

Parliamentary briefing: Online Safety Bill

The Online Safety Bill represents a critical milestone in child protection, with potentially world leading online safety legislation that can protect children and families from unprecedented levels of online grooming and sexual abuse. MPs must take this opportunity to ensure the legislation responds to the scale of the online child abuse threat.

Although we strongly support the Government's ambition, substantive changes are needed to ensure the Bill responds effectively to online child abuse and grooming. This briefing outlines the key areas where the Bill must be strengthened to ensure an appropriately ambitious and effective response.

The Bill must:

- **Tackle the ways in which child abuse is facilitated at scale on social networks ('child abuse breadcrumbing')**
- **Introduce duties for platforms to tackle cross platform child abuse and grooming pathways**
- **Proactively tackle significant child abuse risks in private messaging**
- **Ensure the child safety duty covers all services likely to be accessed by a child, to prevent harm being displaced to smaller sites**
- **Introduce a statutory user advocacy body to protect children's interests in online harms regulation**
- **make senior managers of in-scope services personally liable for implementation of the duty of care, not just compliance with information requests**

Further detail can be found in the NSPCC's [Time to Act Report](#).

MPs can support in reaching this objective by scrutinising and challenging the Bill's ability to prevent online child sexual abuse.

For more information, briefings and advice please contact Hannah Ruschen, Senior Policy and Public Affairs Officer, hannah.ruschen@nspcc.org.uk or 07742185074.

Why does the Online Safety Bill matter?

Online child abuse is not inevitable. Over recent years, online grooming and child abuse image offences have reached record levels because social media companies failed to respond to the child abuse threat. Poor design features and commercial strategies that have often ignored child safety put children at risk from products that are fundamentally unsafe by design.

The Online Safety Bill can change this. We strongly support the ambition of the legislation, and four years after NSPCC secured the initial commitment to introduce the Bill, we commend Government for bringing it forward. **The Online Safety Bill must succeed, and the NSPCC will continue to work tirelessly to ensure it does.**

The Bill is an urgently needed child protection measure that should be judged on whether it delivers a comprehensive package of measures to **prevent inherently avoidable online sexual abuse**. Well-designed legislation **can** effectively balance the fundamental rights of all users, including children who require a higher standard of systemic protection.

As it stands, the NSPCC believes there are some crucial areas where the legislation must be strengthened to ensure a fit for purpose response to online child abuse.

This bill has never been more important. Figures below demonstrate the growing scale and complexity of online abuse that **this bill must tackle**:

1. **In 2020/21, online grooming offences reached record levels** – with the number of sexual communications with a child offences in England and Wales **increasing by almost 70% in three years**;¹
2. **Internet-facilitated abuse has seen a trend towards more serious sexual offences** against children, and the average age of children in child abuse images – particularly girls – is trending younger;²
3. In 2021, **UK law enforcement received a record 97,727 industry reports relating to online child abuse**, a 29% increase from the previous year.³

What needs to change?

As it stands, the NSPCC believes there are some crucial areas where the legislation should be strengthened to ensure a fit for purpose response to online child abuse.

The NSPCC uses a scorecard approach to assess whether the Online Safety Bill will meet our six tests for effective regulation. This scorecard sets out the NSPCC's assessment of the Bill against these tests and can be found at the end of this briefing.

For further information on how the Bill scores, please see the NSPCC's new [Time to Act](#) report.

Below, we set out how the Bill can be strengthened to protect children.

1. The Bill must address the ways in which abusers use social networks to directly facilitate online abuse at scale, but that doesn't meet the criminal threshold

The Bill needs to comprehensively cover the range of ways in which abusers use social networks to form offender networks; post 'digital breadcrumbs' that signpost to illegal content; and share child abuse videos that are carefully edited to fall within content moderation guidelines.

This range of techniques, known as **'child abuse breadcrumbing'**, must clearly and unambiguously be brought into scope of the Bill, to ensure abusers can no longer organise abuse in plain sight, and exploit social networks to signpost to child abuse content hosted on third-party messaging apps, offender forums and the dark web.

The Bill does not require companies to address 'child abuse breadcrumbing' risks as part of either their illegal content or child safety duties. The regulator should be given powers to tackle this behaviour to ensure the Bill provides a sufficiently proactive response, otherwise a crucial opportunity to disrupt child abuse will be lost. **Tens of millions of interactions with accounts that actively enable the discovery and sharing of child abuse images could potentially fall outside of regulatory scope.**

'Child abuse breadcrumbing' can take many forms, but techniques include:

- **'Tribute sites'**: where abusers create social media profiles using misappropriated identities of known child abuse survivors. These are used by offenders to connect with like-minded perpetrators, to exchange contact information, form offender networks and signpost to child abuse material elsewhere online. **In Q1 2021, there were 6 million interactions with such accounts**;⁴
- **Facebook groups**: abusers use Facebook Groups to build offender groups and signpost to child abuse hosted on third-party sites. These groups are thinly veiled in their intentions: for example, groups may be described as for those with an interest in children celebrating their 8th, 9th and 10th birthdays. Several groups with over 50,000 members remain live despite being reported to Meta, and algorithmic recommendations quickly suggest additional groups;⁵
- **Signposting abuse on social networks**: abusers are increasingly using novel forms of technology to signpost to abuse, including QR codes and the metaverse.

To address the impact of material that directly facilitates online child sexual abuse, the Bill must:

1. Amend the scope of the illegal safety duty, placing a specific obligation on companies to address content and material that can reasonably be seen to directly facilitate illegal activity;
2. identify this activity as a primary priority harm, allowing Ofcom to set out appropriate measures in its codes of practice.

2. The Bill must introduce duties for platforms to tackle cross platform child abuse

Four in five UK adults think social media companies should have a legal duty to work with each other to prevent online grooming happening across multiple platforms.

Well-established grooming pathways see abusers exploit the design features of social networks to contact children before they move communication across to other platforms, including live streaming sites or encrypted messaging services. **For example, an abuser may be grooming a child through playing video games and simultaneously building that relationship further via a separate chat platform, such as Discord.** Perpetrators manipulate features such as Facebook's algorithmic friend suggestions to befriend large numbers of children, where they can use direct messages to groom them and then coerce children into sending sexual images via Whatsapp.

No online service can assemble every piece of the jigsaw. **In order to ensure a comprehensive and effective response to child sexual abuse, the Online Safety Bill should place requirements on services to consider how abuse spreads from their platform to others (or vice versa), risk assess accordingly, or to cooperate with other platforms to proactively address harm.** Failure to do so would constrain the overall effectiveness of the Bill – this may have negative interplays with competition law, as well as impacting the Bill's ability to protect from future harms that may arise as the internet becomes more inter-connected, such as through the metaverse.

To address cross-platform risks the Bill must:

1. Require companies to tackle the cross-platform nature of harms when meeting their safety duties;
2. Ensure companies risk assess their products to address how they contribute to grooming and abuse pathways;
3. Place a new duty on in-scope services to co-operate on tackling harms, including systemic mechanisms to share intelligence on new and emerging abuse risks.

3. The Bill must strengthen approaches to child abuse risks in private messaging

Most child abuse on social networks takes place on private messaging:

12 million of the 18.4 million child sexual abuse reports made by Facebook worldwide in 2019 related to content shared on private channels⁶

We strongly welcome the Government's decision to include both public and private messaging in the scope of the Bill. However, the **legislation introduces new constraints on Ofcom's ability to tackle grooming and child abuse in private messages and groups.**

Clause 116 of the Bill introduces restrictions on Ofcom's ability to require a company to use proactive technology to identify or disrupt abuse in private messaging. This would likely restrict Ofcom from being able to include in codes of practice widely used tools such as PhotoDNA 'hash' technology to detect child abuse images, or AI classifiers used to detect self-generated images and grooming behaviour. **This raises significant questions about whether Ofcom could realistically produce a code of practice that can respond to the nature and extent of the child abuse threat.**

If the regulator is unable to proactively tackle online grooming in private messaging, the impact will be disproportionately felt by girls.

NSPCC data shows that an overwhelming majority of grooming offences target girls: **girls aged 12-15 are most likely to be victims of online grooming**. Girls were victims in 83% of offences where this data was recorded.⁷

To address child abuse risks in private messaging, the Bill must:

1. Give the regulator the ability to use its 'child sexual exploitation and abuse (CSEA) warning notice' in clause 103 where they assess harm is 'likely to occur', not only where they already have evidence that child abuse is prevalent;
2. Amend schedule 4 of Bill so that Ofcom can require the proactive use of approved technology in its codes of practice.

4. The Bill must adopt a strengthened approach to tackling harmful content for children

Highly problematic services such as Telegram and OnlyFans may be able to claim they are excluded from the child safety duties if children don't account for a 'significant' portion of their user base. This would result in lower standards of protection for children, with harmful content not being tackled, but displaced to sites that are not covered by the child safety duty.

The Online Safety Bill must tackle clearly inappropriate and potentially harmful content. While we welcome the inclusion of commercial pornography into the scope of legislation (part 5), it is still not clear which harms that impact children will be covered. **The Government should therefore set out a list of priority harms, similar to the approach of listing priority offences in schedule six and seven.**

We are also particularly concerned about the 'children's access assessment' in Clause 31 of the Bill, which assesses the likelihood of whether a child will access a service, and therefore whether the platform will be in scope of the child safety duty.

This children's access assessment sets a higher threshold than the ICO's Children's Code to decide whether a service is likely to be accessed by a child. Companies will only have to comply with the child safety duty if they have a significant number of child users or children form a significant part of each user base. **This may result in lower standards of protection, with highly problematic services such as Telegram and OnlyFans able to claim they are excluded from the child safety duties because children don't account for a 'significant' portion of their user base.** This would result in lower overall standards of protection, and **harmful content being displaced onto sites that are not covered by the child safety duty.** Additionally, online services will have a perverse incentive to stall the introduction of child safety measures until Ofcom has capacity to investigate and reach a determination on the categorisation of their site.

The child safety duty should protect children from a range of harmful content and behaviours, including all pornography, targeted harassment and bullying, the distribution of intimate images that do not meet the threshold for child abuse imagery but can still cause considerable distress; and the promotion of suicide or self-harm material, among others.

To achieve a higher standard of protection for children from legal but harmful content, the Bill must:

1. Set out proposed categories of primary priority content harmful to children as soon as possible during parliamentary passage;
2. Amend the children's access assessment to remove the 'child use test' and ensure any service that is likely to be accessed by children is within scope.
3. Ensure the children's access assessment must be updated and reviewed regularly (not only every 12 months) to capture the fastest growing harms and avoid any lag in harm identification;

5. The Government must commit to a statutory user advocacy body for children

The omission of user advocacy arrangements from the Bill means that **children who experience online sexual abuse will receive less statutory user advocacy protections than users of a post office or passengers on a bus.**

It is essential the Online Safety Bill makes provision for a statutory user advocate for children, funded by the industry levy. The Government should take this opportunity to ensure online safety regulation delivers better outcomes for children, and **and to ensure that regulation is not disproportionately skewed towards the interests of industry not children.**

Fully fledged statutory user advocacy arrangements are used in nearly all regulated consumer sectors including energy, water, post, and transport. A strong, authoritative, and resourced voice that can speak for children in regulatory debates will act as an early warning function that strengthens the overall regime, provide much needed counterbalance to industry, and **ensure complex safeguarding issues are effectively built-in to the regime.**

They play a key role in representing users, particularly vulnerable groups, and ensuring that their voices are appropriately counterbalanced against well-resourced and vocal regulated companies. Without this counterbalance, large tech companies will attempt to capture independent and expert voices; fund highly selective research with the intent to skew the evidence base; and then challenge any decisions which run contrary to the evidence base it has created. **These tactics are not new – similar tactics are used by other regulated sectors, such as the tobacco industry.**⁸

User advocacy is funded by a levy on regulated companies and is therefore neutral to the exchequer. Compared with the significant benefits and improved outcomes it will create, it represents only a minimal additional burden on regulated firms (the 10-year total costs of levy fees is estimated at £313 million.)⁹

To ensure user advocacy is incorporated into the regulation effectively, the Bill must:

1. Introduce provision for statutory user advocacy model to support the delivery and implementation of effective regulation;
2. Provide the advocacy body with powers comparable to other user advocacy organisations, such as Citizens Advice;¹⁰
3. Provide a mechanism to funding statutory user advocacy through an industry levy, in line with the ‘polluter pays’ principle, an exchequer-neutral policy within only a minimal additional burden on regulated firms.

6. The Government must hardwire the safety duties to deliver a culture of compliance in regulated firms

82% of UK adults would support the appointment of a senior manager, or safety controller, to be held liable for children’s safety on social media sites.

The Bill should be strengthened to actively promote cultural change in companies and embed compliance with online safety regulations at C-suite and Board level. A robust corporate and senior management liability scheme is highly desirable and should impose personal liability on directors whose actions consistently and significantly put children at risk.

The Online Safety Bill must learn lessons from other regulated sectors – principally financial services – where regulation imposes specific duties on directors and senior management of financial institutions, and those responsible individuals face regulatory enforcement if they act in breach of such duties.¹¹

Currently, senior managers will not be personally liable for breaching the safety duties, only where they fail to comply with information requests or willingly seek to mislead the regulator. The Government has rejected the Joint Committee’s recommendation that each company appoint a ‘Safety Controller’, at or reporting to Board level. **As a result, there is no direct relationship in the Bill between senior management liability and the discharge by a platform of its safety duties.**

This approach is **poorly targeted towards delivering child safety outcomes: as it stands, the Online Safety Bill is now weaker in this regard than the General Online Safety Bill currently being scrutinised by the Oireachtas**. Ireland's legislation includes senior manager liability for both regulatory breaches and a failure to cooperate with investigations.

To ensure the safety duties are hardwired across in-scope services, to deliver the necessary cultural change across the tech sector, the Bill must:

1. Extend senior management liability to cover substantive product decisions, not simply a failure to cooperate with the regulator;
2. Require companies to appoint a senior manager (Safety Controller) who is personally liable for whether a platform meets its safety duties;
3. Info disclosure duties to put the onus on companies to disclose relevant info to the regulator;
4. Approve risk assessments at Board level.

What can Parliamentarians do to ensure the Online Safety Bill will effectively tackle child abuse online?

It is vital that the Government address these substantive concerns in the Online Safety Bill during parliamentary scrutiny. **Your support can ensure child protection is front and centre of this legislation and future regulation.**

You can do this by:







- Working with the NSPCC to **table and support amendments at report stage** to address these issues.
- Raising these issues across Parliament with **written and oral questions**, and with the DCMS Ministerial team.
- Becoming an active **supporter of the NSPCC's Wild West Web campaign**.
Find out more at <https://www.nspcc.org.uk/support-us/campaigns/end-child-abuse-online>

The NSPCC can support you with briefings, amendments, and advice. To arrange a meeting and discuss how we can work together to achieve this, please contact Hannah Ruschen, Senior Policy and Public Affairs Officer, hannah.ruschen@nspcc.org.uk or 07742185074.

Notes

- 1 NSPCC data on a freedom of information request to police forces in England and Wales, August 2021
- 2 Salter, M; Whitten, T. (2021) An analysis of pre-internet and contemporary child sexual abuse material. Deviant Behaviour, forthcoming
- 3 Data provided by the National Centre for Missing and Exploited Children (NCMEC)
- 4 WeProtect data generated by Crisp Consulting.
- 5 Putnam, L (2022) Facebook Has a Child Predation Problem. New York City: Wired. Article published 13th March 2022. Based on subsequent discussions with Prof Lara Putnam at the University of Pittsburgh
- 6 NSPCC Freedom of Information request to police forces in England and Wales, August 2021
- 7 NSPCC Freedom of Information request to police forces in England and Wales, August 2021
- 8 For example, see Abdalla, A; Abdalla A. (2021) The Grey Hoodie Project: Big Tobacco, Big Tech, and the Threat on Academic Integrity. Proceedings of the 2021 AAAI/ACM Conference on, Ethics and Society. Toronto: University of Toronto; Cambridge, MA: Harvard Medical School.
- 9 HM Government (2022) Online Safety Bill Risk Assessment. London: HM Government
- 10 Consumer, Estate Agents and Redress Act, 2007.
- 11 Chiu, I (2016) [Regulatory duties for directors in the financial services sector, and directors duties in company law](#) – Bifurcation and Interfaces. Journal of Business Law, 2016. Page,

NSPCC’s six tests assessment of the Online Safety Bill

	Test	Scoring	Justification
1	Regulation must have at its heart, an expansive principles-based Duty of Care , capable of driving cultural change		The overarching framework of regulation focuses on systems and processes. However, it is unnecessarily complex and much of the regime is contingent on Ofcom developing the regulatory scheme post Royal Assent.
2	Regulation must meaningfully tackle child sexual abuse		The Bill has a clear emphasis on tackling online sexual abuse. However, it needs to more effectively address cross-platform risks, risks in private messaging and child abuse breadcrumbing.
3	The Duty of Care must meaningfully address legal but harmful content , including how content is recommended and disseminated to users		The Bill offers higher protection to children. However, the ‘children’s access assessment’ may leave problematic platforms, such as OnlyFans and Telegram, out of scope from the child safety duties.
4	There should be effective transparency requirements and investigation powers for the regulator, with information disclosure duties on regulated firms		Ofcom has an effective suite of investigatory powers. However, online services should have information disclosure duties.
5	We need to see an enforcement regime capable of incentivising cultural change , which should include senior management liability for product decisions, and financial and criminal sanctions		Ofcom has strong financial levers. However, the personal liability powers should be extended to cover substantive product decisions.
6	There needs to be statutory user advocacy arrangements for children , including a dedicated user advocacy body funded by the industry levy, so children have a powerful voice that counterbalances that of industry		The Bill does not include statutory user advocacy arrangements.