Northern Ireland Assembly

Research and Information Service
Briefing Paper

Paper 87/25 20 October 2025 NIAR 240-25

The Online Safety Act 2023: A summary and timeline

Dr Dan Hull

This briefing paper provides a brief summary of the Online Safety Act 2023, including a timeline of developments so far with regard to the publication of associated codes of practice and guidance.

An accompanying Topical Digest of reading material has been produced in support of this paper.

This briefing paper contains references to topics some readers may find distressing.

Key Points

- This briefing paper provides a brief overview of the Online Safety Act 2023.
- The Act establishes a new regulatory regime aimed at addressing illegal and harmful content online.
- It updates or creates the following offences: encouraging or assisting serious self-harm, cyberflashing, sending false information intended to cause non-trivial harm, threatening communications, intimate image abuse and epilepsy trolling.
- The Act confers new powers on Ofcom, establishing them as the online safety regulator.
- Ofcom is required to produce various sets of guidance and codes of practice for providers of online services to help them comply with the Act.
- Key milestones so far include the publication on 25 February 2025 of a consultation on draft Guidance: A safer life online for women and girls (final guidance is expected by end of 2025).
- From 25 July, all providers must adhere to child safety duties, including conducting risk assessments and carrying out age verification.
- Criticisms of the Act include a perception that it curtails freedom of expression, and that age verification checks may pose a risk to privacy.
- Some campaigners have said that Ofcom's efforts to restrict teenage access to harmful content have been ineffective so far.
- An inquiry by the House of Commons Science, Innovation and Technology Committee concluded that the Online Safety Act is unable to tackle the spread of misinformation.
- Responding to the consultation on 'A safer life online for women and girls', some respondents complained of a lack of understanding by authorities of the online space, a lack of instruction for platforms on how to deal with stalking behaviour, and that the overall pace of change is too slow.
- Annex 1 provides a timeline of some of the key developments, statements and publications relating to the Act.

Introduction

This briefing paper provides an overview of the Online Safety Act 2023, including an overview of its provisions, the offences which the Act updates or creates, and a description of some of the commentary and criticism of the Act so far in terms of its effectiveness in tackling online harms.

Annex 1 then provides a timeline of some of the key developments, statements and publications as the Act has come into being and then as its various powers have been enacted. The timeline also attempts to set out what further developments are expected in the remainder of 2025 and into 2026.

As the coverage of the Online Safety Act is somewhat broad, and the extent of commentary on its effects, implications and perceived shortcomings has been correspondingly wide, a Topical Digest has been prepared to accompany this paper.

1 Overview

The Online Safety Act 2023 establishes a new regulatory regime with the intention of addressing illegal and harmful content online. It imposes legal requirements on the following[1]:

- Providers of internet services which allow users to encounter content generated, uploaded or shared by other users ('user-to-user services');
- Providers of search engines which enable users to search multiple websites and databases ('search services'); and
- Providers of internet services on which provider pornographic content (pornographic content that is published by a provider and is not user-generated) is published or displayed.

The Act also confers new powers on the Office of Communications (Ofcom), establishing them as the online safety regulator. This role includes overseeing and enforcing the new regulatory regime, as well as producing various sets of

[1] Online Safety Act 2023: Explanatory Notes; see also the summary set out in Section 1 of the Act.

guidance and codes of practice which have been consulted on and then published throughout 2024 and 2025.

Key milestones in this process have included the **child safety duties** coming into force on 25 July 2025; by this date, services likely to be accessed by children are required to have completed a 'suitable and sufficient' children's risk assessment and to have implemented the safety measures.

One of the major developments which is still awaited is the publication of **final guidance on protecting women and girls online**. This guidance is expected to be published by the end of 2025.

2 Specific provisions

In summary, the Online Safety Act makes or amends the following offences:

- Encouraging or assisting serious self-harm
- Cyberflashing
- Sending false information intended to cause non-trivial harm
- Threatening communications
- Intimate image abuse
- Epilepsy trolling

The Act places a duty on providers to carry out risk assessments and to uphold a number of duties placed upon them.

To protect children, platforms must (see overleaf)[2]:

[2] For a useful summary of these measures, see: House of Commons Library, Implementation of the Online Safety Act (25 February 2025)

- Remove illegal content quickly or prevent it from appearing in the first place, including content promoting self-harm;
- Prevent children from accessing harmful and age-inappropriate content including pornographic content, content relating to suicide, self-harm or eating disorders, content depicting or encouraging serious violence or bullying content;
- Use age-checking measures on platforms where content harmful to children is published;
- Ensure social media platforms are more transparent about the risks and dangers posed to children on their sites, including by publishing risk assessments; and
- Provide parents and children with clear and accessible ways to report problems online when they do arise.

The act offers adults a 'triple shield' of protection, as follows:

- Make sure illegal content is removed;
- Enforce the promises social media platforms make to users when they sign up, through terms and conditions; and
- Provide users with the option of filtering out content that they do not want to see.

Overall, the Online Safety Act includes a wide range of provisions, including specifying a number of different offences, duties placed on providers of different forms of internet services, and substantially expanded duties and powers for Ofcom. The following paragraphs are a very brief summary of the content of the Act. However, the descriptions which follow are a summary only, and for a closer understanding of the legislation, readers should consult both the Act itself

as well as reading material suggested in a Topical Digest prepared to accompany this paper.

2.1 Part 1: Introduction

Part 1 contains an introduction section and an overview section, setting out in broad terms what is included in this Act.

2.2 Part 2: Key definitions

Part 2 contains definitions of the services to which the Act applies, including 'user-to-user' services and 'search' services

2.3 Part 3: Providers of regulated user-to-user services and regulated search services: duties of care

Part 3 imposes duties of care that apply to providers of regulated user-to-user and search services. It requires Ofcom to issue codes of practice and guidance relating to those duties.

Included within this part are the following duties:

Sections 9, 26: providers are required to carry out **illegal content risk assessments**. Sections 11, 12, 28: providers are required to carry out **risk assessments on content relating to children**.

Sections 15 and 16: providers have 'a duty to include in a service, to the extent that it is proportionate to do so, features which adult users may use or apply if they wish to increase their **control over content**', including whether or not they receive content related to suicide, deliberate self-injury or eating disorders. Users must also have the ability to control whether they see content which may be abusive towards any of the following characteristics: race, religion, sex, sexual orientation, disability, or gender reassignment.

Sections 17–19: these set out duties on providers to protect '**content of democratic importance**', **news publisher** content and **journalistic** content.

Sections 20 and 21: providers have a duty to allow users to easily **report content** which they consider to be illegal or is likely to be harmful for children, and also to have a complaints procedure.

Section 22: this Section sets out duties about **freedom of expression and privacy**, so that 'when deciding on, and implementing, safety measures and policies, (there is) a duty to have particular regard to the importance of protecting users' right to freedom of expression within the law'.

Section 29: this section defines the duties on search providers to mitigate and manage the risks of harm to children in different age groups, and to minimise the **risk of harm to children** of any age.

Sections 35–37: it is specified in these Sections that providers must carry out **children's access assessments** to determine 'whether it is possible for children to access the service or a part of the service'. This will be the case if either 'there is a significant number of children who are users of the service or of that part of it', or 'the service, or that part of it, is of a kind likely to attract a significant number of users who are children'. If a service is likely to be used by children, additional restrictions are imposed by the Online Safety Act.

Sections 41–51 specify that Ofcom must create **codes of practice** about duties on providers in relation to the following:

- Terrorism
- Child sexual exploitation and abuse offences
- Fraudulent advertising
- Illegal content
- Children's online safety
- User empowerment
- Content of democratic importance
- Journalistic content
- Content reporting
- Complaints procedures

These codes of practice must be approved by the Secretary of State and laid before parliament.

Section 52 specifies that Ofcom must create **guidance for providers** on the following:

- Assessments related to the adult user empowerment
- News publisher content
- Children's access assessments
- Record keeping and review duties
- Content that is harmful to children
- Protecting women and girls

The guidance relating to the protection of women and girls is set out in Section 54. This guidance relates to 'content and activity' which 'disproportionately affects women and girls', and covers both user-to-user and search services. The guidance may contain 'advice and examples of best practice for assessing risks of harm to women and girls'. In producing the guidance, Ofcom must consult with both the Commissioner for Victims and Witnesses and the Domestic Abuse Commissioner (both of which are specific to England and Wales). In contrast to the codes of practice referred to above, this guidance does not have to be laid before parliament and must simply be 'published'.

Sections 55–57 define what is meant by 'regulated user-generated content', 'user-generated content' and 'news publisher content', as well as 'search content' and 'search results'.

Further definitions are provided in Sections 59 and 60, including the definition of 'illegal content', 'terrorism' and 'content that is harmful to children'. Section 63 specifies that Ofcom must review the incidence of content that is harmful to children, and publish a report at least every three years.

Chapter 2 of the Act includes provisions on the **reporting of child sexual exploitation and abuse (CSEA) content**, including that providers must report all CSEA to the National Crime Agency.

Chapter 3 covers what must be set out by providers in their terms of service.

Chapter 4 makes provision regarding **deceased child users**. These Sections specify, for example, that a provider must make it clear in the terms of service what their policy is about dealing with requests from parents of a deceased child for information about the child's use of the service. A provider must have a dedicated helpline or section of the service by which parents can easily find out what they need to do to obtain information and updates in those circumstances. And providers must specify what their procedure is for the parents of a deceased child to request information about the child's use of the service. Section 76 states that Ofcom must produce guidance for providers on these issues.

2.4 Part 4: Other duties of providers of regulated user-to-user services and regulated search services

Part 4 imposes further duties on providers of regulated user-to-user and search services, including relating to user identity verification, CSEA content, and transparency reporting.

2.5 Part 5: Duties of providers of regulated services: certain pornographic content

Part 5 covers the duties of providers of regulated services in relation to pornographic content. These duties include the necessity to have a highly effective age verification system in place. Ofcom must produce guidance for internet services in this regard.

2.6 Part 6: Duties of providers of regulated services: fees

Part 6 concerns the 'qualifying worldwide revenue' of providers. As the principle is established in the Act that the cost to Ofcom of exercising their online safety functions will be met by fees charged to providers of regulated services, this part states that these fees will be calculated on the basis of the overall revenue for each provider.

2.7 Part 7: Ofcom's powers and duties in relation to regulated services

Part 7 sets out **Ofcom's powers and duties** in relation to regulated services. For example, it amends the Communications Act 2003 to include new duties, a summary of which is as follows:

Ofcom must have regard to:

- The risk of harm to citizens presented by regulated services;
- The need for a higher level of protection for children than for adults;
- The need for it to be clear to providers of regulated services how they may comply with their duties set out in the Act;
- The need to exercise their functions while taking account of the size or capacity of the provider in question, and the level of risk of harm presented by the service in question, and the severity of the potential harm;
- The desirability of promoting the use by providers of regulated services of technologies which are designed to reduce the risk of harm to citizens;
- The extent to which providers of regulated services demonstrate, in a way that is transparent and accountable, that they are complying with their duties set out in the Act.

2.8 Part 8: Appeals and super-complaints

Part 8 sets out the appeals and complaints procedures relating to regulated services. Included within this is the establishment of a super-complaints mechanism which 'enables any organisation or other entity that meets the relevant eligibility criteria to bring systemic issues to Ofcom'. Section 169 specifies what a super-complaint consists of. The Explanatory Memorandum provides the following definition:

> 'A super-complaint can be about any feature of a regulated service or conduct of the provider of such a service. It may relate to one or more regulated services or providers and may be about any combination of features and conduct. Where this feature, conduct or

combination of the two is causing, appears to be causing or is at material risk of causing users or members of the public significant harm, significantly adversely affecting their right to freedom of expression, or having a significant adverse impact on them, an eligible entity may make a super-complaint.[3]'

2.9 Part 9: Secretary of State's functions in relation to regulated services

Part 9 sets out the Secretary of State's functions in relation to regulated services.

2.10 Part 10: Communications offences

Part 10 sets out the list of offences created or updated by the Online Safet Act. In summary these are as follows:

False and threatening communications offences

S.	Offence	Details
179	False communications offence	This creates a criminal offence for the sending of 'false communications' – in other words, 'a message conveying information that they know to be false, and at the time of sending it they intend the message to cause non-trivial psychological or physical harm to a likely audience'.
180	Exemptions from false communications offence	Exemptions include messages sent by recognised news publishers or 'in connection with the showing of a film made for cinema to members of the public'.
181	Threatening communications offence	This is defined as sending a message which 'conveys a threat of death or serious harm'.

[3] Online Safety Act 2023: Explanatory Notes

Offences of threatening or showing flashing images

S.	Offence	Details
183	Offences of sending or showing flashing images electronically	This creates a criminal offence for the sending of 'a communication by electronic means which consists of or includes flashing images' where either 'it is reasonably foreseeable that an individual with epilepsy would be among the individuals who would view it' or that the sender knows or suspects the recipient 'to be an individual with epilepsy'.

Offence of encouraging or assisting serious self-harm

S.	Offence	Details
184	Offence of encouraging or assisting serious self-harm	This is defined as encouraging or assisting 'the serious self-harm of another person'. Among other means, this includes sending, transmitting or publishing a communication by electronic means, showing a person such a communication or publishing by any other means.

Offences to be inserted into Sexual Offences Act 2003

S.	Offence	Details
187	Sending etc photograph or film of genitals	This Section creates a new offence of sending a photograph or film of a person's genitals to another person.
188	Sharing or threatening to share intimate photograph or film	This Section creates the offence of intentionally sharing, or threatening to share, a photograph or film which shows, or appears to show, another person in an intimate state, without their consent.

2.11 Parts 11 and 12: Supplementary and general, interpretation and final provisions

Parts 11 and 12 contain miscellaneous and general provisions. In particular, they define key concepts such as providers of regulated services, users, and internet services.

3 Coverage and extent

The Act covers providers of internet services which have links with the UK, no matter where they are based. It includes any service which can be accessed by people within the UK. For example, Section 4 states that the Act applies to any provider of a service where:

> '(a) the service is capable of being used in the United Kingdom by individuals, and
>
> (b) there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the United Kingdom…'

For the most part, the OSA applies to the whole of the UK. However, the following sections do not apply to Northern Ireland:

- Section 187 (cyberflashing);
- Section 188 (sharing of an intimate image or film without consent);
- Section 189(2) (repeals and amendments);
- Section 190 (repeals);
- Section 213 (offence under the Obscene Publications Act 1959: Ofcom defence);
- Section 214(1) to (3) (offences regarding indecent photographs of children: Ofcom defence)

The Northern Ireland Assembly was adjourned during the passage of the Act through the Houses of Parliament so, while the Sections which did not extend to Northern Ireland may ordinarily have been dealt with through similar bills in the Assembly, this could not happen at the time.

However, with regard to Sections 187 (cyberflashing) and 188 (sharing of an intimate image or film without consent), similar offences for Northern Ireland can be found in Part 1 of the Justice (Sexual Offences and Trafficking Victims) Act (Northern Ireland) 2022. Section 2 inserts Article 72A into the Sexual Offences (Northern Ireland) Order 2008 which creates a new offence that is intended to capture the sending of an unwanted sexual image or cyber-flashing. The offence occurs where a person intentionally sends an image of sexual activity or genitals to another person without that person's consent (Section 1 of the legislation also created criminal offences relating to upskirting/downblousing by inserting Article 71A and 71B into the Sexual Offences (Northern Ireland) Order 2008). These offences all came into effect in 2023[4].

Meanwhile Section 6 also covers private sexual images and amended existing provision in section 51 of the Justice Act (Northern Ireland) 2016 which provides for the offence of disclosing private sexual photographs and films with intent to cause distress (revenge pornography). Section 51 is amended to make it an offence to threaten to disclose private sexual photographs and films with intent to cause distress.

The Department of Justice has recently published a consultation[5] which proposes to criminalise sexually explicit deepfake images (or sexual digital forgery)[6], and these may potentially be tabled at Consideration Stage of the Justice Bill[7].

4 Draft guidance: A safer life online for women and girls: practical guidance for tech companies

Ofcom is required to publish guidance setting out how providers can take action against harmful content and activity that disproportionately affects women and

[4] Northern Ireland Executive, Major milestone for sexual offences legislation (27 November 2023)

[5] Department of Justice, A Consultation on Proposals to Criminalise Sexually Explicit Deepfake Images (July 2025)

[6] For background on this issue see: Research and Information Service, Cyberflashing and deepfake pornography (January 2022)

[7] Northern Ireland Assembly, Justice Bill (at Committee Stage, as of 20 October 2025)

girls. Draft guidance and a consultation were issued in February 2025[8], with final guidance due to be published by the end of 2025.

The draft guidance focuses on four categories of online gender-based harms in particular:

- Online misogyny
- Pile-ons and coordinated harassment
- Online domestic abuse, and
- Image-based sexual abuse, including intimate image abuse and cyberflashing.

The draft guidance contains nine actions, as follows:

- Action 1: Ensure governance and accountability processes address women and girls' online safety;
- Action 2: Conduct risk assessments that focus on harms to women and girls;
- Action 3: Be transparent about women and girls' online safety;
- Action 4: Conduct abusability evaluations and product testing;
- Action 5: Set safer defaults;
- Action 6: Reduce the circulation of content depicting, promoting or encouraging online gender-based harm;
- Action 7: Give users better control over their experiences;
- Action 8: Enable users who experience online gender-based harms to make reports; and
- Action 9: Take appropriate action when online gender-based harm occurs

For each of these actions, a set of 'foundational steps' and 'good practice steps' are recommended. For the foundational steps, the draft guidance provides a set of reference points to the relevant legislation and codes, and indicates who is responsible in each case. Good practice steps are recommended so that

[8] Ofcom, A Safer Life Online for Women and Girls: Practical guidance for tech companies (draft) (25 February 2025); see also: Online Safety Act Network, Ofcom's draft guidance on protecting women and girls (2 April 2025)

providers can ‘go further if they are serious about addressing the range of harms women and girls face online’[9].

5 Reception and commentary

5.1 Commentary on the Act in general

Following the coming into force of the Online Safety Act, and during the gradual rolling out of the various regulations, codes of practice and guidance which have followed throughout 2024 and 2025 so far, a number of different organisations and bodies have commented on its implications and effectiveness.

For example, concerns have been expressed that the Act curtails freedom of expression online and that ‘social media platforms have formally become judge and jury over our speech’[10]. The age verification checks which were introduced on 25 July 2025 have caused concern for some that there may be personal data security risks, either from providing photo ID or by using a virtual private network (VPN) which may have less transparency in what data is collected and how it is treated[11].

The Online Safety Act allows Ofcom to categorise online services on the basis of size, applying additional duties only to the larger (‘Category 1’) services. This has led some campaigners to voice criticism that there remain ‘small but risky services that are set up specifically to cause harm – whether that’s encouraging suicide, or targeting minorities with hate and abuse’[12].

Some campaigners, including the Molly Rose Foundation, have said that Ofcom’s efforts to restrict teenage access to content which is not illegal but is

[9] Ofcom, A Safer Life Online for Women and Girls: Practical guidance for tech companies (draft) (25 February 2025), p.4

[10] Big Brother Watch: Five things you need to know about the Online Safety Act (16 September 2025); see also: Brit Brief, Wikipedia Challenges UK's Online Safety Act in High Court Over Free Speech Concerns (11 August 2025)

[11] The unintended consequences of the Online Safety Act The Guardian (7 August 2025)

[12] Online Safety Act Network, Background briefing: House of Lords debate on OSA categorisation regulations (20 February 2025)

harmful (including subject matter related to suicide, eating disorders and self-harm) have been ineffective so far[13].

An inquiry by the House of Commons Science, Innovation and Technology Committee concluded that the Online Safety Act is unable to tackle the spread of misinformation as it was not primarily intended for that purpose[14]. The Committee recommended that the Government creates a new and improved online safety regime, based on five fundamental principles: public safety, free and safe expression, responsibility for content, control over content and data, and technological transparency.

5.2 Commentary on draft guidance 'A Safer Life Online for Women and Girls'

As is referred to in Section 4 of this paper, Ofcom is required to publish guidance setting out how providers can take action against harmful content and activity that disproportionately affects women and girls. Draft guidance and a consultation were issued in February 2025[15], with final guidance due to be published by the end of 2025. An engagement event was hosted by Ofcom at the MAC in Belfast in May 2025. During this consultation, a number of organisations also provided a written response. The selection of responses summarised here were, in general, broadly supportive of the draft guidance. Some respondents particularly welcomed the recognition in the guidance of the specific impact of online harms on women in public life, and also the impact this may have on women and girls who may be reluctant to enter certain careers as a result[16]. The encouragement provided in the guidance for services and

[13] Molly Rose Foundation, Children's exposure t suicide, self-harm, depression and eating disorder content on social media, Research Briefing (October 2025)

[14] Science, Innovation and Technology Committee: UK's Online Safety regime unable to tackle the spread of misinformation and cannot keep users safe online, MPs warn (11 July 2025); Online Sfaety Act Network, Disinformation and disorder: the limits of the Online Safety Act (10 August 2025)

[15] Ofcom, A Safer Life Online for Women and Girls: Practical guidance for tech companies (draft) (25 February 2025)

[16] The Jo Cox Foundation, Response to Consultation on draft Guidance: A safer life online for women and girls (2025); similar recommendations have been made by the Jo Cox Civility Commission

platforms to engage with victims and experts in designing and testing their systems was welcomed in this regard.

However, there were some more specific suggestions for improving the guidance. For example, in terms of encouraging providers to follow the guidance, some organisations had suggested that using the media to highlight where providers had failed, and publish case studies of poor practice, could be effective[17]. It has also been commented on that, even where online abuse is now established in legislation as a criminal offence, 'a significant challenge we face in Northern Ireland is the lack of a robust understanding amongst authorities of the online space as a public space in its own right'[18].

The proposals that providers should work with subject matter experts and to conduct abusability evaluations and product testing were particularly welcomed. A number of consultation respondents stated that they have observed that new and 'innovative' methods are being used by perpetrators of abuse against women and girls on social media. These respondents have suggested that the onus should be on providers to prevent such methods by design, rather than reacting to abusive methods after they have become a trend[19].

While image-based abuse became a specific offence under the Justice (Sexual Offences and Human Trafficking) Act 2022, some consultation respondents have stated that it is still a distressing and difficult process for women to have non-consensual images taken down from the internet. Use of AI to create 'deep fake' images is also a significant and growing concern and it has been stated that 'companies must respond swiftly and robustly when a report is made. Where they fail to do so, action must be taken to ensure that inaction does not become the default'[20].

[17] Belfast Area Domestic and Sexual Violence and Abuse Partnership, Response to Consultation on draft Guidance: A safer life online for women and girls (2025)

[18] As above.

[19] See for example: Womens Aid NI, Response to Consultation on draft Guidance: A safer life online for women and girls (2025)

[20] As above; also, the following journal paper investigates this issue: C McGlynn and R Tuna Toparlak, 'The 'new voyeurism': criminalizing the creation of 'deepfake porn'', Journal of Law and Society, 52(2), pp. 204-228 (2025)

One of the examples of good practice highlighted in the draft Ofcom guidance is a 'trusted flagger' programme[21]. One organisation from Northern Ireland stated the following of this:

> 'It is also important to highlight that the United Kingdom comprises four distinct legal jurisdictions, each with its own justice system and victim support frameworks in relation to violence against women and girls (VAWG). In light of this, we respectfully request that trusted flagger be distributed evenly across the UK to ensure equitable access to linked support services for women and girls, regardless of their postcode.'[22]

Other positive suggestions have included a traffic light rating system to assess good practice on social media platforms.

While the 'foundational steps' and the 'good practice' steps were broadly welcomed by many of the organisations which responded to the consultation, concern was expressed by some about the pace of change. Some respondents suggested that voluntary 'good practice' (such as use of removal tools like hash matching, de-prioritising of harmful content, requiring consent for intimate images to be published and use of automated detection for materials depicting gender-based harms) should rapidly become 'foundational' for providers of online services[23].

Criticisms of the draft guidance include a lack of sufficient instruction for platforms on how to detect and deal with stalking behaviour. As one organisation describes it:

> 'Stalking involves repeated, unwanted behaviours that form a pattern over time, making the course of conduct itself the crime. Despite this,

[21] A trusted flagger programme builds relationships between providers and organisations with expertise in harms such as online domestic abuse and intimate image abuse. These partnerships can also be used to alert providers to emerging forms of harm; see draft guidance, p.51.

[22] Women's Aid NI, Response to Consultation on draft Guidance: A safer life online for women and girls (2025)

[23] Commissioner Designate for Victims of Crime for Northern Ireland, Response to Consultation on draft Guidance: A safer life online for women and girls (2025)

> platforms frequently fail to acknowledge these patterns, focusing instead on whether individual incidents meet harm thresholds. This lack of awareness impedes platforms' ability to take effective action'[24].

One of the solutions suggested is sharing of data across platforms to help identify patterns of stalking.

[24] End Violence Against Women Coalition, Response to Consultation on draft Guidance: A safer life online for women and girls (2025); see also: Suzy Lamplugh Trust, Response to Consultation on draft Guidance: A safer life online for women and girls (2025); though stalking is a priority illegal harm under the illegal harms code.