NSPCC Scotland - Criminal Justice Committee on tackling online child abuse, grooming and exploitation. May 2023.

What is currently defined as online child sexual abuse?

- Online grooming.
    - This will sometimes lead to contact ('in real life') abuse. Sometimes the grooming will remain online, with the offender then exploiting the child e.g. to say certain things, share child sexual abuse material.
- Exploiting children to generate and share child sexual abuse material (CSAM). This material is then often used to blackmail children to share further CSAM, or blackmail them for financial gain.
- Sharing child sexual abuse material with other offenders.
- *[I'd also suggest having a looking at the chapter – 'Test Two: Tackling online child sexual abuse' – which is page 10-14 of our Time to Act Report. It has a good overview of the CSA threat online.]*

What is the scale and extent of this crime?

- **Online child sexual abuse and grooming have rapidly increased over the last decade and have now reached record levels.**

Grooming

- Analysis of Freedom of Information data from 41 UK police forces show there has been an **84% rise in online grooming offences since 2017/2018.**
- Girls aged 12-15 are most likely to be victims of online grooming. In 2021/22, UK police FOI data shows four in five (82%) grooming cases were against girls (where the gender was known).
- Childline counselling data show that there has been a 35% increase in calls about online grooming from April to September 2022, compared to the previous year.

Child sexual abuse material (CSAM)

- Online platforms account for a growing number of new images being produced, with abusers using social networks to coerce children into producing images, or to perform sexual acts on livestream sites.
- 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.
- **More than 100,000 child abuse image crimes were recorded by UK police forces over the last five years**. FOI data from UK police forces show the number of offences relating to possessing, taking, making, and distributing child abuse material peaked at 25,281 in 2020/21 – up 37% from 2016/17.

How agencies and organisations are responding and what are the challenges?

- One of the main challenges for law enforcement agencies is the **scale of online harm and abuse**.

- This abuse has reached unprecedented levels, meaning it is increasingly challenging to tackle.
- This is why it is essential that tech companies take greater responsibility for **preventing abuse from occurring in the first place**. The Online Safety Bill is crucial for placing duties on tech platforms to prevent abuse on their platforms.
- Tech companies must also cooperate with law enforcement to identify child sexual abuse on their platforms.

Protecting children from sexual content online and on social media?

- **Technology companies must take responsibility for preventing children from accessing harmful material**, such as sexual content, on their platforms.
- The Online Safety Bill will require tech platforms which are likely to be accessed by children to protect them from viewing harmful and inappropriate content.
- Companies need to review their **algorithms.**
    - Currently, children are being bombarded with harmful content on social media by algorithms which prioritise engagement over safety.
    - We also know that it is easy for children to both stumble across and seek our inappropriate content.
    - The design of platforms must be changed so that children are prevented from viewing this material.
- Tech companies must implement **robust age assurance** measures to ensure they are effectively identifying child users and ensuring they have an age-appropriate experience.
- Tech companies need to prioritise children's safety, and start to build platforms which are **safe by design** for children.

Educating young people about online abuse, grooming and exploitation. / Providing support for children to recognise they are being abused, groomed or exploited. / Raising awareness of these issues?

- **Children have carried the burden for protecting themselves online for too long**. It is right that the Government is introducing the Online Safety Bill so that tech companies have to start to take responsibility for protecting children on their platforms.
- Schools have an important role to play in helping children stay safe online. **Relationships and Sex Education classes are crucial** for this.
    - RSE has lifelong benefits for children and young people by teaching them about healthy and positive relationships, empowering them to recognise abuse and learn about their rights to be kept safe and healthy.
- NSPCC also encourages **parents to have regular and open conversations** with their children about their online lives.
    - This can include talking about what they are seeing and doing online, talking about safety and privacy features, and what they think is age appropriate.

    - It's really important that children know if they ever feel uncomfortable about something happening online that they can speak up about it.

Measures to identify, report and prosecute this online crime.

- **Technology exists which enables tech companies to scan and detect child sexual abuse on their platforms.**
- For example, hash-matching technology assigns identified child sexual material with a 'hash'. Companies can then search their platforms for matches to this 'hash', enabling them to detect, report and remove child sexual abuse material.
- AI and image classifiers also enable companies to search for and report unknown child sexual abuse material – allowing them to new cases of abuse to law enforcement.
- **It is critical that companies continue to detect and report CSAM on their platforms, and invest in the technology to do this effectively**. This must include identifying and tackling child sexual abuse in end-to-end encrypted environments.

Challenges in regulating the Internet and whether existing offences and legislation are useful and sufficient.

- Technology has developed at a rapid rate, and this has led to new harms and types of abuse experienced by children online.
- It is critical that technology companies build platforms which are **safe by design**, so that children's safety is baked into new technology products, and not an afterthought.
- One example is the Metaverse. Already, examples are being shared publicly about new forms of online child sexual abuse taking place in virtual reality environments.
- Law makers must be live to changing forms of abuse and harm online and ensure that legislation and regulation keeps up to date with the new risks to children.
- It is also **vital that children have a voice in the new regulation**.
    - Listening to children will be key for ensuring that law makers and the regulatory can identify what new risks are emerging, and understand the reality of children's experiences online.

Key Online Safety Bill lines

Call for an Advocacy Body for Children

- **The Bill must ensure that children's experiences and safeguarding expertise are given statutory weight in the regulatory regime.**
- As it is currently drafted, the Online Safety Bill has gaps which mean that children's voices could be lost or drowned out by large tech companies, and that the regulator Ofcom will not have the breadth and depth of insight required to identify and respond to emerging harms.

- The NSPCC is supporting an amendment which will require Ofcom to make arrangements for an Advocacy Body for Children. **This body would be an independent voice for child users of regulated online services.** In this role, they would represent, protect, and promote the interests of child users, and monitor the implementation of the new regulation to ensure it is delivering for children.
- This Body would provide a platform for children's voices and experiences – ensuring they are heard by decision makers, and balancing the power of tech companies who will have significant capacity and resource to influence regulation.
- By identifying and analysing new risks to children in the rapidly changing online world, the Body could raise emerging harms with tech companies and Ofcom to ensure they are dealt with effectively and on an ongoing basis.

Call for extending the scope of Senior Manager Liability

- Government have introduced a new amendment to hold senior managers at the top of tech firms accountable for complying with the new online safety regulation and protecting children.
- However, senior managers will only be held liable for failing to prevent children from seeing harmful content. This will *not* be held liable for failing to tackling child sexual abuse on their platforms.
- **The strongest enforcement measures must be in place for the most serious crimes against children on their platforms.**
- Government must extend the scope of their amendment to ensure senior managers will be held accountable for tackling child sexual abuse on their platforms.

Importance of Online Safety Bill

- **Online child abuse is not inevitable.** Online grooming and child abuse image offences have reached record levels because social media companies have failed to respond to the child abuse threat.
- The Online Safety Bill is a **vital child protection measure**. It will introduce a regulatory framework to ensure that companies can no longer overlook the risks that their platforms pose to children through requiring them to meet new safety duties.
- We strongly support the ambition of the legislation. **Well-designed legislation can effectively balance the fundamental rights of all users**, including children who require a higher standard of systemic protection.
- The NSPCC are the original organisation which won the commitment from Government to introduce legislation to protect children online.
- **The Online Safety Bill is currently passing through the House of Lords. There is still time for Government to strengthen the Bill to ensure it is best placed to tackle child sexual abuse online.**