UCL

TECH ABUSE

Protecting people from Illegal Harms Online
Ofcom Consultation

Written Submission
UCL Gender and Tech Research Group

February 2024

Dr Leonie Tanczer, Jennifer Reed, Kyle Beadle PHD

Covering Note

1. **The size and format of this consultation is likely to create barriers for civil society organisations and individuals - preventing them from fully engaging**. This must be addressed for all future consultations if meaningful engagement is to be delivered. Of particular concern is how domestic abuse organisations will be able to feed in to the future consultation (scheduled for 2025) where they can offer significant expertise and input, if an artificial barrier is effectively put in place by publication of over 1500 pages to read through – this is not feasible.

2. **Overall, there is a heavy focus on processes and take down of content. There is a risk that this becomes a 'tick box' risk exercise** with services not meaningfully understanding or considering what more they can actually do to actively prevent the crimes occurring in the first place. Illegal harms can be devastating for individuals affected, and **more onus on prevention** and taking serious action to tackle harms would be welcome – to complement the efforts on takedown. We expand on this in our response.

3. **There does not seem to be a sufficient focus on action which will support marginalised groups**, or those at increased risk of facing illegal harm – including women and girls. It is important to recognise that harms surface in different ways for some users, and additional or tailored measures may be necessary. These proposals include some specifics, such as for CSAM and Fraud – but nothing for victim-survivors of domestic abuse, or women and girls more broadly. At current, **if these proposals are implemented as they stand, our concern is that the dial would not significantly shift in terms of how technology is used to abuse women and girls**.

Volume 2 – The causes and impacts of online harm.

Q1. Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?

Response:

General

Illegal harms are indeed widespread, growing in prevalence, and more likely to affect individuals with protected characteristics – such as women and girls. There is also evidence that certain groups face a particular risk of exposure to illegal harm, including children[1].

It is also true that the impact of online harms can be extremely severe and deeply affect people's lives – both online and offline. Our research has shown that individuals who have received offensive or threatening messages are 5.49 times more likely to have had suicidal thoughts[2]. We also know that technology-facilitated intimate partner violence is now a significant factor in the majority of domestic abuse cases in England and Wales[3], of which there are 1.5 million every single year (true figures likely to be much higher). Technology-enabled harms also feature in a considerable number of domestic homicides.

We also agree that illegal harm occurs on services of all types, not just mainstream or large platforms. For example, perpetrators of domestic abuse have used **online banking platforms as a communication channel by '*1p ing*' – transferring pennies into the victim's/survivor's bank account to leave messages in the reference notes, to maintain (unwanted) contact, and to continue their harassment**[4].

Functionalities

We believe **hidden and 'mundane' features** must be accounted for when considering 'functionalities' that pose risks.

[1] Safeguarding patients from technology-facilitated abuse in clinical settings: A narrative review. Straw, Tanczer. 2023. Link here.

[2] Receiving threatening or obscene messages from a partner and mental health, self-harm and suicidality: Results from the Adult Psychiatry Morbidity Survey. McManus, Bebbington, Tanczer, Scott, Howard. 2021. Link here.

[3] Select Committee Inquiry. Connected Tech: Smart or Sinister? 2023. Link here.

[4] I feel like we're really behind the game: Perspectives of the United Kingdom's Intimate Partner Violence support sector on the rise of technology-facilitated abuse. Tanczer, Lopez-Neira, Parkin. 2021. Link here.

Perpetrators of domestic abuse – especially in heterosexual relationships – tend to be those who purchase (U2U) gadgets, set up and maintain online accounts or profiles, and generally feel more ‘tech-savvy’, which means they perceive to understand better how devices and services work. Perpetrators take advantage of this power and knowledge imbalance, which enables them to control, coerce, intimidate, harass or otherwise abuse their victims/survivors – often by underplaying or overexaggerating what digital systems can do[5].

For example, if a perpetrator controls the settings of digital systems used within a home, they can add new products and services to existing ones (e.g., such as smart speakers) enabling them to stalk their victims/survivors. Perpetrators may also use ‘stalkerware’ or ‘spyware’ which does not alert their victim/survivor to the fact that this type of app has been downloaded onto their phone (or this can be easily hidden in settings)[6]. Some perpetrators have also used services which have GPS functionality embedded in them to locate the victim/survivor when they have sought to escape an abusive relationship. These issues could extend to many U2U services in scope (e.g., Strava).

In most of these instances, the perpetrators are usually within the ‘home’ or have at one point been part of the ‘network’ of the individual they are harming – they may know passwords or be connected via shared devices. **This risk vector and threat models must be considered**[7] – not just ‘bad actors using large and small services to spread illegal content.’ **This will be particularly important for illegal harms, including harassment and stalking**. Services assessing and managing this risk better could, as a result, make improved use of frequent notifications to users about setting changes or devices they are still connected to[8].

Q2. Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.

Response:

[5] The UK Code of Practice for Consumer IoT Cybersecurity: Where we are and what next. Burton, Tanczer, Vasudevan, Carr. 2021. Link here.

[6] Mapping the State of Knowledge on the Use of Stalkerware in Intimate Partner Violence. Tomás Bermudez, Maddalena Esposito, and Jay Neuner. 2020. Link here.

[7] Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. Slupska, Tanczer. 2021. Link here.

[8] Safeguarding the “Internet of Things” for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design. Brown, Harkin, Tanczer. 2024. Link here.

We agree that online harms and risk factors are changing constantly as technology and society evolve.

Within the context of domestic abuse, many of the behaviours we see such as stalking, harassment, coercive and controlling behaviour – are not new. However, emerging technologies and online services present a new means by which those behaviours can manifest. They extend the reach of the perpetrator and remove the need for them to be physically present to commit their crime. Often, the service will have been maliciously repurposed from its original use, for example, an A/V baby monitor can be used to watch or get images of a victim/survivor unknowingly[9].

Such risk factors must accounted for right from the inception and development of new services or products. Only then, can the ability of services to be (mis)used for harmful activities be 'designed out' from the very beginning.

To achieve this, services could undertake **'abuseability' testing** to explore how their services and products could potentially be misused and repurposed. Additionally, safety-by-design approaches which are harm-preventative methods that anticipate risks and exploitative usage patterns must be deployed. Identifying potential tech-enabled threats in this way could help prevent illegal content appearing in the first place and complement efforts around takedown and removal[10].

Volume 3

Q7. Do you agree with our proposals?

Response:

It is critical that U2U and search services understand the harms fully and properly assess risk. This requires them to track how those harms surface and manifest.

Where risk profiles and other primary mechanisms are not able to provide services with a sufficiently good understanding of their risk levels, Ofcom will recommend services to look at additional evidence – including the views of,

[9] Technology-Facilitated Abuse and the Internet of Things (IoT): The Implication of the Smart, Internet-Connected Devices on Domestic Violence and Abuse. Tanczer. 2023. Link here.

[10] Safeguarding the "Internet of Things" for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design. Brown, Harkin, Tanczer 2024. Link here.

(i) **Independent experts and external research**. Academics and researchers have an important role to play here and can offer a wide array of expertise and evidence related to illegal harms. However, organisations seeking to engage experts or researchers for the first time may benefit from support on navigating the landscape, which could be signposted from Ofcom. This could include a research database or specific policy briefings, to provide additional guidance and access to relevant and up to date material – as well as signposting.

(ii) **Consultation with users or engagement with relevant representative groups**. Consulting with user groups can be complex, especially given that the harms cover highly sensitive, criminal issues. If an organisation were seeking to engage users who had experienced stalking through a U2U or search service, for example, we would expect there to be stringent approvals and protections in place to ensure the engagement was ethical. This is a benchmark that Ofcom could set. When engaging relevant representative groups, it must be recognised that many work on a charitable basis or under considerable resource constraints. They may have understandable limitations on how feasibly they can engage with services (particularly if they are receiving multiple requests following the implementation of the Act.) For example, frontline domestic abuse organisations see technology-enabled abuse surfacing in a myriad of ways through the individuals they support, but they may not always be resourced to engage with organisations – particularly on complex risk considerations for specific services. Ofcom could consider how to engage these voices strategically. Ofcom should also consider, related to enforcement activity, what they deem appropriate should organisations 'seek' the views of representative groups and fail to secure them – what is acceptable bounds here in terms of effort and input.

Volume 4: What should services do to mitigate the risk of online harms.

Q12. Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?

Response:

We agree that U2U services should prepare and apply a transparent "policy about the prioritisation of content for review."

This policy should include **measures of hidden coercion**[11] among users in addition to the "virality of content, potential severity of content, and the likelihood that content is illegal, including whether it has been flagged by a trusted flagger." **Our forthcoming work**[12] on coercion in online, LGBTQ+ communities reveals that users abuse platform features such as downvotes, mentions and replies to enforce conformity of gender and sexual expression. In other words, negative reactions to user content, which are not currently moderated by U2U services, negatively impact the experiences of LGBTQ+ users as they seek to conform to what is seen as "normal" LGBTQ+ expression among their online peers.

Ofcom should further consider including the voices of marginalized and vulnerable populations when considering what they deem the priority factors of content for review.

Q16. Do you have any comments on the draft codes of practice themselves?

Response:

The Act requires U2U and search services to have an easy-to-use complaints process. We would encourage services to include 'offline' options, such as a telephone number or the ability to submit written complaints, in addition to the digital process.

This would offer a route of escalation to individuals who,

- Have submitted their devices (phones, tablets, or other digital systems) to the police as evidence in a case which involves illegal harms, such as stalking or harassment cases, and may not have means to follow a digital process or receive email updates easily. At current, there is no guidance in the U.K about when the police must return phones[13] or other devices in these instances.
- Have had 'stalkerware' or 'spyware' installed on their phone (such as within an abusive and controlling intimate partner relationship) and are unable to access online support.

We agree with Ofcom's position that dedicated reporting channels could be used to address a wide range of harms, beyond just fraud. For example, domestic abuse services and police acting as trusted flaggers for individuals seeking support in relation to stalking or harassment, where there is a clear link to illegal content.

[11] Hidden coercion falls under the definition of digital coercion

[12] When published will be listed on https://kylebeadle.com – theoretical work available Here - Google Scholar, Kyle Beadle

[13] Policing Technology-Facilitated Domestic Abuse (TFDA): Views of Service Providers in Australia and the United Kingdom. Douglas, Tanczer, Mclaghlan, Harris. 2023. Link here.

We would welcome comment around whether an additional dedicated channel for women and girls facing domestic abuse or other forms of gender-based violence, could be explored ahead of the 2025 consultation.

Q18. Do you agree with our proposals? (Content moderation)

Response:

See response to question 12.1

Q20. Do you agree with our proposals? (Automated content moderation (User to User)

Response:

See response to Q12.1

ENDS.

For Further Information & Contact Details for UCL Gender and Tech Research Group please visit please visit our webpage here.