provided to survivors. 95% of survivors in the survey said they were not satisfied with the support they received from the social media company. Many are faced with insufferably long waits for a response after reporting domestic abuse content, all whilst abusive content remains online, and perpetrators are left free to continue to abuse. Over half (53%) of survivors interviewed did not receive a response from the platform to their report. For those that do receive a response, often this is negligible. Shockingly, over half of survey respondents (53%) told us the platform said that the domestic abuse content they had reported did not breach the platform's safety guidelines, despite many platforms outlining their zero tolerance for abuse, threats and harassment.

The failure of platforms to act, or even respond in many cases, has a severe significant impact on survivors' mental health, online and physical safety, relationships with friends and family, and livelihoods. Many are forced to come offline due to a lack of alternatives, silencing thousands of women.

It is evident that social media companies must place greater priority on ensuring women and girls are safe on their platforms, and that specific guidance on addressing online violence against women and girls would help them to do so. Refuge urges the government to strengthen the Online Safety Bill by mandating Ofcom to produce a violence against women and girls Code of Practice and including controlling or coercive behaviour in the list of priority offences. To do so would dramatically transform survivors' experiences of reporting domestic abuse to social media companies.

About Refuge

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 44 refuges, community outreach programmes, child support services, and independent advocacy services for those experiencing domestic, sexual, and gender-based violence.

We also run specialist services for survivors of tech abuse, modern slavery, 'honour'-based violence, and female genital mutilation.

Refuge runs the 24-hour National Domestic Abuse Helpline which receives hundreds more calls and contacts from women experiencing domestic abuse every day and can be reached on 0808 2000 247.

www.refuge.org.uk
www.nationaldahelpline.org.uk
www.refugetechsafety.org

Refuge would like to thank the survivors of domestic abuse who supported this report.

Author: Jessica Eagelton

Refuge
One America Square,
17 Crosswall, London,
EC3N 2LB

020 7395 7700