NSPCC

Parliamentary Briefing: Report Stage of the Online Safety Bill, July 2022

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 and complexity of the online child abuse threat.

Following Committee Stage, Government has tabled some important amendments which we encourage members to support, tackling child abuse facilitation on social networks (breadcrumbing) and high-risk design choices such as private messaging using CSEA warning notices.

Although we strongly support the Government's ambition and recent amendments, **there remain key areas where the Bill must go further to stop preventable online child sexual abuse**. Members now have the opportunity to support the substantive changes that are needed to ensure the Bill responds effectively to online abuse and grooming.

This briefing outlines the key areas where the Bill must be amended to ensure an appropriately ambitious and effective response.

The Bill must:

1. **Tackle the ways in which child abuse is facilitated at scale on social networks ('child abuse breadcrumbing')**
2. **Introduce duties for platforms to tackle cross platform child abuse and grooming pathways**
3. **Address significant child abuse risks in private messaging, through the Codes of Practice.**
4. **Prevent design choices that pose a high risk of child sexual abuse.**
5. **Adopt a strengthened approach to addressing harmful content for children.**
6. **Introduce a statutory user advocacy body to protect children's interests online**
7. **Hardwire the safety duties to deliver a culture of compliance in regulated firms, through senior manager liability and the publication of risk assessments.**

Additionally, we are very concerned about the introduction of government amendment NC14 which could undermine effectiveness of the priority illegal offences, including child sexual abuse, and we encourage MPs to voice their concerns about this clause during the debate.

Further detail on our assessment of the Bill can be found in the NSPCC's **Time to Act Report.**

For more information, case studies and speaking material 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 Committee can amend the legislation to ensure a fit for purpose response to online child abuse.

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

1. **Online grooming offences have increased by 84 per cent in four years** - with the number of sexual communications with a child offences in England and Wales **reaching record levels in 2021/22**;[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]

Below, we set out where MPs can support important amendments that can strengthen the Bill and protect children from harm.

1. The Bill must comprehensively tackle how online child abuse is facilitated at scale on social networks

In response to NSPCC concerns, the Government has tabled several important amendments that will tackle the range of ways in which abusers use social networks to perpetuate harm, often in plain sight and within the threshold of legality to evade detection.

Abusers can form offender networks; post 'digital breadcrumbs' that signpost to illegal child sexual abuse content elsewhere online; and share child abuse videos that are carefully edited to fall within content moderation guidelines.

'**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.

Amendments 58-61 and 102 –

We strongly encourage MPs to support **government amendments 58, 59 and 60**, which will require companies to consider as part of the risk assessment process how their services can be used for the commission or facilitation of priority offences, including online child sexual abuse.

MPs should also support **amendment 61**, which requires companies to effectively mitigate and manage the risks of child abuse breadcrumbing when discharging their illegal safety duty; and **amendment 102** which requires Ofcom to prepare risk profiles relating to the commission and facilitation of such priority harms.

Amendments 15 and 16 –

In addition to the government amendments (58-61 and 102), we urge MPs to support **amendments 15 and 16**, these measures will significantly strengthen the Bill's ability to proactively disrupt and prevent online child abuse, in respect of content which reasonably foreseeably facilitates or aids the discovery or dissemination of CSEA content. The amendments will ensure that we **bring into scope tens of millions of interactions with accounts that actively enable the discovery and sharing of child abuse material**.

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. However, **the current drafting of the Online Safety Bill does not explicitly place requirements on services to consider how abuse spreads from their platform to others (or vice versa) to cooperate with other platforms to proactively address harm.** Failure to do so will inevitably 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 online services becomes more interconnected, such as through the metaverse.

Amendments 17-19

17- We strongly encourage MPs to support **amendment 17,** which would place an explicit requirement on companies to consider cross-platform risk when undertaking risk assessments and would put beyond doubt the intended responsibilities on companies set out by the Minister during Bill Committee.

18- MPs should support **amendment 18**, which would require companies to address how a service may be used to signpost users to child abuse content hosted on third party sites.

19- Finally, **amendment 19** places a clear and unambiguous duty on companies to collaborate to address cross-platform risks, and to take reasonable and proportionate measures to prevent the encountering or dissemination of child abuse content, for example through intelligence sharing on new and emerging threats.

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

Most child abuse on social networks take place on private messaging**: 12 million the 18.4 million child sexual abuse reports made by Meta worldwide in 2019 related content shared on private channels.**

If the regulator is unable to tackle online grooming sufficiently in private messages, the impact will be disproportionately felt by girls. NSPCC data shows that an overwhelming majority of criminal offences target girls: girls aged 12 to 15 are most likely to be victims online grooming**. Girls were victims in 4 out of every 5 offences where this data was recorded this year.**

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 in private messages and groups.

Clause 116 of the Bill introduces restrictions on Ofcom's ability to require companies to use proactive technology to identify or disrupt the peace in private messaging.

This would likely restrict Ofcom from being able to include in codes of practice widely used tool such as Photo DNA '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 responds to the nature and extent of the child abuse threat.**

Amendment 196-

We urge MPs to support **amendment 196**, which would amend schedule 4 so that **Ofcom can require the proactive use of approved technology in its codes of practice**.

This will allow the regulator to guarantee proactive scanning technology is in use, including current industry standard technologies and any technologies developed through their best endeavours, ensuring an adequate response to the known nature and scale of the child abuse threat in private channels.

In the absence of clear requirements set out in Codes, we envisage **some companies might choose to discontinue or delay the rollout of proactive scanning technology, preferring to receive CSEA warning notices that provide an explicit legal instruction**. This could have significant short to medium term implications: for example, **when Facebook stopped scanning under analogous circumstances in the European Union, child abuse reports in the EU dropped by 76 per cent year-on-year.**[6]

NC38 and amendment 153–

MPs should **reject new clause 38 and amendment 153**, which would stop Ofcom from acting against child abuse on end-to-end encrypted platforms. The NCA says referrals from social media companies led to 500 arrests and safeguarded 650 children every month in the UK, but **this would become "much more challenging" to achieve under widespread use of end-to-end encryption**.[7] The Bill should be technology neutral and regulatory action based on the risk services pose to children. This clause, if accepted, may also disrupt the objective of Government amendments under **new clause 11** aimed to incentivise platforms to innovate and develop technologies that protect both children and encryption.

4. The Bill must tackle design choices that pose a high risk of child sexual abuse

We strongly welcome the Government amendments to the legislation that provide Ofcom with additional powers to implement CSEA warning notices for high-risk design features and require companies to use accredited technologies to identify and address CSEA content on their platform. These amendments will ensure that design choices which pose a high risk of being exploited to conduct child sexual abuse online, such as livestreaming or private messaging, must be mitigated with appropriate safety by design features.

NC11–

We urge MPs to support **new clause 11,** which provides Ofcom with significant additional powers that will enable them to address companies that rollout high risk design choices without first putting appropriate child safety safeguards in place.

Under the clause, Ofcom will be able to issue CSEA warning notices that would require companies to use accredited technology to identify or prevent users from encountering child abuse content; and / or require companies to use their best endeavours to develop technology that can detect and disrupt abuse.

This is particularly important to stop companies being able to game the legislation: for example, Meta intends to proceed with end-to-end encryption of its messaging products, **but while it is actively developing technology to enable it to scan encrypted messages for targeted advertising,**[8] **it has ruled out developing the same technology to enable continued detection of child sexual abuse material and grooming**.[9]

There are a variety of novel technologies emerging which could allow for continued CSAM scanning in encrypted environments, whilst retaining the privacy benefits afforded by end-to-end encryption. For example:

- Apple has developed its **NeuralHash technology** which allows for on-device scans for CSAM, before the message is sent and encrypted. This 'client-side' implementation rather than 'server-side' encryption means Apple does not learn anything about images that do not match the known CSAM database. Apple servers flag accounts exceeding a threshold number of images that match a known database of CSAM image hashes so that Apple can provide relevant information to the National Centre for Missing and Exploited Children (NCMEC). This process is secure and is expressly designed to preserve user privacy.
- Homomorphic encryption technology can also perform image hashing on encrypted data without the need to decrypt the data. No identifying information can be extracted, and it does not reveal any details about the encrypted image, whilst allowing for calculations to be performed on encrypted data, for example hash scanning.
- Experts in this space, including Professor Hany Farid at Berkeley who developed PhotoDNA, the current industry standard tool used to detect child abuse images online, insist that scanning in end-to-end encrypted environments without damaging privacy will be possible, if companies commit to providing the engineering resource to work on this.

Amendment 195-

We encourage MPs to also support **amendment 195**, which would further streamline Ofcom's ability to deploy CSEA warning notices, specifically by enabling them to **issue notices to multiple companies that share high risk design characteristics**, as determined by Ofcom's risk profiles under section 84.

This will enable Ofcom to multiple platforms that feature high risk design choices, rather than acquiring the regulator to go through the cumbersome process of preparing issuing warning notices on a provider-by-provider basis.

5. 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), we are still concerned that not all harms that impact children will be covered.

The Government outlined in a written Ministerial statement an indicative list of primary priority content for children, which is welcomed.[10] However, there is a glaring omission with regards to **intimate image abuse of children that doesn't meet the criminal threshold of a child abuse image but can still cause real and significant harm to young people, such as semi-nude self-generated images** that may not classify as a child abuse image but can still be consumed as child sexual abuse material. We urge Government consider how these images would sit in any indicative list of priority content and the impact this can have on children, in particular girls.

We are also 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.

Amendment 162-

The NSPCC is supporting **amendment 162** to amend the legislation through the **removal of the child use test**. This amendment removes the requirement for there to be a "significant" number of child users on a site to require compliance with child safety duties and replaces it with a "number" of child users, which will ensure any service that is likely to be accessed by children is within scope of the child safety duty.

NC18-

We urge Members to support **new clause 18**, to **ensure provisions to empower users online are extended to children**. Clause 14 of the Bill includes provisions for adult **user empowerment duties**, to empower adult users to have more control over their online experience and choose whether to be exposed to harmful content. For instance, adult users can choose to filter out content posed by users which have not verified their identify. These provisions should also be extended to children, to ensure that they are given the same agency as adults over their online experience.

6. 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 Bill's proposals are wholly insufficient to ensure online safety regulation delivers better outcomes for children, and **we are concerned that regulation will be 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.**[11]

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.)[12]

NC28-

The NSPCC is supporting **New Clause 28** to ensure that children at risk of online harms including child sexual abuse are represented by a levy-funded statutory user advocacy body, comparable to arrangements in multiple other sectors. We urge members to support **NC28** to ensure a strong, authoritative, and resourced voice for vulnerable children online.

7. 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 to be held liable for children's safety on social media sites.

The Bill must 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 needed, that imposes 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.[13]

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.**

The NSPCC is supportive of several amendments in this area, which will contribute towards delivering these objectives through the below amendments.

NC17-

The NSPCC is supportive of **new clause 17** which would introduce **liability for directors for compliance failure**, enabling Ofcom to exercise enforcement powers against individual directors for failing to comply with any enforceable requirements under section 112. We urge Members to support this amendment at Report Stage to ensure effective compliance in regulated firms.

NC27-

We ask MPs to support **new clause 27**, which will also help to hardwire compliance across in-scope companies by requiring category 1 services to **publish their risk assessments** in full on their website.

It is positive to see commitment in a recent Ministerial statement that government intend to require the highest risk companies to publish a summary of their illegal and child safety risk assessments and submit these in full to Ofcom.[14] **However, full transparency of risk assessments will be vital to civil society groups looking to assess and identify any areas where a company may not be meeting its safety duties, and to make full and effective use of the proposed super complaints mechanism**. Current experience is that companies are unwilling to share risk assessments, even when requested to do so, and published summaries are unlikely to include the necessary information needed for effective scrutiny to protect children online.

Concerns with New Clause 14: Ensuring the consistent and appropriate application of the illegal safety duty

We are concerned that the Government's **new clause 14** could significantly undermine the of the effectiveness of the Bill to tackle priority illegal offences, including child sexual abuse.

The new clause attempts to provide clarification about how online services should determine whether content should be considered illegal, and therefore the illegal safety duties should apply. However, we have concerns that the clause is likely to have the problematic effect of significantly reducing the amount of illegal content that is correctly identified and actioned.

For example:

- Companies will be expected to determine if content is illegal based on information that is "reasonably available" to a provider, with reasonableness determined in part by the size and capacity of the provider. This could present the risk that smaller platforms may effectively be subject to a less onerous application of the illegal safety duty, with malign actors incentivised to migrate illegal activity to smaller sites that have less pronounced regulatory expectations placed upon them. Conversely, it is possible that larger sites could argue that their size and capacity, and the corresponding volumes of material they are moderating, means the information is not reasonably available to reliably and consistently identify illegal content.
- Subsection 6 requires the provider to have reasonable grounds to infer that all elements necessary for the commission of an offence, including mental elements, are present and satisfied. We are concerned that this amendment could significantly raise the threshold at which companies are likely to determine content is illegal. In practice, we have routinely seen companies fail to remove content where there is clear evidence of legal intent, for example in cases of child abuse breadcrumbing and how they operationalise definitions of what constitutes a child abuse image for moderation purposes. We have concerns that some companies may seek to 'game' this clause through an application of 'mens rea' that minimises their regulatory obligations to act.
- The clauses of NC14 do not appear to be adequately future proofed. For example, it states that judgements should be made based on all relevant information that is reasonably available to the provider. However, on Meta's Oculus Quest product (its first metaverse device) the company only records on a rolling basis the previous 2 minutes of footage, making it more difficult to detect evidence of grooming. Our concern is, in a scenario like this, companies may rely on this provision to argue they cannot detect illegal content because the information is not reasonably available to them and so not take action.

We would welcome MPs exploring the implications of this amendment in Report Stage debate. We encourage MPs to voice their concerns about this clause and press the Government to ensure the Bill maintains a consistent and effective response to priority illegal offences, including child sexual abuse online.

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) Am 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 NCMEC (2021) Impact of the Electronic Communication Code
7 NCA reporting on police response to online child abuse, https://www.theguardian.com/uk-news/2022/jan/22/nca-says-end-to-end-encryption-challenge-law-enforcers
8 Meta is developing a technique called homomorphic encryption, which enables companies to read and analyse data while it remains end-to-end encrypted. Microsoft and Google are also working on such approaches.
9 For example, WhatsApp boss Will Cathcart ruled out using the technology to detect CSA, seemingly driven by the company's ideological and strategic stance
10 Written Ministerial Statement on 7 July 2022, UIN HCWS194. https://questions-statements.parliament.uk/written-statements/detail/2022-07-07/hcws194
11 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.
12 HM Government (2022) Online Safety Bill Risk Assessment. London: HM Government
13 Chiu, I (206) Regulatory duties for directors in the financial services sector, and directors duties in company law – Bifurcation and Interfaces. Journal of Business Law, 2016. Page,
14 Ministerial Statement made on 7 July 2022, UIN HCWS193 https://questions-statements.parliament.uk/written-statements/detail/2022-07-07/hcws193

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

The NSPCC can provide statistics, case studies Childline data and further briefing on any of these points above. Please contact Hannah Ruschen, Senior Policy and Public Affairs Officer, at hannah.ruschen@nspcc.org.uk or 07742185074.