Technology-facilitated abuse Inquiry

(House of Commons Science and Technology Committee)

November 2026

Introduction

1. MWNUK has been advancing equality, and social justice for Muslims women and girls since 2003 and is a registered charity (no.1155092) with a national membership. We provide direct support through our Muslim Women's Network Helpline (www.mwnhelpline.co.uk) which focuses on gender-based violence, (primarily domestic abuse and related issues) and Muslim Safety Net Helpline (www.muslimsafetnet.org.uk) which focuses on anti-Muslim abuse, hostility and discrimination. We also conduct research and use lived experiences to identify policy and practice gaps which informs our advocacy, campaign and resource production work to empower women. Further information about our work can be found on our main organisational website (www.mwnuk.co.uk) .

2. Muslim Safety Net was established in response to a report published by Muslim Women's Network UK (MWNUK) following the racially and religiously aggravated riots in the summer of 2024. The report, Anti-Muslim Hate – Concerns and Experiences, https://www.mwnuk.co.uk//go_files/resources/Anti-Muslim-Hate-Report-concerns-and-experiences-new.pdf revealed that 80% of victims do not report anti-Muslim incidents, meaning the true scale of hatred and discrimination is being significantly underestimated. Only 3000-4000 incidents are reported to police annually. If 80% are not reporting, then actual number of incidents are more likely to be 15,000 to 20, 000.

3. Since 2023, MWNUK has also seen a rise in anti-Muslim-related calls to its Muslim Women's Network Helpline, which is primarily for domestic abuse victims. In response, it was decided that a dedicated website and reporting database would better capture these experiences and encourage more Muslims, both women and men, —to come forward and report incidents. It is important to capture data in anti-Muslim incidents to understand the scale nature and scale of the problem, which is crucial to hold governments and public institutions accountable, so they can be urge to take stronger action against anti-Muslim hatred and discrimination.

(AI was used to assist with editing, structuring and grammatical improvements.)

In what ways is technology used to facilitate abuse of individuals – particularly women and girls – and how are these changing?

4. Technology-facilitated abuse takes many forms, including:

5. Anti-Muslim hostility and harassment: Abusive comments, religious slurs, threats and derogatory messages targeting Muslim women because of their faith, ethnicity or appearance. Muslim women are increasingly being targeted through AI tools that remove their headscarves from photographs, causing distress and humiliation. This type of abuse may not necessarily meet the threshold of a criminal offence.

6. Gendered and sexualised abuse: Unwanted sexual messages, sexual harassment, threats of sexual violence and degrading comments about women's bodies, clothing and religious identity.

7. Cyberstalking and digital surveillance: Using social media, location tracking, spyware and monitoring applications to follow, monitor or control women. For example, on our MWN Helpline, we supported a service user (SU) who was being tracked through tracking applications on her phone and tracking devices. This surveillance was used by her husband to control her movements and restrict her freedom. She was unable to go out or meet up with friends freely, as her husband would know her whereabouts and come to collect her. This demonstrates how digital surveillance can be used as a tool of coercive control, isolating women and restricting their independence.

8. Doxxing and misinformation: Publishing personal information, photographs, addresses or workplace details without consent, alongside deliberately spreading false or misleading information. For example, Nora Mubarak, a Muslim woman from Grimsby, was filmed by a bystander in July 2026 while saving a seagull. False claims were subsequently circulated online that she intended to eat or harm the bird, exposing her to significant online abuse and harassment.

9. Image-based sexual abuse: Taking, creating or sharing intimate images without consent, including manipulated photographs, deepfakes and AI-generated sexual images. On our MWN Helpline, we supported a service user (SU) who hired a DJ for her 18th birthday party. The DJ asked to meet her in person to collect the deposit. During the meeting, he sexually abused her and recorded the incident using Meta smart glasses. He then threatened to share the footage online and with her parents. This case highlights how wearable technology can be used to record sexual abuse without consent and how threats to distribute the footage can be used to intimidate, exploit and control victims.

10. Coordinated online harassment and intimidation: Organising groups to target women through mass comments, threats, personal information and abusive images. Such campaigns can also be designed to silence women, discourage them from expressing opinions and undermine their participation in public debate.

What responsibilities should technology companies and online platforms have for preventing or mitigating technology-facilitated abuse?

11. Technology companies and online platforms have a responsibility to ensure their products and services do not enable, facilitate or amplify abuse. Their responsibilities should extend beyond responding to individual complaints. They must proactively identify risks, prevent foreseeable misuse and provide effective protection for victims.

12. This is particularly important for Muslim women and girls, who can experience overlapping forms of abuse relating to gender, race and religion. Platform algorithms and recommendation systems can also amplify anti-Muslim hostility and disinformation, increase the visibility and reach of harmful content.

13. Content moderation on X (formerly Twitter) has weakened since Elon Musk's takeover, with concerns about reduced safeguards and the amplification of anti-Muslim disinformation and abusive content. Other platforms have also relaxed aspects of their content policies.

Following Donald Trump's election to a second term, Meta eased some content restrictions and announced the replacement of independent factchecking in the United States. These developments raise further concerns about protections against online hostility and misinformation.

14. Technology companies should recognise intersectional abuse by ensuring their policies explicitly address misogyny, racism and anti-Muslim hostility, including how these forms of abuse intersect; improve content moderation by identifying and promptly removing threats, targeted harassment, impersonation and non-consensual intimate images, while recognising repeated targeting and the wider context of abuse; prevent the creation and circulation of abusive material by introducing robust safeguards against non-consensual sexual images and preventing removed material from being repeatedly uploaded; provide effective reporting mechanisms that ensure victims receive timely responses, clear explanations and meaningful support without repeatedly having to recount traumatic experiences; address algorithmic amplification by ensuring recommendation systems do not promote misogynistic, racist or anti-Muslim content simply because it generates engagement; protect privacy through effective safeguards against doxxing, stalking, impersonation and unwanted contact, while giving users greater control over their photographs, personal information and location data; and consult affected communities, including Muslim women's organisations, specialist support services and other marginalised communities, when developing and evaluating safety policies.

15. Platforms must also be held accountable when they repeatedly fail to address abuse. Publishing community standards is insufficient if those standards are poorly implemented or victims cannot obtain meaningful protection.

16. Crucially, responsibility must not be shifted onto Muslim women. Women should not be expected to remove photographs, stop wearing visible religious clothing, restrict their online presence or withdraw from public debate to protect themselves. The responsibility must rest with perpetrators and the companies whose products and services facilitate abuse.

How effective are existing platform policies, reporting systems and moderation processes?

17. Although most major social media platforms have policies prohibiting harassment, hate speech, threats and the sharing of non-consensual intimate images, there remain significant concerns about how consistently these policies are implemented.

18. A central problem is that reporting systems do not always recognise the intersection of misogyny, racism and anti-Muslim hostility. When incidents are assessed individually, platforms can overlook repeated targeting and the cumulative seriousness of the abuse.

19. Key weaknesses include inconsistent content moderation, limitations in automated systems' ability to recognise coded language and context-specific abuse, and complicated reporting processes that often result in automated rather than meaningful responses. There is also a lack of transparency about decisions and actions taken, while perpetrators can continue harassment through new accounts or across platforms. Reporting systems also frequently fail to recognise patterns of coordinated targeting and overlapping forms of discrimination.

20. There is also a significant issue concerning intimate image abuse. MWNUK's helpline experience demonstrates that perpetrators can use intimate images and recordings as tools of coercion and control without necessarily distributing them. A victim may know that a former partner has secretly recorded her or possesses fabricated sexual images but have no way of knowing whether the material has been shared or who has seen it.

21. Current reporting mechanisms are unlikely to address the full extent of this abuse where material is retained privately, shared directly with selected individuals or used as a threat outside the platform itself.

22. We recommend that platforms introduce reporting options that explicitly recognise misogynistic, racist and anti-Muslim abuse, including intersectional incidents; allow victims to report patterns of harassment rather than individual incidents separately; provide human review for serious cases involving threats, sexual exploitation, stalking and non-consensual intimate material; offer clear explanations of decisions and accessible routes to appeal; strengthen safeguards against repeat offenders and the re-uploading of abusive material; and publish anonymised data on reports, response times, content removals and enforcement outcomes, with appropriate disaggregation where possible.

23. Greater accountability is also needed for anonymous accounts used to facilitate harassment, hate speech and disinformation. Freedom of expression must come with accountability, and appropriate mechanisms should exist to identify perpetrators and hold them responsible while protecting legitimate anonymity and privacy.

24. Ultimately, the effectiveness of platform policies should be measured by whether they prevent abuse, protect victims and hold perpetrators accountable, rather than simply by the existence of reporting mechanisms.

How should tech companies identify and respond to risks associated with new products, services and features?

25. Technology companies should adopt a preventative approach to online safety. Potential risks should be identified, assessed and addressed before new products, services or features are made available to the public.

26. This is particularly important as artificial intelligence, facial recognition and image-manipulation technologies create new opportunities for abuse. For Muslim women and girls, risk assessments should consider how these technologies could be misused to target individuals because of their gender, religious identity, ethnicity or appearance.

27. For example, AI image-generation tools could be used to manipulate photographs of Muslim women wearing hijabs, create fabricated sexual images or produce content intended to humiliate and intimidate them. Facial recognition and image-search technologies could also make it easier to identify women in photographs, connect online profiles to real identities and expose personal information.

28. Companies should conduct equality and human rights impact assessments before launching new products and features; assess the potential for technologies to facilitate gender-based, racist and anti-Muslim abuse; involve Muslim women, girls and specialist organisations in product development and safety testing; introduce robust safeguards against the creation and distribution of non-consensual AI-generated sexual material; consider risks associated with fabricated sexual audio, voice cloning and impersonation, not just manipulated photographs and videos; ensure users have meaningful control over their personal information, photographs and location data; assess whether recommendation algorithms and automated systems could amplify hateful or abusive content; and regularly review products after launch to identify emerging forms of misuse and respond to newly identified risks.

29. Attention should be paid to technologies that allow intimate images, recordings or personal information to be created, manipulated or distributed without someone's knowledge or consent. Risk assessments must also recognise that harm can occur even when material is

not publicly distributed. As MWNUK's helpline experience demonstrates, simply knowing that someone possesses secret recordings or fabricated intimate images can be used to intimidate and control victims.

30. Companies should be transparent about how they assess these risks and what action they take when vulnerabilities are identified. Safety assessments should also recognise that Muslim women are not a homogeneous group. The experiences of visibly Muslim women, converts, younger women, women from different ethnic backgrounds and women with disabilities may differ considerably.

31. The development of new technology must not come at the expense of women's safety, privacy, dignity or ability to participate equally in digital spaces.

To what extent does existing legislation and policy address technology-facilitated abuse?

32. The UK has an existing legislative framework addressing several forms of technology-facilitated abuse. However, questions remain about whether current legislation provides sufficiently comprehensive protection against the different and overlapping forms of abuse experienced by Muslim women and girls.

33. The Online Safety Act 2023 is an important part of this framework. It places legal responsibilities on regulated online platforms and services to assess and manage risks associated with illegal content and comply with relevant online safety duties. Ofcom is responsible for regulating and enforcing these requirements.

34.Other relevant legislation includes the Protection from Harassment Act 1997, which provides protection against harassment, including patterns of unwanted behaviour facilitated through digital technology; the Equality Act 2010, which provides protection against discrimination on grounds including sex, race and religion or belief in relevant circumstances; the Sexual Offences Act 2003, which contains offences relating to sexual abuse and image-based abuse, including provisions concerning cyberflashing and certain forms of non-consensual intimate image abuse; the Malicious Communications Act 1988 and Communications Act 2003, which have historically addressed certain forms of abusive and threatening communications, although subsequent legislation has changed parts of this framework; the Data (Use and Access) Act 2025, which introduced further offences relating to the creation or requesting of purported intimate images of adults without consent; and the

Crime and Policing Act 2026, which introduced further measures concerning modification tools and protections relating to non-consensual intimate images.

35. Despite these developments, important gaps and challenges remain.

36. First, the law does not always adequately reflect the intersectional nature of abuse. Muslim women can experience misogyny, anti-Muslim hostility and racism simultaneously. Although individual incidents may be addressed through existing harassment, sexual offences or equality legislation, the combined nature and cumulative impact of this abuse may not be fully recognised.

37. Second, there are gaps in protection relating to intimate images and recordings. MWNUK has raised concerns about the use of secret recordings, digitally fabricated images and intimate material as tools of coercion and control. The harm can occur even when material is not distributed, or when perpetrators simply disclose that they possess it. Victims must be adequately protected against the creation, possession, disclosure and threatened use of intimate material in circumstances involving abuse.

38. There is also a need to examine protections concerning non-consensual audio recordings of sexual activity and digitally fabricated sexual audio. A person's voice can be identifiable, and its misuse can cause serious harm, yet this aspect of technology-facilitated sexual abuse receives considerably less attention.

39. Third, there are practical barriers to enforcement. Victims may struggle to identify perpetrators, preserve digital evidence and navigate reporting processes. Investigations can become more complicated when perpetrators use anonymous accounts, multiple platforms or services operating across international borders.

40. Fourth, not all harmful behaviour is necessarily criminal. Some online content may be deeply misogynistic, racist or anti-Muslim without meeting the legal threshold for a criminal offence. This can leave women exposed to harmful behaviour that platforms may also fail to address adequately.

41. Finally, legislation must keep pace with technological developments. AI-generated sexual images, deepfakes, voice cloning, modification applications and increasingly sophisticated surveillance technologies create challenges for existing protections.

42. The Women and Equalities Committee's January 2026 report called for the Government to consider whether the existing legislative and regulatory framework, including the Online Safety Act, is sufficient to address online anti-Muslim hatred. In its May 2026 response, the Government referred to existing platform duties and Ofcom's enforcement role while acknowledging the need for further action.

43. We recommend that the Government undertake a comprehensive review of the legal framework, specifically examining whether it adequately addresses the experiences of Muslim women and girls. This should include the creation and use of intimate images without consent, including AI-generated material; threats involving intimate images, including circumstances where material is not actually distributed; secret recordings of sexual activity, including audio recordings; the use of intimate material as a means of coercion, intimidation and control; the role of online platforms and AI developers in facilitating abuse; and the intersection of anti-Muslim hostility, misogyny and racism in technology-facilitated abuse.

44. The objective should be to ensure that women are protected from the actual harm and abuse they experience, rather than relying on legal definitions that may not adequately reflect how technology is being misused.

How can Government ensure that protections keep pace with technological developments?

45. The pace at which technology-facilitated abuse evolves is extremely rapid, while lawmakers often respond too slowly. Rather than anticipating how emerging technologies could be misused and introducing protections early, action is frequently taken only after a problem has become widespread.

46. MWNUK previously raised concerns about intimate audio abuse and the need for it to be outlawed. At the time, the Government indicated that it had not received many complaints suggesting this was a significant issue. This illustrates the danger of waiting for high numbers of reported cases before recognising emerging forms of abuse and acting.

47. Government must ensure that legislation, regulation and public policy evolve alongside technological developments. This requires a proactive approach that anticipates emerging risks rather than responding only after new forms of abuse have become widespread.

48. We recommend action in seven areas:

49. Government should regularly assess whether existing legislation adequately addresses emerging forms of technology-facilitated abuse. This should include reviewing protections against AI-generated sexual images, fabricated sexual audio, digital surveillance, online stalking, doxxing, secret recordings and coordinated harassment. Reviews should involve specialist organisations supporting victims and consider the practical difficulties women face when seeking legal protection.

50. Government should ensure that Ofcom has the resources, powers and expertise needed to hold technology companies accountable when they fail to meet their legal responsibilities. Regulatory scrutiny should examine how platforms respond to misogynistic, racist and anti-Muslim abuse and whether moderation systems adequately protect women from minority communities. Companies should demonstrate measurable improvements in victim protection, reporting outcomes and the prevention of repeat abuse.

51. There is a significant need for better evidence about the experiences of Muslim women and girls online. Government should support research examining the prevalence, nature and impact of technology-facilitated abuse, including the intersection of gender, religion and ethnicity. Data collection should consider age, disability and other relevant characteristics while ensuring victims' identities and privacy are protected. Research should also examine less visible forms of abuse, including secret recordings, threats involving intimate images, AI-generated sexual material and the use of digital technologies to facilitate coercive control.

52.Government should involve Muslim women's organisations, grassroots community groups and specialist support services in developing online safety legislation, policies and regulatory approaches. These organisations have direct experience of the barriers women face when reporting abuse, accessing support and seeking protection. Their expertise is particularly important in understanding how online abuse can interact with domestic abuse, honour-based abuse, sexual exploitation and community pressures. Consultation should be ongoing, properly resourced and capable of influencing policy decisions.

53.Digital literacy and online safety education should address the different forms of abuse women and girls may experience. This should include helping young Muslim women and girls understand their digital rights, recognise online harassment, protect their personal information and access appropriate support. Education should also challenge anti-Muslim hostility, misogyny and harmful stereotypes that contribute to online abuse. Prevention work

must address perpetrators and wider societal attitudes, rather than placing responsibility solely on women and girls.

54. Government should support accessible reporting mechanisms and specialist services for victims of technology-facilitated abuse. Support should be culturally competent, confidential and sensitive to the experiences of Muslim women. Women should not feel they need to justify their religious identity, explain anti-Muslim hostility or overcome assumptions about their culture before their experiences of abuse are taken seriously. Specialist services should also be equipped to support victims experiencing image-based abuse, digital surveillance, threats involving intimate material and other forms of technology-enabled coercive control.

55. Online safety strategies should not assume that all women experience technology-facilitated abuse in the same way. Muslim women, particularly those who are visibly Muslim, should be represented in research, consultations and policy development. Their experiences should inform how Government assesses the effectiveness of online safety legislation, regulatory measures and support services.

56. Ultimately, Government must ensure that technological innovation does not outpace the protections available to women and girls. This requires sustained collaboration between regulators, technology companies, law enforcement, civil society and organisations representing Muslim women.

Conclusion: Key recommendations

57. The evidence presented in this submission demonstrates that technology-facilitated abuse against Muslim women and girls must be understood within the wider context of violence against women and girls, anti-Muslim hostility and racism.

58. Three overarching principles should guide the Government's response:

59. Technology-facilitated abuse against Muslim women is not simply a generic online safety issue. It can involve the intersection of misogyny, anti-Muslim hostility and racism, alongside sexual exploitation, coercive control and other forms of violence. Policies and legislation must recognise these overlapping experiences.

60. Technology companies, regulators and Government must be held accountable for ensuring that online spaces and emerging technologies do not facilitate abuse. Reporting

systems, moderation processes and legal protections must be effective in practice, not simply exist on paper.

61. Muslim women and the organisations supporting them must be meaningfully involved in developing legislation, technology safety policies and regulatory responses. Their experiences and expertise should inform decision-making rather than being treated as an afterthought.

On behalf of Muslim Women's Network UK,

Neelam Rose

(Advocacy Officer)

November 2026