

Your response

Please refer to the sub-questions or prompts in the [annex](#) of our call for evidence.

Question	Your response
<p>Question 1: Please provide a description introducing your organisation, service or interest in Online Safety.</p>	<p><i>Is this response confidential? – Y/ N (delete as appropriate)</i></p> <p><u>About Refuge</u></p> <p>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 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.</p> <p><u>Summary</u></p> <p>Refuge welcomes the opportunity to respond to this call for evidence and supports the broad aims of the Online Safety Bill to introduce regulation of user-to-user online services. 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 Social media platforms and other online services are frequently used by perpetrators of domestic abuse to control, monitor and harm survivors, yet many companies are failing to respond. In response to the growing threat of tech abuse, Refuge pioneered a specialist tech abuse service. Our expert team support survivors experiencing complex forms of tech abuse, and demand for the service continues to grow. Our aim is to empower women to use technology safely, rather than suggesting survivors limit their use of technology or come offline.</p> <p>Refuge would be pleased to support Ofcom in its new regulatory role by sharing the expertise and insight of our tech abuse team.</p> <p><u>VAWG Code of Practice</u></p> <p>We strongly recommend that a dedicated Code of Practice specific to violence against women and girls (VAWG) be developed by Ofcom. This recommendation is supported by a wide coalition of organisations and academics, including End Violence Against Women Coalition, Glitch, Carnegie UK, NSPCC, 5Rights and Professors Clare McGlynn and Lorna Woods, as well as the Domestic Abuse Commissioner and Victims’</p>

¹ ONS (2020), [‘Domestic abuse prevalence and trends, England and Wales: year ending March 2020.’](#)

	<p>Commissioner.^{2 3} Without clear and specific guidance to social media companies on tackling VAWG perpetrated online, we fear the Online Safety Bill and regulatory regime will fail to ensure platforms put in place the appropriate measures needed for women and girls. A dedicated Code, drafted in collaboration with VAWG specialists, would provide suitable guidance to services and ensure existing best practice is shared more widely on the appropriate prevention and response to VAWG. For example, platforms often fail to understand the gravity of online domestic abuse and do not consider the risk to survivors’ physical safety. Specific guidance on how abuse escalates would help services to better prioritise safety measures.</p> <p>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.</p> <p>In order to show that a VAWG Code of Practice would be workable and in line with the systems- and risk-based approach of regulation, we have developed a draft Code alongside sector partners (‘Joint Code of Practice’). The Joint 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. We hope that this document could serve as a useful basis for Ofcom’s development of a VAWG Code and stand ready to support with this work.</p> <p>Our primary recommendation throughout this response is that Ofcom develop a dedicated Code of Practice on VAWG. The recommended measures outlined in this response would ideally sit within a VAWG Code.</p> <p>Please note that our response focuses on social media, or user-to-user, platforms/providers.</p>
<p>Question 2: Can you provide any evidence relating to the presence or quantity of illegal content on user-to-user and search services?</p>	<p><i>Is this response confidential? – Y/ N (delete as appropriate)</i></p> <p>Last year, Refuge conducted research into the prevalence, nature and impact of tech abuse on social media. This included in-depth consultations with 18 survivors, and a nationally representative survey in August 2021, which was completed by 2,264 UK adults, of which 1,158 were female. The full findings of the research can be found in our Unsocial Spaces report.⁴</p>

² 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,

³ Victims Commissioner, ‘[The Impact of Online Abuse: Hearing the Victims’ Voice](#)’, 2022.

⁴ Refuge (2021), Unsocial Spaces, <https://refuge.org.uk/wp-content/uploads/2021/10/Unsocial-Spaces-for-web.pdf>

Prevalence

More than 1 in 3 women (36%) responding to the survey reported experiencing at least one behaviour suggestive of online abuse or harassment. Online abuse was almost twice as common among young women, with 62% experiencing online abuse. 1 in 6 women (16%) said that the online abuse they suffered came from an intimate partner or former partner. This is equivalent to almost 2 million women. Again, this figure rises among young women - 1 in 5 (22%) reported online abuse came from a partner or former partner.

Types of tech abuse

Tech abuse can take many different forms, and survivors often experience a combination of types of abuse. Among the survivors we interviewed, common forms of tech abuse on social media disclosed were online harassment (such as being bombarded by abusive messages), stalking and monitoring, the hacking and controlling accounts, and use of social media to determine survivors' locations, including successful attempts. Survivors also report that abusers use social media to perpetrate economic abuse (the restriction of a person's ability to acquire, use and maintain money or other economic resources). This can include targeting survivors' online businesses and spreading malicious lies on survivors' employers' social media accounts. In addition:

- 23% of survivors in the survey said they had, or had reason to believe, they had been stalked or monitored online.
- 22% received threats of physical or sexual violence.
- 21% reported someone else had access to an account they did not want them to.
- 17% had experienced non-consensual intimate image sharing, and 14% experienced a threat to share an intimate image or film. Our research has also shown that 1 in 14 adults have experienced threats to share their intimate images or films, an act which was criminalised in the Domestic Abuse Act 2021 following a campaign by Refuge.⁵
- 11% reported doxing.

It is vital that guidance to providers outlines the different forms that domestic abuse and VAWG may take, and the dynamics of domestic abuse. In our experience of supporting survivors of domestic abuse on social media, providers often fail to grasp the context, subjectivity and gravity of domestic abuse. For example, survivors supported by Refuge have received images of their front doors and road signs after fleeing the perpetrator and moving to a safe, secret location. This can be extremely traumatic for survivors, with women feeling physically unsafe because the perpetrator knows their location. When judged at face value, as simply images of a

⁵ Refuge (2020), 'The Naked Threat,' <https://www.refuge.org.uk/wp-content/uploads/2020/07/The-Naked-Threat-Report.pdf>

door, such content would likely not be seen as harmful or in breach of community standards. But when viewed within the context of domestic abuse, this content is clearly harmful and threatening.⁶ In particular, there is a lack of understanding among providers of controlling and coercive behaviour. Controlling and coercive behaviour is one of the most common forms of domestic abuse and carries serious risk – it is a key indicator for domestic homicide.⁷ On social media, it can take the form of making threats to harm and to kill, monitoring, humiliation and degradation, and spreading malicious lies, all with the underlying aim of isolating the victim and making them dependent upon the perpetrator. Codes relating to illegal content must include information on the different forms of domestic abuse, including coercive and controlling behaviour. Further detail on suggested measures platforms can take to address controlling and coercive behaviour are provided in response to question 18.

In addition, perpetrators are targeting survivors' family and friends as part of their abuse. 50% of survivors responding to our survey said that their family or friends had been targeted as part of the online abuse, including 12% who sadly reported their children had been targeted by their partner or former partner. Children are now legally recognised as victims of domestic abuse, following the passage of the Domestic Abuse Act 2021. Perpetrators are also encouraging their own family members and friends to take part in abuse - 51% of survivors said that a third party was also involved in the abuse. 19% of these survivors said that this was the family of their partner or former partner.

Impact

The impact of tech abuse can be devastating. Our research revealed that 95% of the women responding to the survey said that the abuse from their partner or former partner on social media impacted them negatively. More than 1 in 3 felt anxious and stressed (37% and 36%), and 1 in 5 felt ashamed and isolated (21% and 19%). 1 in 10 survivors (10%) felt suicidal. 38% of survivors of tech abuse also said they felt unsafe or less confident online, illustrating the impact on women's access to online spaces.

Our research also showed that survivors are experiencing tech abuse for extended periods of time. On average, survivor survey respondents endured tech abuse for at least six months. Several survivors we spoke with were also unsure if the abuse on social media was ongoing because they had come offline because of the tech abuse. This is likely to have caused further stress and harm, as survivors did not know if the perpetrators were continuing to post abusive messages, or was contacting their social network, without their knowledge.

⁶ We are pleased that the proposed new harm-based communication offence will consider the context in which the communication was sent, and that the government has stated that these examples would be covered by this new offence. For further detail, please see: <https://www.gov.uk/government/news/online-safety-law-to-be-strengthened-to-stamp-out-illegal-content>

⁷ Analytics Cambridge and QE Assessments Ltd for the Home Office (2021), 'Key findings from analysis of domestic homicide reviews,' <https://www.gov.uk/government/publications/key-findings-from-analysis-of-domestic-homicide-reviews/key-findings-from-analysis-of-domestic-homicide-reviews>

	<p><u>Platforms where abuse takes place</u></p> <p>99% of survivors responding to the survey reported experiencing domestic abuse on a Meta-owned platform (Facebook, WhatsApp, Instagram). Facebook was the most commonly reported site used to perpetrate abuse, with 45% saying this is where the abuse occurred, followed by 32% for Instagram and 21% for WhatsApp. Over 1 in 10 (12%) had experienced tech abuse on a dating website or app. However, perpetrators will use any means necessary to pursue survivors, including using smaller services and moving from one service to another, if they are blocked on one service. Survivors often also experience abuse across more than one platform, as perpetrators move from one site to another to continue their abuse. It is therefore important that all platforms, regardless of size, should be required to prioritise preventing and addressing tech abuse.</p> <p><u>Survivor stories</u></p> <p><i>“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.”</i></p> <p><i>“He’d send me voicemails - you can do that on Instagram. He made other accounts where he threatened to kill me and then he messaged my family on (social media)”</i></p>
<p>Question 3: How do you currently assess the risk of harm to individuals in the UK from illegal content presented by your service?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>
<p>Question 4: What are your governance, accountability and decision-making structures for user and platform safety?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>
<p>Question 5: What can providers of online services do to enhance the clarity and accessibility of terms of service</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p> <p>Providers must list domestic abuse and other forms of VAWG within their terms of service and community standards as crimes which will not be tolerated on their platforms and take robust actions to uphold these terms.</p>

<p>and public policy statements?</p>	<p>Providers should ensure users communication needs are met and that any communication barriers are removed, in order to allow users to effectively engage and consider terms of service and public policy statements. These documents must consistently be provided in formats and languages which can reach users, such as British Sign Language, languages other than English, Easy read and large print.</p> <p>Survivors of tech abuse are often made to feel by perpetrators that they are not ‘tech savvy’, and/or actively prevented from using technology, meaning they may be less confident navigating online services and understanding terms of service and community standards. For example, a national survey carried out by Refuge and Avast found that only 64% of women in the UK have admin control over the internet-connected devices in their own homes; and one in four (27%) stated that admin access for these devices has not been shared equally or with transparency in their household.⁸ Providers of services should therefore ensure that their terms of service and related documents do not contain any tech jargon or phrases that cannot be easily understood, to ensure they are accessible to those with less knowledge of technology.</p> <p>Terms of service should also have clear policies and procedures to deal with threats to inflict harm, including protection from fake accounts. Many social media companies are not taking adequate steps to tackle fake accounts used by abusers. For example, Facebook state that fake accounts do not breach their community standards, yet perpetrators make frequent use of fake accounts, often setting up many accounts to abuse a survivor, even if survivors have blocked them, or sanctions imposed on one account. Noting that some survivors of domestic abuse rely on fake accounts for their own safety, terms of service should therefore be clear about the creation and use of fake accounts to abuse, and platforms should improve the detection and tackling of fake accounts set up by perpetrators, including their removal. Further detail on the role of fake accounts is provided in answer to question 18.</p>
<p>Question 6: How do your terms of service or public policy statements treat illegal content? How are these terms of service maintained and how much resource is dedicated to this?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>
<p>Question 7: What can providers of online services do to enhance the</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p> <p>One of the key barriers to addressing tech abuse is the inadequate reporting mechanisms provided by social media platforms. A key priority for</p>

⁸ Research by Censuswide for Refuge and Avast in July 2021, with 2,000 women in the UK aged 18 and over, <https://www.refuge.org.uk/refuge-and-avast-hidden-home-dangers/>

transparency,
accessibility, ease
of use and users'
awareness of their
reporting and
complaints
mechanisms?

survivors is often for abusive content to be removed as quickly as possible. However, survivors reporting content and/or users to platforms are frequently left waiting weeks for a response. Some never receive a reply or are told that content does not breach community standards, despite clearly being evidenced as domestic abuse. Our Unsocial Spaces research showed that over half (52%) of women experiencing online abuse who reported this to the social media company said that the platform handled their report badly. An analysis of survey responses to a question on what online platforms did following a report of online abuse showed the most commonly used term was “nothing.” Companies are often failing to understand the risks and nature of VAWG, and due to unsatisfactory responses to reported content, many women feel they have little choice but to come offline. This could risk an escalation of the abuse as a perpetrator may opt to show up in person when they are unable to get in touch with the survivor online.

Refuge will publish further research on survivors' experiences of reporting tech abuse to social media companies in autumn 2022. We would be pleased to share this report with Ofcom as soon as it is available.

In order to improve reporting mechanisms so that they are fit for purpose for survivors of domestic abuse, Refuge recommends the following measures are adopted by providers to provide effective and easy to use reporting functions. Further details can be found in our Unsocial Spaces report (pg. 26) and in the Joint Code of Practice (pg. 25).

- **Work in collaboration with specialist VAWG services to bring victims' experiences into the design of reporting systems.** Too often companies have claimed to rely on internal VAWG expertise which does not translate into wider practices across the service and is often not transparent. Providers should engage with external VAWG organisations, who can provide the greatest source of insight and evidence on high level emerging issues and provide adequate remuneration to these organisations.
- **Make the reporting process as quick and efficient as possible.** All platforms should 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. These response times must be adhered to, and details published on the speed at which platforms respond. Survivors are currently waiting weeks, or even months, for a response. Until very recently, and despite being over two years since the first national lockdown in the UK, Facebook was sharing an automatic response to trusted flagger referrals stating that 'due to COVID-19, we are currently experiencing delays in responding to most reports.' Users should also be directly informed of any decision made by platforms and be provided with a specific point of contact so that they can follow up on decisions made.
- **Victims should be able to provide the username of the perpetrator,** rather than reporting individual pieces of content. Survivors must usually report individual pieces of content in turn

and are not able to report a user. Perpetrators will often send dozens or hundreds of messages, making reporting a time-consuming and potentially re-traumatising process for survivors.

- **Providers should ensure that abuse can be more easily reported across multiple platforms**, and that providers cooperate to ensure perpetrators are identified and sanctions imposed on them. Where abuse has been cross-platform, currently users must report content to each platform individually. This appears to be the case even when platforms are owned by one parent company, such as Facebook, WhatsApp, and Instagram.
- **Users must be able to effectively report content that is illegal or harmful to regulated services through clear and transparent flagging mechanisms.** Current processes sometimes 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, meaning survivors cannot easily inform platforms that they are experiencing domestic abuse. This often leads to even lengthier delays in reporting waiting times.
- **Systems must be able to account for the context, complexity and subjectivity of domestic abuse.** As outlined in response to question 2, survivors supported by Refuge have received images of their front doors and road signs after fleeing the perpetrator and moving to a new location. Reporting processes must be capable of considering the wider context in which content has been sent or shared, rather than simply viewing content and online activity in a vacuum. Users must be given the ability to submit third-party content in relation to specific cases of content violation. Training and investment in content moderation staff could also help improve providers' ability to identify tech abuse on their platforms. Please see our response to question 11 for further detail on moderation.
- **Consideration should be given to reporting processes for non-users such as teachers or family friends and support services**, who are able to report without the victim needing to engage further with the abuse. The Joint Code of Practice recommends that services must consider putting in place an appropriate trusted flagger programme that maintains independence from the online service and from government. The programme must include UK based non-government organisations and other experts, including the specialist VAWG sector, who will be vetted, to inform on policy development and report on new trends in harmful and illegal content. Providers with a trusted flagger policy should not use flaggers as the sole provider of flagging content, should ensure flaggers are appropriately compensated, and commit to an expectation on response times to flagged report of 24 hours. Further detail on aspects of a successful VAWG trusted flagger policy can be found on page 27 of the Joint Code.

	We refer to the Joint Code of Practice for recommendations on dispute resolution and complaints functions.
Question 8: If your service has reporting or flagging mechanisms in place for illegal content, or users who post illegal content, how are these processes designed and maintained?	<i>Is this response confidential? – Y / N (delete as appropriate)</i>
Question 9: If your service has a complaints mechanism in place, how are these processes designed and maintained?	<i>Is this response confidential? – Y / N (delete as appropriate)</i>
Question 10: What action does your service take in response to reports or complaints?	<i>Is this response confidential? – Y / N (delete as appropriate)</i>
Question 11: Could improvements be made to content moderation to deliver greater protection for users, without unduly restricting user activity? If so, what?	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p> <p>Refuge agrees that improvements can be made to content moderation to secure greater protections for users without unduly restricting user activity. We wish to emphasise that women and girls’ online activity is already being restricted by the lack of protections afforded to them in online spaces. Ofcom research has shown that women are less confident about their online safety than men, are more negatively affected by discriminatory content and feel less able to have a voice online.⁹ Some survivors supported by Refuge report that they have been advised to ‘come offline’ as a ‘solution’ to the abuse they are experiencing, and indeed, 38% of survivors of tech abuse said they felt unsafe or less confident online.¹⁰</p> <p>Providers should invest in a sufficient number of human moderators who have been fully trained in identifying and responding to different types of tech abuse and other forms of VAWG. They must also be trained in providing support to survivors and signposting to specialist support services. To the untrained eye, tech abuse can often be hard to recognise without an</p>

⁹ Ofcom, [‘Ofcom urges tech firms to keep women safer online,’](#) 1 June 2022.

¹⁰ Refuge (2021), Unsocial Spaces.

	<p>understanding of the broader context of domestic abuse and coercive control. An element of human oversight in content moderation will always be needed – it is likely that automated/AI content moderation would fail to identify the contextual and subjective nature of tech abuse. Human moderators should be equipped to identify nuances within domestic abuse and VAWG and to provide support to users experiencing these harms. Such training should include new emerging forms of abuse, as well as making clinical supervision available to staff.</p> <p>Clear timelines should be set for content moderation, in line with our recommendations in response to question 7, and moderators should keep users up to date and provide clear explanations of decisions.</p>
<p>Question 12: What automated moderation systems do you have in place around illegal content?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>
<p>Question 13: How do you use human moderators to identify and assess illegal content?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>
<p>Question 14: How are sanctions or restrictions around access (including to both the service and to particular content) applied by providers of online services?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p> <p>Sanctions and restrictions to access are currently applied poorly by providers, and survivors of tech abuse often find they are given few options to address the abuse they are experiencing. There are few consequences for perpetrators, partly because providers rarely ban them entirely from their platforms. Where platforms do take steps to impose sanctions on perpetrators, or where survivors block an abuser’s account, perpetrators will often simply create a new fake account. Platforms must improve the detection of fake accounts set up by perpetrators, and take more robust action to address them, including removing fake accounts used to abuse.</p> <p>Tech abuse will often escalate over time, increasing the risk of harm to the survivor. 48% of the female survivors responding to our survey said that the abuse they experienced on social media got worse over time.¹¹ Increased sanctions for perpetrators are needed to help ensure they are more easily identified, and abuse stopped at an earlier stage to protect survivors.</p> <p>Often, survivors are restricted in the actions they can take to blocking the perpetrator – which has minimal impact when the perpetrator can easily set up new fake accounts – or coming off of the online service, which as outlined previously may lead to an escalation of abuse.</p>

¹¹ Ibid.

	<p>Increased sanctions should therefore be imposed in consultation with the survivor and in tandem with measures to better detect and address fake accounts set up to abuse. This could include timed and permanent user bans, with permanent bans for serious cases of tech abuse. Services should also draw on insight from the specialist VAWG sector so as not to take actions which may inadvertently escalate the risk of harm to survivors.</p> <p>Even where providers do take robust action, this is rarely done in coordination with other providers, meaning perpetrators are often able to simply continue abuse on another platform. Platforms should work together to take joint actions against perpetrators, and parent companies of multiple services should also ensure users banned on one of their sites are banned across all platforms.</p>
<p>Question 15: In what instances is illegal content removed from your service?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>
<p>Question 16: Do you use other tools to reduce the visibility and impact of illegal content?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>
<p>Question 17: What other sanctions or disincentives do you employ against users who post illegal content?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>
<p>Question 18: Are there any functionalities or design features which evidence suggests can effectively prevent harm, and could or should be deployed more widely by industry?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p> <p>The design of safer features and functionalities is an important aspect of improving women and girls’ safety online. Providers of online services must adopt a safety by design approach and consider how their products can be used to perpetrate tech abuse. Some features of services inadvertently allow or even encourage tech abuse. This can include generic default passwords and ‘ring-fencing’ location features, where devices moving into or out of a specific physical area can be tracked and alerts received on movements. Companies should consider from the earliest design stages how their products may be used to abuse women and girls, and work in consultation with the specialist violence against women and girls sector to design these features out as far as possible.</p> <p>Equally, some design features and functionalities currently employed by providers can be effective in helping to prevent harm. For example, the</p>

ability to filter harmful comments and phrases, such as on Instagram and TikTok, is a tool that is well used by survivors of tech abuse. It can be helpful for survivors to prevent them from seeing abusive and triggering comments sent by the perpetrator, whether by using his own account or a fake account, or comments sent by his friends and family.

In addition, Instagram also offer an optional feature when blocking an account to pre-emptively block new account/s created by the same user. This can help survivors to proactively block future accounts created by their perpetrator. However, there are limitations to this feature, as this only works if the perpetrator uses the same details when creating the new account.

The above examples are both measures that could be employed by more providers to proactively address offences of controlling and coercive behaviour. Providers could also look at behavioural indicators to identify coercive control. For example, a case of multiple accounts harassing a user may be an instance of a perpetrator setting up fake accounts to abuse a survivor, or an indication that they have instigated a 'pile on' and/or shared the survivors' user details with third parties for the purposes of 'outsourcing' the abuse.

With regard to the extent to which functionalities that allow users to have an anonymous profile help prevent or facilitate harm, Refuge would like to point to the number of domestic abuse survivors who rely on online anonymity for their own safety. Survivors must be able to continue to utilise anonymous or pseudonymous profiles. It should be recognised too that the use of such profiles is a common tactic used by perpetrators of domestic abuse to abuse and harass survivors. In some cases, survivors have been contacted by dozens or hundreds of fake accounts, all of which they suspect to be the perpetrator or his network. Providers often fail to take action to address these accounts, where the perpetrators are known (or suspected) but hiding behind fake profiles and pseudonyms. Even when supported by Refuge's tech abuse team, survivors face significant barriers when trying to persuade online providers to take action. In our experience, social media companies typically fail to acknowledge the presence of fake accounts on their sites or to investigate suspected fake accounts. Platforms profit from the number of users present on their site via advertising, so there is often little incentive for them to remove fake accounts. For further detail on account creation, please see the Joint Code (pg.16).

Perpetrators frequently seek to use online platforms to determine a survivor's location, for example via location settings and geo-tagging functions. 19% of survivors supported by Refuge's tech abuse team said their location had been compromised because of the tech abuse.¹² This has implications for survivors' physical safety - almost 1 in 5 women (17%) said they felt afraid of being attacked or being subjected to physical violence because of the tech abuse.¹³ We would encourage platforms to integrate

¹² Statistics for July 2020 to March 2021.

¹³ Refuge (2021), Unsocial Spaces.

	<p>similar features to Apple’s Safety Check, which enables users to review their sharing and access settings, and to reset privacy permissions for all apps, restricting access to their messages, app access, location tracking and other information.</p> <p>The Legacy Contact feature on Facebook is another example of how the poor design of new features on platforms is misused by perpetrators. The feature enables a chosen user to look after another user’s account if they have passed away. Refuge is aware of cases where perpetrators have appointed themselves as legacy contacts and falsely informed Facebook that the survivor has died. Facebook have then refused to communicate with the survivor or accept that she is alive and help her regain access to the account. In addition, the accounts of murdered domestic abuse victims have not been closed by Facebook, because the introduction of Legacy Contacts has not been applied retroactively. This means that the bereaved families of murdered women continue to see posts shared, including birthday wishes, to their daughters’ accounts. We suggest that a simple process by which a family member or friend shares proof of death with the platform should suffice for the platform to close an account.</p> <p>As mentioned earlier in this submission, changes to reporting processes could also help to effectively reduce and prevent harm occurring. For example, users are often required to report every piece of harmful content individually. This can be retraumatising particularly given perpetrators will typically contact survivors repeatedly in multiple ways across different platforms. Allowing users to provide the username of a perpetrator, rather than reporting each piece of content individually, would help expedite the reporting process and reduce the risk of re-traumatisation.</p> <p>In addition, providers should develop and routinely promote user safety guidance. Safety guidance should include recommended steps to take if users suspect they are victims of tech abuse, as well as guidance on what support is available to them. Refuge has developed a suite of resources on identifying tech abuse and step-by-step guides to securing technology, as well as a dedicated website on tech abuse (https://refugetechsafety.org/).</p>
<p>Question 19: To what extent does your service encompass functionalities or features designed to mitigate the risk or impact of harm from illegal content?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>
<p>Question 20: How do you support the safety and wellbeing of your users as regards illegal content?</p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>

Question 21: How do you mitigate any risks posed by the design of algorithms that support the function of your service (e.g. search engines, or social and content recommender systems), with reference to illegal content specifically?	<i>Is this response confidential? – Y / N (delete as appropriate)</i>
Question 22: What age assurance and age verification technologies are available to platforms, and what is the impact and cost of using them?	<i>Is this response confidential? – Y / N (delete as appropriate)</i>
Question 23: Can you identify factors which might indicate that a service is likely to attract child users?	<i>Is this response confidential? – Y / N (delete as appropriate)</i>
Question 24: Does your service use any age assurance or age verification tools or related technologies to verify or estimate the age of users?	<i>Is this response confidential? – Y / N (delete as appropriate)</i>
Question 25: If it is not possible for children to access your service, or a part of it, how do you ensure this?	<i>Is this response confidential? – Y / N (delete as appropriate)</i>
Question 26: What information do you have about	<i>Is this response confidential? – Y / N (delete as appropriate)</i>


<p>the age of your users?</p>	
<p>Question 27: For purposes of transparency, what type of information is useful/not useful? Why?</p>	<p><i>Is this response confidential? – Y/ N (delete as appropriate)</i></p> <p>The Bill requires providers to produce information on their service, which may include 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 Ofcom. This will be welcome information, but specific data on online violence against women and girls must also be collected and published as part of the transparency reporting process. We support the recommendation made by a wide coalition of organisations in the ‘VAWG Principles for the Online Safety Bill’ for transparency reporting to include a separate VAWG category.¹⁴ As part of the annual transparency reporting process, providers should be required to specifically compile, report, and publish information on:</p> <ul style="list-style-type: none"> • The prevalence and different forms of tech abuse, and other forms of online violence against women and girls, occurring on the platform, including emerging types of abuse. • The actions taken by the platform in response to this content. For example, the percentage and number of content take-downs, complaints, appeals processes, sanctions imposed, and the time taken to review, and action reported content. • The above 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. • All transparency reports should be made publicly available. <p>Providing the above information will help improve accountability, and highlight weaknesses in content reporting systems, design features and functionalities, which would support Ofcom to identify and act on poor practice. The collection of VAWG-specific data would also support the early identification of emerging forms of VAWG and changing patterns of harms perpetrated against women and girls. As well as providing vital information to Ofcom in its role as regulator, this data would be valuable to law enforcement and the specialist VAWG sector. Providers should also ensure data on trends is shared regularly with the specialist VAWG sector, and that clear communication channels are established to capture, and act on, intelligence gathered by the sector on patterns and trends.</p> <p>Providers must be more transparent about their content moderation and investment and resourcing in moderation, and transparency reporting should include a requirement related to this. User feedback and satisfaction should be also sought. In addition, we would recommend that Ofcom</p>

¹⁴ ‘VAWG Principles for the Online Safety Bill,’ (2021), a joint briefing produced by #NotYourPorn, Angelou Centre, Chayn, Dr Fiona Vera-Gray, End Violence Against Women Coalition, Faith & VAWG Coalition, Glitch, Imkaan, Professor Clare McGlynn, Rape Crisis England & Wales, Refuge, Welsh Women’s Aid, Women & Girls Network, Women’s Aid Federation of England, <https://www.endviolenceagainstwomen.org.uk/wp-content/uploads/Online-Safety-Bill-Full-Brief-final.pdf>

	<p>undertake research with users of online services who have experienced online VAWG in order to understand their experiences and make recommendations to platforms on how to improve practice.</p> <p>A potential unintended consequence of publishing data on VAWG is that perpetrators may be alerted to new ways to abuse. This may be mitigated by close attention to wording and the detail provided, for example on emerging forms of VAWG. Specialist VAWG sector organisations are also well placed to advise, with adequate remuneration provided for time and expertise. More detailed transparency information can then be provided directly to the regulator and shared with specialist VAWG organisations.</p> <p>Further recommendations on transparency can be found in ‘VAWG Principles for the Online Safety Bill.’¹⁵</p>
<p>Question 28: Other than those in this document, are you aware of other measures available for mitigating risk and harm from illegal content?</p>	<p><i>Is this response confidential? – Y/ N (delete as appropriate)</i></p> <p>Refuge would also recommend that Ofcom play a role in ensuring that providers work more closely with law enforcement in the investigation of criminal offences perpetrated online. Survivors supported by Refuge have suggested that links could be improved between the police and social media companies, for instance to expedite the collection of data and evidence to prosecute perpetrators. Many survivors who report tech abuse to the police tell us that their report was handled badly, as the survivor stories below highlight. Survivors say that abuse was not investigated adequately or taken seriously enough, and that it is often not understood within the context of domestic abuse. As mentioned earlier in this submission, some survivors have been advised by the police to come offline as a ‘solution’ to the abuse they are experiencing. An analysis of responses to our Unsocial Spaces survey suggests that there is a lack of police action following reports of online abuse, as the term most commonly used by respondents to describe the police response was “nothing.”¹⁶ To support an improved criminal justice response to tech abuse and VAWG, providers should be required to provide law enforcement with data and evidence to investigate and prosecute perpetrators.</p> <p><u>Survivor stories</u></p> <p><i>“I reported it to the police because it became too much. Their advice [was] to get rid of social media.”</i></p> <p><i>“They [online platforms] should obviously help with the evidence side of things, if there’s deleted messages they should be able to get that up.”</i></p> <p><i>“Everything was in his laptop, my Instagram my Facebook. He check[ed] basically everything on my mobile and my bank account. The police just told me you can delete him at first and I told the police, I don’t want to delete him, I just want to prove that he is (in the account) – he has control even</i></p>

¹⁵ See ‘VAWG Principles for the Online Safety Bill.’

¹⁶ Refuge (2021), Unsocial Spaces.



now and he has no right to control me. After that I just delete[d] him, and the next week the police call[ed] me and told me we can help you with Instagram - it was too late I [had] already deleted him.”

Please complete this form in full and return to OS-CFE@ofcom.org.uk