Tackling Online Abuse: Written evidence submitted by NSPCC on 13/10/2021 (TOA0019)

The NSPCC is the UK's leading children's charity, preventing abuse and helping those affected to recover. Our work to keep children safe from abuse online has played an instrumental role in the development of the Government's online harms proposals.

The NSPCC has been at the forefront of the campaign for online harms legislation that introduces a social media regulator. Last year the NSPCC set out six tests that the Online Safety Bill must meet if it is to effectively tackle online child abuse, which included introducing a Duty of Care on tech companies. The draft Online Safety Bill is now subject to pre-legislative scrutiny. It has potential to deliver a robust but proportionate systemic approach, that requires platforms to proactively identify and mitigate the potential risks to children. However, we have significant concerns about whether the draft Bill is suitably ambitious to protect children from preventable and avoidable online abuse.

1. The scale and impact of online abuse on internet users, including disabled people, the LGBT+ community and other minority groups

The scale and impact of harmful content and communication online poses various risks for children and young people. We know that unsuitable content or behaviour online can have a significant impact on a young person's wellbeing, and throughout the course of the pandemic we have seen an increase in both legal but harmful content online as well as illegal child sexual exploitation and abuse. The pandemic has compounded a variety of broader issues that already existed in the online space. For children, we know that the online environment poses specific risks to their safety and wellbeing, including online bullying and harassment, exposure to harmful content, contact or conduct as well as sexual exploitation and abuse.[1]

Exposure to harmful content online

Pre-pandemic, Ofcom research compiled in our NSPCC 'how safe are our children?' report, shows that 31 per cent of children aged 12 to 15 report seeing worrying or nasty online content. 16 per cent of surveyed primary school children and 19 per cent of secondary school children said they had seen content which encouraged people to harm themselves. Similar data from children aged 11 to 18 shows that 33 per cent reported seeing the bullying of others online, and 29 per cent saw violent images or videos.[2] Childline counselling sessions about online bullying had increased by 88 per cent from 2011-2016, with these numbers continuing to rise.[3]

---

[1] And because of this they warrant special protection, in particular with reference to UN General Comment no. 25, https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx and GDPR article 8 and recital 38. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-rights-do-children-have/

[2] 'How Safe are our Children?' Report, NSPCC, 2019. https://learning.nspcc.org.uk/media/1747/how-

The pandemic has fundamentally changed the way that we interact and communicate online, as well as changing the nature and dynamics of online abuse. As a result, half of children and teens have been exposed to harmful online content during coronavirus lockdowns, often daily. 47% of teens say they have seen content online they wish they hadn't seen whilst in lockdown, and one in seven see inappropriate content every day.[4]

Recent research from Ofcom published during the pandemic shows that half of 12-15 year olds have had some form of negative experience online, including: being contacted by a stranger online, seeing or receiving something scary or troubling, seeing something of a sexual nature or, feeling pressure to send photos or information about yourself or others online.[5]

Harmful content online is a particularly prevalent issue for minority groups. For example, recent research from the TIE campaign into LGBTQI+ young people's experiences of online behaviour during lockdown, reported that more young people had seen or experienced both inappropriate content, as well as specifically homophobic and transphobic remarks and bullying since coronavirus. [6] Similarly, research conducted by Brook/CEOP found that LGBTQ+ groups are more likely to use online platforms to meet people for relationships, but also more likely to be 'cat fished' - meaning lured into a relationship online with someone using a fake identity.[7]

Online child sexual abuse

During the pandemic, we have also seen a dramatic increase in online child sexual abuse. There was a record-high 70% increase in Sexual Communication with a Child offences recorded between April 2020 and March 2021. Almost half of the offences used Facebook owned apps, including Instagram, WhatsApp and Messenger.[8] The Internet Watch Foundation saw a 77% increase in reports of 'self-generated' child sexual abuse material in 2020,[9] and NSPCC helplines saw a 60%

safe-are-our-children-2019.pdf
[3]'What children are telling us about bulling' Childline Bullying Report, NSPCC, 2016. https://learning.nspcc.org.uk/media/1204/what-children-are-telling-us-about-bullying-childline-bullying-report-2015-16.pdf
[4] BBFC (2020) https://www.bbfc.co.uk/about-us/news/half-of-children-and-teens-exposed-to-harmful-online-content-while-in-lockdown
[5] Ofcom (2021) https://www.ofcom.org.uk/__data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf
[6] 'Online in lockdown', Time for Inclusive Education (TIE), 2020, https://www.tiecampaign.co.uk/reports
[7] McGeeney, E., & Hanson, E. 'Digital Romance: A research project exploring young people's use of technology in their romantic relationships and love lives.' London: National Crime Agency and Brook, 2017. http://legacy.brook.org.uk/data/DR_REPORT_FINAL.pdf
[8] NSPCC (2021) https://www.nspcc.org.uk/about-us/newsopinion/2021/online-grooming-record-high/
[9] IWF (2021) https://www.iwf.org.uk/news/call-experts-help-tacklegrowing-threat-'self-generated'-online-child-sexual-abuse-material

increase in the number of contacts concerning online child sexual abuse, compared to the period before the pandemic.[10]

How corona virus has changed the nature of online abuse

The development and expansion of new online technologies throughout the pandemic has increased the scale and impact of online abuse. For example, live streaming and video chatting - children livestream in far larger numbers than previously understood.

NSPCC research into this issue shows that 24 per cent of all children (19 per cent primary-aged children and 29 per cent of secondary-aged children) have taken part in a livestream broadcast, 24 per cent of those primary school children were made to feel uncomfortable when livestreaming, and 6% of all children have received requests to change or remove their clothes whilst livestreaming. Additionally, 12 per cent of all children have video-chatted with someone that they do not know in person, and during those video chats 10% of primary aged and 11% of secondary aged children have been asked to take off or remove their clothes.[11] This usage has increased throughout the pandemic, where new and emerging technology has contributed to the increased risk children face of being groomed. In a rush for market share, platforms have rapidly expanded these products before appropriate safety measures can be developed and rolled out, or with deeply concerning design features, such as the ability for anyone to join a video chat and share their screen, that clearly prioritise user growth over safety.

An increase in this kind of content is particularly concerning given that technical and moderation responses to this distribution are far behind the technology available for still images. More work is needed to understand how these long-term changes to working patterns may result in continued higher demand for child abuse images, and an increase in grooming to fuel it.

2. Government proposals to tackle the issue, including the Online Harms White Paper

The Online Harms Bill is now more urgent than ever. The pandemic has highlighted the need for better proactive detection and disruption of abuse, rather than implementing safety features that work to mitigate harm after the abuse has occurred.
Facebook reported more than 21 million child sexual abuse images on its platforms in 2020, more than any other company.[12] Whilst it positive to see action being taken to remove this content, these figures show a clear need for proactive design

[10] NSPCC (2020) The impact of the coronavirus pandemic on child welfare: online abuse London: NSPCC
[11] 'Live-streaming and Video-chatting Snapshot', NSPCC Learning, 2018. https://learning.nspcc.org.uk/media/1559/livestreaming-video-chatting-nspcc-snapshot-2.pdf
[12] '2020 reports by Electronic Service providers', National Center for Missing and Exploited Children, 2020. https://www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf

features to be implemented, that prevent the dissemination and distribution of child sexual abuse material before it is produced and shared on social media platforms.

The NSPCC has always recognised the need to draft this complex legislation carefully, and it is now vital that the Government strengthens the Bill in a number of key areas to deliver a suitably bold and ambitious approach:

1. **Regulation must have, at its heart, an expansive principles-based duty of care, capable of driving cultural change**

Although the draft Online Safety Bill proposes a largely systemic approach, it does not propose an overarching general safety duty. The draft Bill should set out an overarching safety duty that 'sits above' the different safety duties that are proposed. This overarching safety duty would provide clarity to a structurally complex piece of legislation and keep the resulting range of secondary legislation, codes and guidance focused on its fundamental safety objectives.

2. **Regulation must meaningfully tackle child sexual abuse**

The draft Bill fails to tackle the way online abuse spreads across platforms through well-established grooming pathways, in which abusers exploit the design features of social networks to make effortless contact with children. The Bill needs to introduce a duty on Ofcom to address cross-platform risks, and to place a clear requirement on platforms to co-operate on cross-platform risks and respond to cross-platform harms when discharging their safety duties. The scope of the safety duty on illegal content should be amended to treat material that directly facilitates abuse with the same severity as illegal content.

3. **The Duty of Care must meaningfully address legal but harmful content, both content and how it is recommended to users**

The Online Safety Bill must tackle clearly inappropriate and potentially harmful content. This includes material that promotes or glorifies suicide and self-harm, which most major sites prohibit but often fail to moderate effectively. In many cases, the potential for harm is likely to come from platform mechanisms that promote or algorithmically recommend harmful content to users.

Additionally, the way the draft Bill defines harm runs the risk of offering lower standards of protection to children than has been established in the Video Sharing Platforms regulation, which sets out to protect all children under the age of 18 from 'material that might impair their physical, mental or moral development'. Clause 45(3) of the draft Bill defines harmful content as having a 'significant adverse physical or psychological impact on a child of ordinary sensibilities', and is unclear if platforms should consider the cumulative impact of content, including material recommended as a result of algorithmic design choices. The Government

should ensure future legislation does not provide lower levels of protections for children online than current regulation provides.

4. **There should be effective transparency requirements and investigation powers for the regulator, with information disclosure duties on regulated firms**

Information disclosure duties could play a valuable role in hardwiring safety duties into corporate activity. It is therefore disappointing the Government has failed to integrate this aspect of regulatory design into the proposed approach, particularly given how effectively this works in financial services.

5. **We need to see an enforcement regime capable of incentivising cultural change, which should include senior management liability, and criminal and financial sanctions**

Senior managers exercising a 'significant influence function' should be subject to a set of conduct rules that incentivise senior managers to internalise their regulatory requirements when setting business strategy and taking operational decisions. Under such a scheme, the regulator could bring proceedings against senior managers that breach their child safety duties, with proportionate sanctions such as fines, disbarment or censure.

6. **There needs to be user advocacy arrangements for children, including a dedicated user advocate voice, funded by the industry levy, so children have a powerful voice in regulatory debates.**

Effective user advocacy is integral to the success of the regulatory regime. The draft bill doesn't include user advocacy measures, but the Government has committed to bringing forward proposals during pre-legislative scrutiny. While this is welcome, the Government needs to be much more ambitious in its plans. It is essential the Online Safety Bill makes provision for a statutory user advocacy voice for children, funded by the industry levy. Statutory user advocacy is vital to ensure there is effective counterbalance to well-resourced industry interventions, and to enable civil society to offer credible and authoritative support and challenge.

The Minister for Digital, Culture, Media and Sport Nadine Dorries has signalled her support for prioritising child protection in this legislation, so it is vital that the Government address these substantive concerns in the draft Online Safety Bill during the period of pre-legislative scrutiny. The NSPCC estimates suggest that there are up to 90 reports of online child sexual abuse every day – we must act now to avoid further harm.[13]

3. **Legal and technological solutions to take action against people who commit online abuse**

---

[13] 'Estimated 90 cybercrimes recorded a day against children', NSPCC, 2020. https://www.nspcc.org.uk/about-us/news-opinion/2020/cybercrimes-against-children/

Legal solutions

Legal solutions to the removal of harmful content and conduct for children should focus on the young person's right of erasure through GDPR legislation. For example, if a photo of themselves is uploaded maliciously without their consent, that individual is able, under GDPR law, to ask for the photo to be removed. Sites are not currently operationalising this right that already exists under UK law, and therefore future legal solutions should work to practically apply this aspect of existing legislation. As part of a joint initiative, the NSPCC and IWF have developed an online 'Report Remove' tool using this legal function, allowing children to report images of themselves known to be online, and then remove these images, following right to erasure legislation.[14]

In parallel to the Online Safety Bill, the Law Commission has proposed substantive changes to the legal framework on communications offences. This includes a new harm-based communications offence; an offence of encouraging or assisting serious self-harm;[15] and intimate image-based offences, including an offence of taking or sharing an intimate image without consent.[16] While these proposals are to be welcomed, not least because criminal law has failed to keep pace with the growing risks of technology-facilitated abuse, the lengthy timescales associated with this work means this will at best be happening simultaneously with parliamentary passage, and alongside the development of Ofcom's regulatory scheme. Substantial areas of harm, including material that facilitates child sexual abuse and that encourages or incites self-harm, might in future be reclassified as relevant criminal offences. This creates significantly high levels of ambiguity for parliamentary scrutiny, and uncertainty around legal definitions of harm online.

Technical solutions

Technological solutions used by companies to protect against online harms on their platforms need to consider the age and stage of the child using the site, and consider the appropriate changes over the course of a child's life that should shape online approaches to harmful content and conduct. For example, this could develop from a walled garden approach for the youngest users, filtering and blocking inappropriate language, phone numbers or harmful communications, and then adapting and modifying these protections as users age. As part of developing technical solutions with age in mind, companies need to have an awareness of the age of their users, taking a proactive approach to using data to profile users and place them within age bands, better understanding their users and the risks they may face, whilst developing appropriate responses accordingly.

---

[14] 'Report Remove', Childline, 2020. https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online/#:~:text=if%20you're%20having%20problems,the%20title%20'Report%20Remove'.

[15] Law Commission (2021) Modernising Communications Offences: final report. London: Law Commission

[16] The final recommendations on intimate image based offences will not be published until spring 2022.

Technological solutions to the risks posed by private messaging will also be an integral part of future responses to online abuse. In 74 per cent of cases where children were messaged first by someone they hadn't met in person, they were initially contacted through private messages.[17] We know that private messaging can be a major source of abuse, and are therefore pleased to see private messaging included in the scope of the draft Bill, and the regulator be given powers to compel companies to use approved technologies to detect child abuse content on their platforms under a 'technology warning notice' (Clause 63). However, we are concerned that the proposals may set the threshold too high for the regulator to use these powers. Ofcom may find itself in a 'Catch 22' of being unable to use the technology warning notice: it must first demonstrate there is persistent and prevalent abuse, but may find itself unable to do so because of design choices such as end-to-end encryption that significantly erode reporting capability and abuse volumes.

Action against anonymity and online abuse

Technical solutions to the abuse risks posed by anonymous accounts online should consider how introducing friction into the user experience of anonymous accounts at the point of harm, and other design feature changes that take a safety by design approach to anonymity, could mitigate the risk posed by these accounts.

The NSPCC recognises that online anonymity is a complex issue, where anonymity is a clear driver of illegal and harmful activity, but can also provide benefits and protections to vulnerable groups such as LGBTQ+ children and young people, who may use anonymity to explore their sexual and gender identity.

We oppose any outright ban on online anonymity, but consider that the key harms and risks posed by anonymous accounts should be addressed through adopting a risk mitigation strategy as part of the framework to be set out in the draft online safety bill.

Platforms are not neutral actors, and as such the regulator, Ofcom, should actively require companies to address the content and behaviour risks that stem from online anonymity, with enhanced risk assessment mechanisms for high-risk platforms built around anonymity as a central design choice. As part of in-scope platforms Duty of Care requirements, active steps should be taken to mitigate the potential risks of anonymous accounts online, adopting a safety by design approach that will help to both mitigate harms without removing benefits for vulnerable groups of users.

---

[17] Office for National Statistics (2021) children's online behaviour in England and Wales: year ending March 2020. Newport: ONS