DRAFT ONLINE SAFETY BILL: WRITTEN EVIDENCE SUBMITTED BY SUZY LAMPLUGH TRUST

November 2021

LIVE
LIFE
SAFE
suzy lamplugh
trust

Introduction and key recommendations

Suzy Lamplugh Trust has over 30 years' experience supporting victims of violence, 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 runs the National Stalking Consortium, comprised of several frontline stalking support services, who have seen an increase in online abuse in stalking cases with covid-19. The National Stalking Helpline shows a 7% rise in social media abuse in stalking cases, and 100% of cases involve some form of cyber abuse. Our recent 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 role of specialist support services. We make key recommendations as related to the Bill's objectives, content in scope, services in scope and the role of Ofcom.

Key recommendations:

Objectives

1.1.1 Transparency reporting must include detail on complaints and actions taken, including signposting to specialist services.

1.1.2 Transparency reporting must include thematic reporting to understand intersectional harms.

1.2.1 Reporting and redress duties must ensure complaints are handled by trained professionals with users signposted to specialist services.

1.2.2 Reporting and redress duties must ensure users are encouraged to report concerns to platform, as well as police where illegal content.

1.2.3 Reporting and redress duties must ensure perpetrators profiles/accounts are removed from the platform, with a mechanism to ensure perpetrators cannot sign on with new name.

1.2.4 Reporting and redress duties must ensure service providers assist with any criminal investigation where the platform has been misused for illegal behaviours.

1.2.5 Reporting and redress duties must ensure responses to incidents and common patterns of abusive behaviour are collated and used for improvement.

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

Content in Scope

2.1.1 The definition of harmful conduct must be further developed via codes of practice.

2.1.2 Interest groups and specialist services must have the opportunity to feed into definitions/decision-making on what is included as harmful and priority harmful content.

Services in Scope

3.1.1 The regulator must consult with interest groups and specialist services when researching category threshold conditions and when establishing/maintaining the register.

The Role of Ofcom
4.1.1 The Bill must specify the appointment of an independent expert advisory panel to scrutinise the work of the regulator.
4.2.1 Ofcom must be trained in safeguarding and personal safety, as well as discrimination based on personal characteristics.

Full Response

1. Objectives

1.1 Transparency Reports

With reference to Part 3, Chapter 1, clause 49

1.1.1 Detailed case studies

While welcoming requirements for transparency reporting, the Trust is concerned that reporting criteria focuses too narrowly on incidence and systems/processes. We recommend transparency reports also include 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.

Recommendation 1.1.1 Transparency reporting must include detail on complaints and actions taken, including signposting to specialist services.

1.1.2 Thematic reporting

Thematic areas of reporting would also be useful to better understand how harms are affecting vulnerable and marginalised groups. An intersectional approach is important in understanding the harms groups of people face online according to gender, race, age, sexuality etc. For example, three quarters of respondents to our Cyber Safety at Work survey felt that the online abuse was targeted on their personal characteristics: 36% felt they were singled out based on their gender, 33% based on their race and 33% on their age. Furthermore, online sexual harassment or cyberflashing constituted 12% of the abuse experienced.

Recommendation 1.1.2 Transparency reporting must include thematic reporting to understand intersectional harms.

1.2 Reporting and redress duties

With reference to Part 2, Chapter 2, clause 15 & Chapter 3, clause 24

1.2.1 Handling of complaints and specialist support services

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.

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 often traumatised victims.

Recommendation 1.2.1 Reporting and redress duties must ensure complaints are handled by trained professionals with users signposted to specialist services.

1.2.2 Encouraging users to report

Service providers should also encourage users to report incidents and concerns to the platform, as well as to report illegal content to the police. Research carried out in 2017 by independent online researchers YouGov2 on behalf of the Suzy Lamplugh Trust and funded by dating service, Match, found that a third of online daters have been concerned for their personal safety when communicating online (32%) or on meeting (37%) potential partners from a dating website or app. However, over half (56%) of those who have been concerned have never reported the incident to the dating provider.

Recommendation 1.2.2 Reporting and redress duties must ensure users are encouraged to report concerns to platform, as well as police where illegal content.

1.2.3 Removing perpetrator profiles/accounts

If a perpetrator's profile has been removed from the platform following abusive behaviours, any further profiles/accounts made by them should be removed. A mechanism must be in place to ensure perpetrators cannot sign on with new name. Platforms should investigate whether an individual or profile removed for serious unacceptable behaviour has been in contact with others on the service and might pose some threat to the safety of these other users.

Recommendation 1.2.3 Reporting and redress duties must ensure perpetrators profiles/accounts are removed from the platform, with a mechanism to ensure perpetrators cannot sign on with a new name.

1.2.4 Assisting criminal investigations

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 investigation. This could be detailed in the relevant code of practice.

Recommendation 1.2.4 Reporting and redress duties must ensure service providers assist with any criminal investigation where the platform has been misused for illegal behaviours.

1.2.5 Monitoring of reporting for improvement

Monitoring of reporting times, responses to incidents and common patterns of abusive behaviour should be collated and used for improvement.

Recommendation 1.2.5 Reporting and redress duties must ensure responses to incidents and common patterns of abusive behaviour are collated and used for improvement.

1.3 Risk Assessment Duties

With reference to Part 2, Chapter 2, Clause 7

1.3.1 Detail on risk assessment

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 test the impact. 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 with specialists where necessary, including specialist services.

Recommendation 1.3.1 More detail on risk assessments must be provided, including how service providers will show they are actively trying to understand the harm that is being caused on their platforms, working with specialists where necessary.

2. Content in scope

2.1. Harmful Material

With reference to Part 2, Chapter 6, clauses 45-47

2.1.1 Detailed guidance on harmful content

Despite general definitions of harmful content included in the Bill, we are concerned these definitions are not sufficiently detailed to guide service providers in assessing risk of harm. We propose that detailed guidance be developed via codes of practice, including examples of harmful content.

Recommendation 2.1.1 The definition of harmful conduct must be further developed via codes of practice.

2.1.2 Consulting with interest groups/specialist services on harmful material

More information is required on decision making as to what is included as harmful but legal material. It is also imperative that interest groups and other specialist services have the opportunity to feed into definitions and decision-making on harmful content, particularly with relation to content affecting groups or people with certain characteristics. In particular, interest groups and other specialist services must have ample opportunity to feed into Ofcom's advice to the Secretary of State on priority harmful content and subsequent regulations designating priority harmful content. Interest groups and specialist services must also have the option to feed into Ofcom's 3-year review reports on the regulations, and to bring evidence to inform decision-makers about legal but harmful behaviour that comes to their attention.

Recommendation 2.1.2 Interest groups and specialist services must have the opportunity to feed into definitions/decision-making on what is included as harmful and priority harmful content.

3. Services in scope

3.1 Category recommendations

With reference to Part 4, Chapter 2, 59-60 and Schedule 4

3.1.1 Consulting with interest groups/specialist services on category recommendations

Suzy Lamplugh Trust is concerned about the implications of incorrectly categorising service providers or missing relevant service providers from the register from a risk-management perspective. The Trust is particularly concerned that service providers may be inadvertently missed from Category 1. To mitigate this risk, in assessing services, the regulator should consult with specialist services and interest groups when establishing and maintaining the register to ensure all platforms are included under the appropriate category. We also recommend specialist services have the opportunity to feed into the specification and making of category threshold regulations by the Secretary of State. Specifically, Ofcom must consult with specialist services and interest groups when conducting their research on category thresholds conditions.

Recommendation 3.1.1 The regulator must consult with interest groups and specialist services when researching category threshold conditions and when establishing/maintaining the register.

4. The role of Ofcom

4.1 Transparency and accountability

With reference to Part 6, clause 111.

4.1.1 Need for independent expert advisory panel

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 interest group 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.

Recommendation 4.1.1 The Bill must specify the appointment of an independent expert advisory panel to scrutinise the work of the regulator.

4.2 Training

With reference to Part 4

4.2.1 Training for Ofcom

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.

Recommendation 4.2.1 Ofcom must be trained in safeguarding and personal safety, as well as discrimination based on personal characteristics.