Dame Nicole Jacobs
Domestic Abuse Commissioner for England and Wales
2 Marsham Street, London SW1P 4JA
commissioner@domesticabusecommissioner.independent.gov.uk

20 October 2025

Sent via email to: Ofcom Consultation Team (ASMconsultation@ofcom.org.uk)

Copied to: Melanie Dawes, Ofcom Chief Executive Officer

Ofcom Consultation: Online Safety - Additional Safety Measures

I write in my capacity as the Domestic Abuse Commissioner for England and Wales, a statutory consultee under the Online Safety Act 2023 (OSA), to respond to the Online Safety – Additional Safety Measures consultation, published 30 June 2025.

I welcome Ofcom's commitment to strengthening the Illegal Content and Protection of Children Codes of Practice, particularly the proposals aimed at preventing the dissemination and amplification of harmful content, including non-consensual intimate imagery (NCII) and child sexual abuse material (CSAM). These forms of harm exist within a wider continuum of technology-facilitated abuse, where perpetrators misuse digital systems and platform functionalities to monitor, control, and harm victims. The introduction of proactive measures, including the expansion of hash-matching technology to adult NCII, represents an important step forward. It demonstrates recognition that the circulation of intimate images without consent is a serious form of abuse with profound psychological, social, and sometimes physical consequences.

However, while these proposals are welcome, there remain areas where the regulatory approach requires further clarification and reinforcement to ensure meaningful protection for survivors. Chief among these is the allowance for service providers to claim "technical infeasibility" when implementing hash-

matching and other technical safeguards. Without rigorous scrutiny and accountability, this caveat risks leaving survivors exposed to ongoing abuse and undermines the intended benefits of the Online Safety Act.

I therefore make the following 10 recommendations to strengthen the proposals, which speak to themes of technical standards and enforcement, survivor-centred design and response, and coordination and resourcing. My letter will then set out further background and context to these recommendations.

1. **Define risk environments precisely**, ensuring high-interaction and high-risk contexts within live-streaming, for example, real-time gifting, trigger heightened and non-discretionary obligations.

2. **Link transparency reporting directly to enforcement outcomes**, requiring platforms to publish specific, measurable and auditable data on the effectiveness of their safety measures, including detection thresholds, mitigation steps, and algorithmic configuration.

3. **Apply a baseline of enforceable technical standards** to all providers, including smaller or niche services, to prevent gaps in protection gaps and ensure consistent safety measures across platforms, ensuring a minimum level of safety for all users.

4. **Specify mandatory technical tools and standards explicitly**, including hash-matching for adult NCII, proactive detection, abusability testing, algorithmic safeguards, and proactive and VAWG-trained human moderation, closing off "technical feasibility" loopholes.

5. **Mandate ongoing review of technical safeguards**, including hash-matching precision and recall, algorithmic recommendations, and human moderation processes, with regular reporting to Ofcom.

6. **Mandate specific and actionable rapid response mechanisms** with critical support elements for viral and escalating abuse incidents, including immediate removal of abusive content and accounts, user bans and provision of survivor support.

7. **Embed academic, survivor and specialist expertise** in auditing, oversight, and abusability testing, ensuring that safety interventions demonstrably reduce harm in practice.

8. **Require survivor-centred and co-produced design** across all interactive features, to include collaboration with criminal justice professionals, ensuring that privacy, safety defaults, and rapid escalation mechanisms are integrated into platform development from the outset and complement any potential criminal investigation.

9. **Ensure cross-platform coordination** through interoperable detection systems, shared NCII hash databases, and joint investigative protocols to prevent abuse migration between services and enable collective action against repeat offenders.

10. **Sustain dedicated funding** for specialist domestic abuse and VAWG services, including technology abuse experts and partner agencies, to support the implementation of the Online Safety Act and meet the anticipated increase in survivor reporting and requests for assistance.

As I have highlighted in my previous consultation responses, I also note again the volume of content and the highly technical language used in this consultation. This creates a barrier for domestic abuse and VAWG organisations (most of which are non-profit organisations and have very limited resources) and people with lived experience to meaningfully engage and provide detailed feedback, which is a vital component to delivering comprehensive and sufficient online safety for all.

The complex online risk environment for domestic abuse victims and survivors

Domestic abuse increasingly intersects with technology, and abusers frequently weaponise digital platforms to monitor, control, and harass survivors. The features that make platforms attractive—friend suggestions, comments, gifting mechanisms, live-streaming capabilities, and location metadata—can all be abused to exert coercive control, stalk, or intimidate victims. Victims and survivors report instances where abusers exploit automated friend recommendations to track their social connections, use location-based features to identify and follow them offline, or manipulate gift and engagement features to coerce attention and

compliance. This amplifies harm and creates a pervasive risk environment in which abuse can extend seamlessly between online and offline contexts.

Survivors' experiences of technology-facilitated abuse differ widely. Intersecting inequalities—of gender, race, disability, and immigration status—affect both exposure to risk and access to protection. Effective online safety measures must therefore be proportionate and inclusive, addressing how platform design and moderation practices can reinforce these disparities.

These unequal conditions are compounded by the fragmented digital landscape that survivors must navigate. Abuse is rarely confined to a single service; perpetrators often coordinate across multiple platforms to evade detection and continue harassment. The circulation of intimate images without consent, doxxing, targeted threats, and online stalking frequently overlap with offline risks, including physical violence, coercive control, and financial exploitation.

Exposure through metadata and location services is particularly concerning. Many survivors are unaware that even seemingly benign features, such as geotagging or friend suggestions, can provide abusers with actionable information about their location and social networks. Default anonymisation, limited sharing of sensitive data, and privacy-preserving safety defaults must therefore be standard for users identified as at risk. Reporting systems should be accessible, survivor-centred, and provide rapid escalation routes, with immediate removal of abusive content and accounts.

High-interaction environments, such as live-streaming and real-time gifting, are particularly high-risk. They enable real-time abuse and increase the likelihood of victim exposure to harmful content. Platforms must integrate technical safeguards, including hash-matching, algorithmic monitoring, proactive human moderation, and rapid escalation, to protect survivors in these high-risk contexts.

Effective use of hash-matching

The proposed expansion of hash-matching technology to detect NCII involving adults is a welcome development. Hash-matching, including perceptual hash-matching, allows platforms to create digital fingerprints of images and detect repeated uploads of abusive content. This approach has been successfully deployed to prevent the recirculation of CSAM and can be adapted to NCII, providing a technological barrier to the widespread dissemination of intimate images shared without consent.

Effective implementation, however, requires more than simply applying hash-matching, and must be mandated for adult content as it is for child-specific content. Older teen girls are one of the most vulnerable cohorts online but are left with less support and fewer safeguards than their slightly younger peers, despite facing similar risks.

Proactive and specially trained human moderation, continuous evaluation of detection accuracy, and integration with rapid reporting mechanisms are essential. All victims and survivors must be able to report content quickly, have it removed without delay, and receive guidance and support throughout the process. Proactive detection systems should be complemented by victim-centred "abusability testing"[1] for new interactive features, including live-streaming, gifting, and location-enabled functionalities, ensuring that platforms cannot introduce high-risk features without robust protective measures.

Furthermore, the consultation's provision allowing platforms to cite "technical infeasibility" for non-compliance presents a significant concern. Survivors are often disproportionately affected by the repeated circulation of intimate images; if platforms are permitted to defer or scale back protective measures on technical grounds, victims remain exposed to substantial harm. To mitigate this risk, Ofcom should require providers to submit detailed evidence supporting any claim of infeasibility, including technical documentation, implementation timelines, interim mitigation strategies, and independent validation by accredited auditors, academics and specialist domestic abuse and VAWG organisations. Such scrutiny will ensure that technical difficulty cannot be exploited to avoid meaningful protection.

In addition to hash-matching, algorithmic systems for recommendation, ranking, and trending must be configured to minimise amplification of abusive content. Victims and survivors are at heightened risk when platforms promote, highlight, or resurface harmful images or videos, either algorithmically or via user-generated amplification. Proactive detection technologies, combined with victim-centred abusability testing for all new interactive features, should be standard practice. These assessments should identify foreseeable risks before new functionalities

[1] Slupska, J., & Tanczer, L. (2021). Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. J. Bailey, A. Flynn, &, N. Henry (Eds.), The Emerald International Handbook of Technology Facilitated Violence and Abuse (pp. 663–688). Bingley: Emerald Publishing Limited. https://www.emerald.com/books/oa-edited-volume/12133/chapter/82202491/Threat-Modeling-Intimate-Partner-Violence-Tech

are deployed, ensuring safety-by-design principles are embedded into service development[2]. These approaches to prevention and response must also be co-produced with criminal justice professionals, to ensure that any actions taken by platforms to prevent harm and safeguard victims and survivors do not undermine any ongoing or potential future criminal investigations.

Perpetrator accountability and cross-platform safeguards

Protecting survivors requires proactive, effective action against perpetrators. Platforms should go further than removing harmful content, implementing mechanisms to hide or suspend abusive accounts, preventing re-registration under linked identities, and sharing relevant information with law enforcement[3] where appropriate. These measures are essential for disrupting cycles of abuse and ensuring perpetrators cannot exploit gaps between platforms.

Cross-platform interoperability is critical. Many perpetrators operate across multiple services, exploiting differences in detection and enforcement practices to continue abuse undetected. Coordinated approaches, including shared hash databases for NCII, joint investigative protocols, and rapid reporting mechanisms, are necessary to provide meaningful protection for survivors.

The risk posed by the "technical infeasibility" caveat must also be mitigated in this context. Providers should be required to justify any delays or limitations in implementing protective measures, with oversight from independent auditors and domestic abuse specialists. Victims and survivors must not be left exposed due to technical loopholes or delays in enforcement.

Oversight, transparency, and enforcement

Technology alone cannot protect survivors; accountability and enforcement are critical. Ofcom's powers to issue direction orders, impose financial penalties, and enforce compliance must be applied consistently and transparently. Reporting obligations should extend beyond generic compliance statements to include

---

[2] Brown, A., Harkin, D., & Tanczer, L. (2024). Safeguarding the 'Internet of Things' (IoT) for Victim-Survivors of Domestic and Family Violence (DFV): Anticipating Exploitative Use and Encouraging Safety-by-Design. Violence Against Women. https://journals.sagepub.com/doi/10.1177/10778012231222486

[3] Douglas, H., Tanczer, L., McLachlan, F., & Harris, B. (2023). Policing Technology-Facilitated Domestic Abuse (TFDA): Views of Service Providers in Australia and the United Kingdom. Journal of Family Violence. https://link.springer.com/article/10.1007/s10896-023-00619-2

granular detail on technical safeguards, moderation practices, algorithmic configuration, and the deployment and efficacy of hash-matching systems.

Algorithmic transparency is especially crucial: platforms should demonstrate that their ranking, recommendation, and trending systems are configured to avoid amplifying content harmful to survivors and provide auditable records of interventions.

Independent oversight must integrate the expertise of academics, domestic abuse specialists and survivors themselves. This ensures that compliance is not merely technical but genuinely mitigates harm in practice.

Funding and specialist support

As I have highlighted in response to previous Ofcom consultations on online safety, the successful implementation of these measures relies on adequately funded specialist services. Specialist services provide expertise that cannot be replaced by automated systems alone. This includes advising on risk assessment, configuring proactive detection technologies, conducting victim-centred abusability testing, and providing training to platform staff. With the Online Safety Act actively encouraging increased reporting of online harms, funding for these organisations must reflect the anticipated uplift in demand.

Sustained funding ensures that survivors have timely access to support and that platforms can implement safeguards effectively, informed by practical experience and specialist knowledge.

Concluding remarks

The Additional Safety Measures provide a critical opportunity to embed victim and survivor safety within the Online Safety Act's regulatory framework. Success will depend on Ofcom using its full powers to require platforms to implement proven technical safeguards, meet measurable standards of compliance, and prevent "technical infeasibility" from becoming a route to inaction.

The consensus among specialist organisations and academic research is clear: safety-by-design must be a regulatory requirement, not an aspiration. Platforms must adopt a proactive, survivor-centred approach, supported by independent oversight, cross-platform coordination, and robust funding for specialist services. Only by taking these steps can the full potential of the Online Safety Act be

realised, providing meaningful protection for victims and survivors of domestic abuse and online harms.

I urge Ofcom to demonstrate bold leadership in this area and look forward to supporting the implementation of measures that deliver robust, evidence-based outcomes for victims and survivors. I remain available to discuss any of these important issues with you and look forward to our continued engagement.

Yours sincerely,

Domestic Abuse Commissioner for England and Wales