Your response

Volume 2: The causes and impacts of online harm

Ofcom's Register of Risks

Question 1:	
i)	Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?

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.

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

[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

[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.

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].

ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 2:	
i)	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: 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

[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.

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].

ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

[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.

Volume 3: How should services assess the risk of online harms?

Governance and accountability

Question 3:	
i)	Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice?
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 4:	
i)	Do you agree with the types of services that we propose the governance and accountability measures should apply to?
Response:	
ii)	Please explain your answer.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 5:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 6:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Service's risk assessment

Question 7:	
i)	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,

(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.

ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Specifically, we would also appreciate evidence from regulated services on the following:

Question 8:	
i)	Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 9:	
i)	Are the Risk Profiles sufficiently clear?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
Response:	
iv)	Please provide the underlying arguments and evidence that support your views.
Response:	
v)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 11:	
i)	Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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

Our approach to the Illegal content Codes of Practice

Question 12:	
i)	Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?
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.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 13:	
i)	Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 14:	
i)	Do you agree with our definition of large services?

[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

Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 15:	
i)	Do you agree with our definition of multi-risk services?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 16:	
i)	Do you have any comments on the draft Codes of Practice themselves?

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.

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.

ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 17:	
i)	Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?
Response:	

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

ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Content moderation (User to User)

Question 18:	
i)	Do you agree with our proposals?
Response: Please see response to question 12.1	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Content moderation (Search)

Question 19:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Automated content moderation (User to User)

Question 20:	
i)	Do you agree with our proposals?
Response: See response to question 12.1	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 21:	
i)	Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Do you have any relevant evidence on:

Question 22:	
i)	Accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 23:	
i)	Ability of services in scope of the CSAM hash matching measure to access hash databases/services, with respect to access criteria or requirements set by database and/or hash matching service providers;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 24:	
i)	Costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching for CSAM URL detection;;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 25:	
i)	Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 26:	
i)	An effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and any information you have on the costs and efficacy of applying hash matching and URL detection for terrorism content to a range of services.
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

User reporting and complaints (U2U and search)

Question 28:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Terms of service and Publicly Available Statements

Question 29:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 30:	
i)	Do you have any evidence, in particular on the use of prompts, to guide further work in this area?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Default settings and user support for child users (U2U)

Question 31:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 32:	
i)	Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

Question 33:	
i)	Are there other points within the user journey where under 18s should be informed of the risk of illegal content?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Recommender system testing (U2U)

Question 34:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 35:	
i)	What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive.

Question 36:	
i)	Are you aware of any other design parameters and choices that are proven to improve user safety?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Enhanced user control (U2U)

Question 37:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 38:	
i)	Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 39:	
i)	Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

User access to services (U2U)

Question 40:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically:

Question 41:	
i)	What are the options available to block and prevent a user from returning to a service (e.g. blocking by username, email or IP address, or a combination of factors)?
Response:	
ii)	What are the advantages and disadvantages of the different options, including any potential impact on other users?
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 42:	
i)	How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

There is a risk that lawful content is erroneously classified as CSAM by automated systems, which may impact on the rights of law-abiding users.

Question 43:	
i)	What steps can services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Cumulative Assessment

Question 45:	
i)	Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 46:	
i)	Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
Response:	

ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Statutory Tests

Question 48:	
i)	Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Volume 5: How to judge whether content is illegal or not?

The Illegal Content Judgements Guidance (ICJG)

Question 49:	
i)	Do you agree with our proposals, including the detail of the drafting?
Response:	
ii)	What are the underlying arguments and evidence that inform your view?
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 51:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Volume 6: Information gathering and enforcement powers, and approach to supervision.

Information powers

Question 52:	
i)	Do you have any comments on our proposed approach to information gathering powers under the Online Safety Act?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Annex 13: Impact Assessments

Question 54:	
i)	Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?
Response:	
ii)	If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	