Suzy Lamplugh Trust submission to Online Safety Bill Committee

Suzy Lamplugh Trust has over 35 years' experience supporting victims of violence and aggression including stalking and harassment, as well as campaigning for better protections for victims in policy and law. Tackling online harms has been a central thread in our work, and we are therefore uniquely placed to comment on the Draft Online Safety Bill, which provides an important opportunity to achieve a safer society for all.

The Trust chairs the National Stalking Consortium, comprised of experts including specialist frontline stalking support services, who have seen an increase in online abuse in stalking cases with covid-19. The National Stalking Helpline has seen a 7% rise in social media abuse in stalking cases since the start of the pandemic, and 100% of cases involve some form of cyber abuse. Our report 'Cyber Safety at Work' in October 2020 also demonstrated a concerning escalation of online abuse since Covid-19, with a startling one third of participants currently experiencing cyber abuse at work.

Suzy Lamplugh Trust welcomes the draft Online Safety Bill and supports the government's manifesto commitment to make the UK the safest place in the world online while defending free expression. However, we are concerned that aspects of the Bill require strengthening, particularly regarding the responsibility of platform providers to monitor and prevent crime as well as the role of specialist support services. We make key recommendations related to the Bill's objectives, content in scope, services in scope and the role of Ofcom.

Overview

In its current form, the Bill fails to specifically address Violence Against Women and Girls in the legislation, meaning Bill does not address the harms that many women face on a daily basis. We are also concerned the is relying on secondary legislation to provide detail, which is as yet missing. It is therefore unclear to what extent the Bill will be an effective legislative tool for tackling online abuse, as it purportedly sets out to do.

- The Bill does not represent the disproportionate harm faced by women and girls online, and the ways in which misogyny and abuse online perpetuates violence against women and girls in wider society. Currently, there is no mention at all of gender-based harm within the Bill including stalking.
- Online VAWG must be included as a specific harm in the Bill. Whilst stalking and harassment are named as priority offences, if you do not situate these offences

within a VAWG framework you will fail to capture the full spectrum of incidents, motivations and behaviours that constitute these crimes.

- Online platforms frequently do not understand VAWG when it is reported to them, so it is vital that there is a code of practice in place to build this understanding of VAWG.
- This code needs to include recognition of repeated patterns of harmful behaviour such as stalking and harassment, by perpetrators across a multitude of platforms and directed at a multitude of victims, as well as establishing methods of information sharing between platforms and companies to better identify and manage perpetrators.
- Research shows that online abuse disproportionately impacts women of colour, disabled and LGBT+ people. A VAWG Code of Practice must be intersectional, recognising the multiple intersecting characteristics of women subjected to online VAWG and the harm it creates.
- Women and girls must be free to participate in the online and offline world without fear of violence.
- Too often, women receive advice from police that they should come offline as a response to the abuse they have received. This culture must change, starting with shifting the responsibility from the victim to come offline onto the platforms to mitigate risk and proactively respond to perpetrators within a defined timeframe.

Research

Cyberstalking

The Suzy Lamplugh Trust has found evidence of a rise in cyberstalking and online harassment as a result of the pandemic. Cyberstalking refers to using any form of online or digital technology to carry out fixated and obsessive behaviour (stalking) towards a victim. This includes all forms of social media and communications platforms, as well as technology that can be used on devices such as Apple Air Tags and phone tracking apps such as Find My Friends. Cyberstalking should be treated as seriously as offline stalking, with a consistent response to victims, whether the stalking takes place online or offline.

In our Cyber Safety at Work report as many as 12% of the respondents experiencing cyber abuse stated that it took the form of online sexual harassment or cyber-flashing. Alongside this, digitally enabled stalking was experienced by 11% of respondents. Online abuse can have detrimental effects on the victim. Among the victims of online abuse within our pilot study, 92% reported that this impacted their mental health. The findings of our report demonstrate the clear escalation of online harms and the increasingly blurred lines between work and home life as a result of the pandemic.

The National Stalking Helpline furthermore sees regular cases of cyber-flashing and revenge porn, with 100% of cases presenting to the Helpline now involving a cyber element. Threats to share intimate images or content of a sexual nature with the victim's place of work are common, potentially resulting job loss, causing economic issues for the family in question and potentially isolating the victim further. Furthermore, according to the Revenge Porn Helpline, there has been a rise in cases of revenge porn since Covid-19 and in sexploitation across a number of industries, notably in academia resulting in job losses and detrimental financial impact on victims. Our report, Unmasking Stalking: A Changing Landscape, found that both online and offline stalking have increased during the pandemic. However, the rise in online stalking behaviours appears to be greater overall, aligning with evidence documented by the National Stalking Helpline of an increase in cyberstalking during the pandemic.

Three-quarters of respondents (75%) confirmed that they experienced both online and offline behaviours, which likely compounds the trauma of being stalked. Online/digital stalking behaviours were slightly more commonly experienced by respondents whose experience of stalking started after the first lockdown, with 88% experiencing one or more online/digital behaviours. This compares with 85% of respondents whose experience of stalking started before the first lockdown.

Online Harmful behaviour at work

Since Covid-19, there has been a major increase in the number of online platforms being used as people isolate and work from home. Approximately half the UK working population were by definition lone workers at home after 23rd March 2020. A pilot study conducted by Suzy Lamplugh Trust found that this has prompted an escalation of online abuse. Key findings from our Cyber Safety at Work report highlighted that a startling one third of participants are currently experiencing online abuse at work. Of these victims, 83% state that the abuse has escalated over the period of the pandemic.

The report also found that the three platforms through which online abuse was overwhelmingly perpetrated were Facebook, at 40%, WhatsApp, at 36%, and Email, at 35%. This was focusing specifically on abuse experienced during a person's working day, we acknowledge that abuse is experienced across multiple platforms, including Instagram and Twitter.

Online dating

Suzy Lamplugh Trust seeks to promote personal safety at all times and has long advocated for safe internet use and following safety guideline whilst meeting people on dates. We have a history of working with organisations such as Match.com to provide safety advice for

users and draw attention to the abuse faced by some users on these services. Independent online research carried out by YouGov carried out on behalf of Suzy Lamplugh Trust and funded by dating service, Match.com, shows that nearly three quarters of online daters share personal information about themselves earlier than they would do in other situations.

This research also found that a third of online daters have experienced safety concerns when dating online and yet over half are never reported, amounting to potentially over a million concerns that dating agencies don't know about. In addition, our research shows that the majority of those who have had concerns for their safety simply block perpetrator profiles, with 15% of daters feeling their report would not be acted upon by the service provider, 12% saying there wasn't an easy way to report the concern on the dating website, and 7% feeling too embarrassed to report it.

We have urged all dating agencies to encourage and support their members to report all incidents and concerns and ensure that the mechanism for reporting is clear and easy to follow. This not only helps the individual involved, but may also safeguard other users, as online dating agencies can spot potential problems and act immediately to protect their members. We have called for online dating agencies to develop in-house expertise to deal with complaints around personal safety with specific advice from external specialists that are trained in dealing with cases of violence and abuse.

In addition, we have also advocated for online dating agencies working together in the industry to share information amongst each other about users who demonstrate abusive behaviour such as stalking, harassment or other forms of abuse and establish criteria for determining this. Customer reporting should always be made as easy as possible via email and/or phone.

Other online harmful behaviours

There is an abundance of research demonstrating the disproportionate harm faced by women and girls online. The 'Her Net Her Rights' report found that globally women are 27 times more likely to be harassed online than men. In Europe, 9 million girls have experienced cyber violence by the time they are 15 years old. Online VAWG can therefore be seen as part of a continuum of violence against women and girls and aims to maintain male domination in the digital sphere. Women and girls experience violence via the use of new technologies, including online harassment, stalking, sexist hate speech, cyber bullying, threats, impersonation, or non-consensual sharing of graphic contents.

New research carried out by the Victims Commissioner, Dame Vera Baird QC, found that typically people experienced multiple types of online abuse, with the average being 4.2

types of abuse. Women reported experiencing higher numbers of abuse, with an average of 4.4 harms for women vs 3.9 for men. In 12 of the 21 categories of online abuse, women reported higher levels of victimisation. Abuses such as intimate image abuse, cyber stalking and cyber flashing were significantly more likely to be experienced by women. The research found that online abuse could sometimes occur for many years. Victims of cyber stalking reported the longest time frames with 40% of victims reporting experiencing the abuse for more than 2 years.

The report also found that whilst reporting levels were high, with 62% of respondents reporting to either the police or internet companies, dissatisfaction with that reporting was also high. 65% of people who reported to the internet companies and 55% of people who reported to the police dissatisfied with their experience of reporting.

A recent Ofcom report found that women are less confident about their online safety than men and are more affected by discriminatory, hateful and trolling content. The report found that, in the previous four weeks, women who went online were more likely than men to have seen or experienced content relating to negative body image (9% vs. 6%), misogynistic content (9% vs. 7%) and content relating to self-harm or suicide (4% vs. 2%).

Women were found to be more negatively affected by the harmful content they encounter. Women aged 18-34 were more likely than any other group to disagree with the statement that "being online has a positive effect on my mental health" (23% vs. 14% for the average UK adult, and 12% of men). Notably, nearly a quarter (23%) of Black women also disagreed with this statement, higher than white women (16%) and Asian women (12%). Consequently, women feel less able to have a voice and share opinions online.

Proposed amendments

We propose the following amendments be made to the Online Safety Bill to better ensure the protection of women and girls from online abuse.

(1) "Online Violence Against Women and Girls Offences" should be added as a "Relevant Offence" cl 52(4) with an additional schedule in the bill alongside schedule 5 ("Terrorism Offences") and schedule 6 ("Child Sexual Exploitation and Abuse Offences"). With supporting obligations for Ofcom to produce Codes of Practice for VAWG.

We strongly recommend that violence against women and girls is named within the Bill as a priority harm within Schedule 7. This should draw on the Istanbul Convention definition of

VAWG, the gold standard treaty for combating gender-based violence that the government has recently agreed to ratify. There is currently no mention of gender or sex in the Bill, instead attempting to address VAWG through the list of priority illegal content in Schedule 7. Whilst we welcome the inclusion of harassment and stalking within this list, in the absence of a VAWG framework, we risk missing the nuances of stalking including the motivations and behaviours that underpin these crimes. Having not consulted with VAWG organisations about the definitions, we do not feel that in its current form the Bill will adequately address the nuances of these crimes and the breadth of practices and behaviours that make up VAWG.

The Bill is misguided in adopting a gender-neutral approach, in which VAWG is likely to be addressed only in a narrow and limiting way. Currently, the requirements placed on tech companies have been reduced by only addressing certain content and behaviours listed in the Schedule 7 offences and other illegal content.

We welcome changes made to the Online Safety Bill that set out priority offences, including stalking, in primary legislation within the Bill. These offences represent the most serious and prevalent illegal content an activity online and will require companies to take proactive steps to tackle such content. Companies will need to design and operate their services to be safe by design and prevent users encountering illegal content. However, currently these priority offences are not defined within the legislation, so it is unclear how each will be legislated for. The definition of harmful conduct must be further developed via the VAWG Code of Practice.

Suzy Lamplugh Trust supports the VAWG Code of Practice that has been developed by the EVAW coalition to be included in the Bill as it recognises the gendered nature of abuse online. We therefore also support amending clause 37 of the Bill to introduce a VAWG Code of Practice. If enacted, online VAWG would be taken seriously, with stricter actions taken by the regulatory body Ofcom.

(2) Clause 8, page 7, line 14, at end insert— "(h) how the service may be used in conjunction with other regulated user-to-user services such that it may— (i) enable users to encounter illegal content on other regulated user-to-user services, and (ii) constitute part of a pathway to harm to individuals who are users of the service, in particular in relation to CSEA content."

This amendment would incorporate into the duties a requirement to consider cross-platform risk. While welcoming requirements for transparency reporting, the Trust is concerned that reporting criteria focuses too narrowly on incidence and systems/processes.

We are concerned that currently the Bill does not require user-to-user services to share information about concerning users or patterns of behaviour perpetuated by individuals. We know that perpetrators use multiple platforms to target and harass multiple victims, and that's why we need information sharing across platforms to identify this behaviour.

Suzy Lamplugh Trust defines stalking as a pattern of fixated and obsessive behaviour which is repeated, persistent, intrusive and causes fear of violence or engenders alarm and distress in the victim. On the National Stalking Helpline we see that it is common for perpetrators to use multiple platforms to inflict abuse on victims. Often one incident is part of a wider pattern of behaviour that escalates into violence and aggression. This was particularly prevalent in the case of Matthew Hardy, labelled 'Britain's worst cyberstalker', who stalked multiple women online for over a decade. Whilst it is hard to know the true extent of the abuse, one force alone, Cheshire constabulary, was contacted about Hardy more than 100 times by 62 victims over an 11-period. Hardy used victim's social media accounts, created fake accounts in their name, pose as the victim to have sexual explicit conversations and send stolen intimate photographs. If platforms had worked together to identify this pattern of behaviour across multiple accounts and platforms, reporting incidents of abuse would have been an effective way of tackling these crimes.

It is therefore imperative that platforms ensure responses to incidents and common patterns of abusive behaviour are collated and used for improvement across multiple services. Platforms must amend user terms and conditions across the board to enable sharing of information across sites where a personal safety issue has been flagged. Crucially, reporting must be accessible, and victim centred by design.

We recommend reports increase transparency by also including information on how service providers have dealt with complaints and acted to support victims of online harms, including signposting to specialist services. Service providers must report on cases in detail to ensure victims are receiving the support they need, and that providers act to tighten up their procedures according to the risks identified. When including cases in transparency reporting, services providers must anonymise the cases. If a service provider is made aware of misuse of its platform for illegal behaviours such as stalking and harassment, they must provide information about perpetrators, where known, in order to assist in criminal investigations. Transparency reporting must include detail on complaints and actions taken, including signposting to specialist services. Signposting should be made to key specialist services relating to VAWG, such as the National Stalking Helpline, with training provided for those doing the signposting.

(3) Clause 12, page 12, line 10, at end insert— "(4A) A duty to publish the adults' risk assessment and proactively supply this to OFCOM."

This amendment creates a duty to publish the adults' risk assessment and supply it to OFCOM. We need to see more detail about how service providers will be required to show they are actively trying to understand the harm that is being caused on their platforms. Platforms should be required to undertake research to assess the risk posed to their clientele. Platforms should provide risk assessments on their users, giving specific attention to minoritised groups, and work with specialist support services to understand what that risk is. More detail on how the regulator will require platforms to show their risk analysis is necessary as if risk analysis is purely based on complaints made this will not be sufficient in protecting people from online harms. In carrying out risk assessments, platforms must work proactively with specialists where necessary, including specialist services, to prevent future harm

More detail on risk assessments must be provided, including how service providers will show they are actively trying to understand and mitigate the harm that is being caused on their platforms, working with specialists where necessary.

Further Recommendation: The Role of Ofcom

(1) Transparency and accountability

With reference to Part 6, clause 111.

Need for independent expert advisory panel

We welcome the duty on service providers to ensure users and affected persons can easily report illegal or harmful content, however we believe the duty requires further detail in primary legislation and codes of practice. Platforms must ensure reports are dealt with by professionals who have the knowledge and skills to sensitively handle complaints and signpost to specialist victim support services depending on the harms experienced. We would further recommend that platforms develop ongoing partnerships with independent specialised services that address specific types of abuse, as well as statutory services such as the police.

The Bill's provisions for an advisory committee to Ofcom do not go far enough to promote transparency or accountability. The Bill must specify the appointment of an independent expert advisory panel from interested groups and specialist support services, as well as

independent online safety experts, which will scrutinise the work of the regulator and ensure that codes of practice are developed and adhered to robustly. The panel should spot-check cases and assess for the impact and proportionality of the regulator's work. This should include seeking evidence from parliamentary bodies as well as user and civil society groups.

The Bill must specify the appointment of an independent expert advisory panel to scrutinise the work of the regulator.

(2) Training for Ofcom and collaboration with specialist services

Ofcom should be trained in safeguarding and personal safety to ensure they can appropriately carry out their regulatory role, receive complaints and respond to super-complaints. This should include training on all forms of violence, aggression and intimidation, including harassment, stalking, cyber bullying, hate crime, as well as discrimination based on personal characteristics, such as gender, race, age, and sexuality.

A report published by Suzy Lamplugh Trust for National Stalking Awareness Week 2021 on 'Unmasking Stalking: A Changing Landscape' highlighted the rise in online stalking behaviours during COVID-19. 82% of victims whose experience of being stalked started during the pandemic have experienced stalking behaviours via social networking sites. Some of the most common online/digital stalking behaviours for survey respondents where stalking started after the first lockdown were social networking sites (82%), online third-party contact (65%) and threats via digital communication (47%). The report found that less than two-thirds (63%) of all survey respondents indicated that they had reported stalking to the police in the UK. When respondents explained why they had not reported, the answers highlighted a concerning lack of trust in the police and wider criminal justice system. These findings alone show the necessity in signposting other avenues of more specialist service support. It is common within cases of stalking for victims to be unaware of a swathe of stalking behaviours being perpetrated against them, especially when it comes to online harms such as hacking and tracking devices. Therefore, ensuring that specialist services who are trained in stalking and other harmful/illegal behaviours are signposted for users is vital to appropriately support victims who are often traumatised by their experience.

Ofcom must be trained in safeguarding and personal safety, as well as discrimination based on personal characteristics.

(3) Enforcement

We are calling for the establishment of Ofcom to have the authority to issue licences, impose requirements, restrictions, and conditions, set standards and secure compliance and enforcement. Ofcom should be given statutory power to enforce the VAWG Code of Practice through the Online Safety Bill**.** These standards should be subject to a statutory consultation requirement requiring expert advice. Penalties should include fines and the revoking of licences of those providers who fail to comply with basic requirements, conditions and standards as set by the regulatory body. The regulatory body should be responsible for the overall oversight of this industry, to ensure robust implementation of standards and penalties for failure to comply.