

Your response

Question (Volume 2)	Your response
<p>Question 6.1:</p> <p>Do you have any comments on Ofcom's assessment of the causes and impacts of online harms? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.</p>	<p><i>No</i></p> <p>The Online Safety Act presents a crucial opportunity to protect women and girls from online abuse. As quoted in the consultation, women and girls are 27 times more likely to experience abuse online than men. The National Stalking Helpline furthermore sees incidents of cyber-flashing and revenge porn as part of a wider pattern of stalking, with 100% of cases presenting to the Helpline now involving a cyber element. Our report, <i>Unmasking Stalking: A Changing Landscape</i>, 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.</p> <p>We therefore welcome the inclusion of stalking as a priority illegal offence within the legislation, and, indeed, much of the framing of the harm and impacts of cyberstalking laid out in Volume 2 are true and representative of the victims we support. However, there is a need to situate these offences within the wider continuum of Violence Against Women and Girls (VAWG) behaviours. We understand that the societal harms related to online VAWG will be considered in the forthcoming VAWG guidance, however it remains the case that this is not adequately addressed in this consultation. There is a consideration of wider societal harms in relation to hate speech for example, and online VAWG deserves the same level of parity. Given that Ofcom acknowledges that women and girls are more likely to be targeted on the internet as a result of their gender, we'd expect the consultation to request evidence from companies that associated risks for women and girls are being mitigated.</p> <p>We welcome acknowledgements within the guidance of the way user networking – such as user tagging</p>

Question (Volume 2)	Your response
	<p>and connections, and user communication – such as livestreaming, direct messaging, posting and reposting content – can compound the risks of stalking on user-to-user sites. However, in Vol 2 the section on cyberstalking concludes that “No specific evidence was found on how business models may influence risks of harm to individuals for this offence.” This neglects to take into account that most sites accounts will be set to ‘public’ by default instead of ‘private’, which facilitates a greater amount of information being publicly accessible to perpetrators. Design features such as the ones referenced above quite clearly influence the risk of harm of this offence. This is more evidence that while the analysis of the risks and harms might be comprehensive (set out in Vol 2), the mitigation measures proposed in the codes are minimalist, showing the low intervention approach being taken by Ofcom.</p> <p>Under sections 6E there is an emphasis on threats and aggression in communication as stated: e.g. ‘Repeated threatening or abusive behaviours can amount to stalking or harassment offences.’ ‘Stalking and harassment cases can involve a repeated behaviour, such as persistent unwanted messages on social media services, or a range of different behaviours, such as sending abusive messages as well as monitoring victims and survivors’ accounts.’ However, we would like to emphasise that overt threats and abuse are not required to evidence stalking which can equally be evidenced in repeated and unwanted communications and contact with the victim which by virtue of being unwanted and repeated have a huge impact on the mental health of those who are targeted. See our point on risk further to this below.</p>
<p>Question 6.2:</p> <p>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.</p>	<p>We are concerned that there is no link made between stalking and domestic abuse within Vol 2. Data from the National Stalking Helpline shows that the majority of stalking cases will be in the context of domestic abuse (60% in 2023). While the analysis acknowledges the disproportionate risk of online harms on women, there is no recognition of the different risks for victims of DA related stalking which</p>

Question (Volume 2)	Your response
	<p>may manifest differently to someone who doesn't know their stalker.</p> <p>For example, if someone is stalking a celebrity, there is likely to be less chance of that person being targeted in real life, although there is still a very real psychological impact for victim, compared to ex-partner stalking which may include making threats to rape or kill, and in some cases carrying out the threat (see cases of Shana Grice and Alice Ruggles).</p> <p>There is also no discussion about how online behaviour coexists with offline behaviour. Many stalking cases will include a proximal element as well as an online element. By failing to make this link, there is no reference to the links between online and physical violence. This is despite stalking being positioned at stage 5 of 8 stages on Professor Jane Monkton Smith's homicide timeline. We are therefore concerned that tech platforms will not understand stalking as a 'high risk crime', despite the high risk of escalation stalking poses.</p> <p>This escalation of risk from an ex-partner, both online and offline, is highlighted by this case study from the Suzy Lamplugh Trust:</p> <p>Case study 1: The perpetrator is an ex-partner, they share children. The stalking has gone on for a year. The perpetrator has broken every order that has been put in place including a non-molestation order and police bail. The victim just wants to be left alone but the perpetrator is using the children as an excuse to continue stalking her. The perpetrator stopped for a while but has now started the stalking through social media, using multiple accounts such as TikTok and WhatsApp. He has used multiple numbers and emails too. The messages on social media are "love letters" - trying to get her back, then turn nasty when she does not reply and recently he did approach her physically and follow her in his car.</p> <p>While we welcome the acknowledgement in 6E.22 that 'Identifying content that causes fear or distress demands an understanding of the context. For example, sending a picture of someone's front door or workplace address might seem innocuous, but may be highly threatening, by making victims and survivors aware that the perpetrators can access them physically', we fear there is too much emphasis</p>

Question (Volume 2)	Your response
	<p>on overt threats providing a higher risk, for example 'Repeated threatening or abusive behaviours can amount to stalking or harassment offences.' It is the repeated and unwanted nature of the contact that causes the distress, which can present whether there are overt threats or not.</p>

Question (Volume 3)	Your response
<p>Question 8.1:</p> <p>Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice? Please provide underlying arguments and evidence of efficacy or risks to support your view.</p>	<p><i>No</i></p> <p>The governance and risk assessment proposals take at face value evidence from the platforms that they are "doing much of this already" and therefore the suggested measures will not incur any costs. This does not take account of the costs to society, the impact of business models nor the principle that the regulatory approach should focus on the overall objective (making services safer), rather than a tick-box process for compliance. We believe that the overall message that emerges from the consultation documents, compounded by the weak "safety by design" foundations, is that the regime is not outcome-orientated (e.g. to deliver improved safety) but focused on processes that companies need to follow in a tick-box way to comply. The obligation to measure the result of mitigation measures and improve them in risk assessments is undermined by the decision to take a process-driven approach in the codes. We therefore believe that the codes should impose a more stringent duty on platforms to prevent harm occurring their platforms rather than relying on reactive measures to illegal content.</p>

Question (Volume 3)	Your response
<p>Question 8.2:</p> <p>Do you agree with the types of services that we propose the governance and accountability measures should apply to?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 8.3:</p> <p>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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question: 8.4:</p> <p>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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 9.1:</p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 9.2:</p> <p>Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

Question (Volume 3)	Your response
<p>their wider obligations under the Act?</p>	
<p>Question 9.3: Are the Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service?¹</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 10.1: Do you have any comments on our draft record keeping and review guidance?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 10.2: 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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

¹ If you have comments or input related the links between different kinds of illegal harm and risk factors, please refer to Volume 2: Chapter 5 Summary of the causes and impacts of online harm).

Question (Volume 4)	Your response
<p>Question 11.1:</p> <p>Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?</p>	<p><i>No</i></p> <p>We are concerned that as drafted, the consultation reflects a business-centric approach. This is reflected in the disproportionate focus on the “costs” and perceived burdens for tech companies, with no equivalent consideration given to the cost and resources associated with the harms to individual women and girls and wider society - including the costs of support needs after harm. This has resulted in a reduced scope on platforms to address harms disproportionately impacted women and girls.</p> <p>Throughout the document, we also observe statements which rely on optimistic assumptions that companies will comply satisfactorily, e.g. that they will have processes for assessing illegal content that are of a higher benchmark than Ofcom has set out in Volume 5. We suggest that this assumption is in direct contrast with the spirit of the parliamentary debates prior to the introduction of the Act which underpinned the law, and a backdrop in which there was widespread acknowledgement that business initiatives had not gone far or fast enough, and that without the right incentives, tech companies will not do what is needed to protect their users.</p> <p>Relatedly, the approach taken by Ofcom to ask respondents to “evidence the harm, evidence the risks” also assumes that the online environment provided by platforms is currently neutral and/or inherently safe. In our view, this starting point is misguided. The onus should instead shift to businesses to provide evidence that their platforms and services have considered risk and are safe for women and girls.</p> <p>Aligned with this overall approach, is the fact that the consultation document, including the codes of</p>

Question (Volume 4)	Your response
	<p>practice, are largely inaccessible for a huge swathe of civil society. Whilst Ofcom staff have been responsive and engaged with stakeholder meetings, the reality is that the format makes it extremely difficult for third sector organisations to participate. We understand that this is an issue that has also been raised by the Domestic Abuse Commissioner. We are concerned by the risk that the views of victims and services representing them will not be adequately represented in this consultation, given that civil society organisations have comparatively less resources to engage with it.</p>
<p>Question 11.2:</p> <p>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?</p>	<p><i>No</i></p> <p>We do not agree that the most onerous measures set out in the Codes should only apply to services which are large and/or medium/ high risk. In our experience, smaller sites can be where some of the most significant harm is situated for women and girls, and the most extreme content. However, smaller companies are, in many instances, exempt from implementing particular mitigating measures due to Ofcom’s proportionality analysis. Even when limited to content moderation (i.e. not addressing systemic and functionality mitigation measures), small/single-risk services are “let off hook” based on their size and the proportionality assessment.</p>
<p>Question 11.3:</p> <p>Do you agree with our definition of large services?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

Question (Volume 4)	Your response
<p>Question 11.4:</p> <p>Do you agree with our definition of multi-risk services?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 11.6:</p> <p>Do you have any comments on the draft Codes of Practice themselves?²</p>	<p><i>No</i></p> <p>The measures set out in Volume 4 are prescriptive, tick-box and process-driven rather than delivering improved safety for users. We can see this in the inordinate amount of space given to the ‘blocking’ function and the ‘disabling comments’ function which must be introduced by providers in order for users, particularly women and girls, to stay safe from threats of abuse. Such measures, already widely used by service providers, provide potential respite after the abuse has already occurred, and does not seek to prevent the harm in the first place, a trend replicated across other measures suggested in Volume 4. They also put the onus on the victim to keep themselves safe from harm and abuse rather than ensuring resource is spent on safety by design features that would more robustly mitigate risk, such as controls to identify repeat perpetrators. There is an important need to accompany features such as blocking with relevant information related to course of conduct crimes, including signposting to specialist support services such as our own National Stalking Helpline. There is a concern that, whilst providing some respite for users experiencing stalking or harassment, blocking or disabling comments may mean that the escalation of communication is not picked up and the subsequent risk is missed. It is therefore important that users have access to specialist independent support on stalking or harassment no matter what course of action they choose to pursue.</p> <p>Volume 4 references the potential for a mechanism through which users must verify their identity as a way to combat the anonymity granted to perpetrators of crimes such as stalking. As referenced in the Register of Risk in Volume 2, the ability to make user</p>

² See Annexes 7 and 8.

Question (Volume 4)	Your response
	<p>profiles anonymous may embolden users to engage in stalking behaviours without fear of repercussions. Despite this acknowledgement, Volume 4 section 21.88 sets out that any such requirement would impede too heavily on user's freedom of speech- "Measures requiring services to establish a user's identity could potentially assist services in complying with the illegal content safety duty in section 10(2) of the Act. However, as we go on to explore in more detail below, based on the evidence we consulted we do not believe that the benefits of recommending a Code measure requiring services to adopt IDV to tackle illegal harms would justify the potential impacts on users' privacy and freedom of expression." This is an example of a broader trend whereby user's freedom of speech is prioritised over the safety of users and the detection and prevention of crimes, such as behaviours amounting to stalking.</p>
<p>Question 11.7: Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 12.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 13.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

Question (Volume 4)	Your response
<p>Question 14.1:</p> <p>Do you agree with our proposals? Do you have any views on our three proposals, i.e. CSAM hash matching, CSAM URL detection and fraud keyword detection? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 14.2:</p> <p>Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 14.3:</p> <p>Do you have any relevant evidence on:</p> <ul style="list-style-type: none"> • The accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services; • The 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; • The costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of 	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

Question (Volume 4)	Your response
<p>fuzzy matching³ for CSAM URL detection;</p> <ul style="list-style-type: none"> • The costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services; and • 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. 	
<p>Question 15.1:</p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 16.1:</p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

³ Fuzzy matching can allow a match between U2U content and a URL list, despite the text not being exactly the same.

Question (Volume 4)	Your response
<p>Question 17.1:</p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 17.2:</p> <p>Do you have any evidence, in particular on the use of prompts, to guide further work in this area?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 18.1:</p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 18.2:</p> <p>Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 18.3:</p> <p>Are there other points within the user journey where under 18s should be informed of the risk of illegal content?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

Question (Volume 4)	Your response
<p>Question 19.1:</p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 19.2:</p> <p>What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 19.3:</p> <p>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. Are you aware of any other design parameters and choices that are proven to improve user safety?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 20.1:</p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

Question (Volume 4)	Your response
<p>Question 20.2:</p> <p>Do you think the first two proposed measures should include requirements for how these controls are made known to users?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 20.3:</p> <p>Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 21.1:</p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 21.2:</p> <p>Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically:</p> <ul style="list-style-type: none"> • 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)? What are the advantages and disadvantages of the different options, including 	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

Question (Volume 4)	Your response
<p>any potential impact on other users?</p> <ul style="list-style-type: none"> • How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed? • 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. 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? 	
<p>Question 22.1:</p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 23.1:</p> <p>Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

Question (Volume 4)	Your response
<p>Question 23.2:</p> <p>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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 23.3:</p> <p>We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 24.1:</p> <p>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? If not, why not?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

Question (Volume 5)	Your response
<p>Question 26.1:</p> <p>Do you agree with our proposals, including the detail of the drafting? What are the underlying arguments and evidence that inform your view.</p>	<p>No</p> <p>The proposals set out in Volume 5 appear to focus on content which is of an illegal nature, such as threats of an obscene nature, rather than the course of behaviour which may constitute a crime, such as stalking. Whilst we welcome duties on platforms to take down posts that constitute harassment, there is a danger that the guidance is overly focused on determining the illegality of each piece of content rather than setting a duty for platforms to design system and processes to reduce harmful material or the perpetration of course of conduct</p>

Question (Volume 5)	Your response
	<p>crimes such as stalking. We see no mechanism through which platforms are required to make links between individual reports of harmful content and a wider course of conduct crime, which means risk of escalation may not be picked up in these cases. More widely, Volume 5 does not associate 'illegal content' with its approach to tackling stalking occurring on providers platforms, despite the ability for perpetrators to use platforms to share content about victims, send threatening and abuse messages, and gain information about the victim (which is all recognised in Vol 2.) There is therefore a disconnect between the evidence of harm in the risk profiles set out in Vol 2 and the mitigation measures in the codes of practice.</p> <p>The case study below demonstrates how even individual messages could be deemed 'illegal content' to be addressed in Vol 5 yet must still be recognised as part of the course of conduct crime that is stalking.</p> <p><i>Case study 2: The client was in a high-risk abusive relationship with the perpetrator which ended around 2 years ago, during this relationship she experienced physical, sexual and emotional abuse to a high level. In the 2 years since the relationship ended client has experienced consistent stalking from the perpetrator, usually in the form of him creating fake instagram or snapchat accounts to threaten and intimidate her (often using very graphically violent language, threatening to kill or sexually abuse client and at times her family members), then deletes the accounts so it is very difficult for police to evidence that the messages are coming from him. This happens usually around once a month, the most recent incident was 19/07/23 in which the messages included what client was wearing at the time she received them and the hospital she was leaving where she works (she had thought he was not aware of this location). The messages also included threats of sexual violence and kidnapping. Client has reported each incident to the police, the case was no further actioned earlier this year then opened up again. Police are struggling to gather evidence that the stalking is coming from the perpetrator, which is leaving the client at further risk. The perpetrator is in a new relationship however still continues to harass my client.</i></p>

Question (Volume 5)	Your response
	<p>We are also concerned by the following assumption in 26.19: ‘Many services will already have terms of service or their equivalent in place that are more expansive than the Act in defining what content may be deemed violative and will already be taking down above and beyond what the law requires in terms of preventing users encountering illegal content.’ We would like to understand the evidence base for this statement and caution against any assumption that services will in any way go over any above any requirements in the guidance. We would therefore strongly request that the guidance require the highest possible level of prevention and regulation to minimise the harms outlined in Volume 2.</p>
<p>Question 26.2:</p> <p>Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 26.3:</p> <p>What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?</p>	<p><i>No</i></p> <p>We question Ofcom’s approach to the definition of illegal content. Whilst we understand that Ofcom must work within the scope of the Act, there are areas in which it is ambiguous. We suggest that Ofcom is interpreting the provisions overly narrowly, by limiting it to individual pieces of content, rather than a systems-based approach that considers elements such as algorithm weighting, nudges, content revenue sharing practices - which don’t apply only to a narrow lens on a piece of content and the intention behind it.</p> <p>We also acknowledge the inclusion of the following:</p> <p><i>26.137 Once services have considered all the offences which are necessarily carried out by threats or abuse, a set of offences remain which can be carried out by threats or abuse, but which need not be – they are the offences to do with harassment, stalking and coercive and controlling behaviour.</i></p>

Question (Volume 5)	Your response
	<p><i>26.138 These offences include conduct which is very serious indeed and which disproportionately affects women and girls</i></p> <p>However, we believe that there is too much weight given to reporting as an indicator of harm online. We know that the majority of survivors do not report, and this should not be the primary basis for the measure of safety for a given platform. A systems-based approach is needed to root out harmful practice and patterns of behaviour and not rely on reporting of behaviours by the victim.</p> <p>We are concerned about the following criteria as set out in 26.26 a) <i>Content information: The type of information that is most likely to be reasonably available to services when making an illegal content judgement is the information contained within the content itself e.g., what the text displayed within an image reads.</i></p> <p>As highlighted above the content which forms part of the crime of stalking may not contain offensive or harmful words or images in and of itself but forms part of a course of conduct of stalking which is repetitive and unwanted which results in harm to the victim.</p> <p>b) <i>Complaints information: Services may also want to consider information they receive which is contained in a complaint from a third party (e.g. law enforcement, a trusted flagger, a user). When using this type of information, the service may also want to consider who that third party is and how robust and reliable the information may be based on this</i></p> <p>As stated above, we are concerned that there is an emphasis on reporting and complaints rather than seeking to identify harmful content in order to remove it. We also see through our National Stalking Helpline Service that it is common for platforms to have limited communication with users who have been victims of stalking when they have reported a perpetrator using their platform to contact and harass them, often failing to follow up on instances of stalking that have been reported. We would urge consideration of information put forward by specialist stalking advocates from frontline support services on behalf of victims and work</p>

Question (Volume 5)	Your response
	<p>with them to address the stalking behaviours occurring on their platform. We would also urge Ofcom to implement a duty on platforms to set up a trusted flagger system on their platforms to ensure open communication between platform providers and specialist support services like the National Stalking Helpline which will enable swifter action on stalking behaviours.</p> <p>We have set out our position on these issues in further detail in a joint formal response to Ofcom's consultation. However, we would welcome your consideration of these related issues in the round.</p>

Question (Volume 6)	Your response
<p>Question 28.1:</p> <p>Do you have any comments on our proposed approach to information gathering powers under the Act?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question 29.1:</p> <p>Do you have any comments on our draft Online Safety Enforcement Guidance?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

Question (Annex 13)	Your response
<p>Question A13.1:</p> <p>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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p>Question A13.2:</p> <p>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.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>

Please complete this form in full and return to IHconsultation@ofcom.org.uk.