SELFIE GENERATION

What's behind the rise of self-generated indecent images of children online?

APPG on Social Media

appg

UK Safer Internet Centre

SELFIE GENERATION

What's behind the rise of self-generated indecent images of children online?

CONTENTS

FOREWORD

Today's children grow up simultaneously in two different worlds. There is the world offline – familiar enough to those of us whose childhoods were merely 'analogue', – and then there is the digital world online: intangible, always transforming itself, but just as real, engrossing and addictive.

But along with the tremendous opportunity promised by the continuing digital revolution, there are new threats to children and their safety, as well as old threats taking new forms. The breath-taking pace of technological change, affecting the way that individuals interact with one another online, has meant that policy, legal reform, and standards of best-practice have come to dangerously lag the digital reality they are supposed to regulate. We cannot let this continue. The safety of children, in extreme cases from sexual abuse and exploitation, is at stake.

This report is about a specific source of harm to children: the proliferation of self-generated child sexual abuse imagery, and the various ways that it is solicited, created, and distributed online. The term 'self-generated' is itself problematic. It refers to sexual imagery produced by the subject themselves, which is then often viewed and shared without their knowledge or agreement. But the term should not be taken to imply that such children have any share in the moral responsibility for their abuse.

One theme which recurred continually during the APPG's evidence sessions was that too often historical interventions intended to help children have suffered from being overly moralistic, blaming, uncomprehending of the nuances of contemporary online life, and, for these reasons, ineffective.

We must not alienate victims of child sexual abuse if we are to help them effectively. We have an obligation to listen and to try to understand their experience of the online world, and give them a realistic preparation for the kinds of threat they might encounter there.

But it is clear that first-personal strategies for safely navigating the online world are not sufficient to guarantee safe passage. The landscape itself must change. Social Media is failing in their moral obligation to keep young users safe. Institutional re-design is called for, including the introduction of a duty-of-care on the part of companies toward their young users. Firms must be more pro-active and forthcoming when it comes to abuse images. There is an urgent need for social media platforms to be transparent with young users about the mechanisms available to them to remove and complain about these harmful images. The government's forthcoming Online Safety Bill should be a vehicle for meaningful reform of this kind. There must be robust age-verification requirements on websites hosting adult content and social media companies should not encrypt their service, unless they can guarantee that they can still remove illegal content and cooperate with law enforcement in the same way they do now.

The online world continues to evolve in startling and often unexpected ways at pace, and children are invariably the first to know about it. If we are to keep the online world safe for them, we must marshal a creative, serious-minded, and imaginative response.

CHRIS ELMORE MP
Chair of the APPG on Social Media

KEY RECOMMENDATIONS

1. Tech companies should not introduce encryption unless they can guarantee that they can still remove illegal content and cooperate with law enforcement in the same way they do now.

2. The RSE curriculum should facilitate constructive conversations about healthy relationships in a digital age, that avoid blaming children. The Department for Education and devolved Education Departments must ensure that schools are well-resourced, and teachers receive appropriate training to facilitate these messages. The APPG recommends that interventions are targeted at primary aged children[1], as well as older teenagers.

3. The Home Office should review all relevant legislation to ensure it is as easy as possible for children to have their images removed from the internet and ensure that they can have confidence in the removal process.

4. Tech companies should be proactive in taking responsibility for ensuring they act with a duty of care towards their users. They should cooperate constructively with Government and other stakeholders. Platforms should ensure there are clear ways for users to raise complaints and request images are taken down.

5. "Self-generated" indecent imagery should be referred to as "first person produced imagery".

6. There should be clearer guidelines established for policing throughout England, Wales, Scotland and Northern Ireland relating to Outcome 21[2] to ensure a more consistent outcome that does not blame or criminalise children unnecessarily.

7. The Online Safety Bill and other relevant legislation such as the Audio-Visual Media Services Directive should encourage age verification of adult websites to prevent children from accessing them.

8. The Government should publish more information about the requirements in the Online Safety Bill as soon as possible, including how Ofcom will designate expert co-regulators in priority areas such as child sexual abuse.

9. The Government should ensure that organisations working to remove illegal content or preventing offending are well-funded and resourced, particularly areas that were previously EU-funded.

10. Platforms should take all possible measures to tackle harmful fake accounts, particularly those held by sex offenders.

1. Years 3 to 6.

2. Outcome 21 allows the police to deal with sexting offences without criminalising children and young people.

ABOUT THE APPG ON SOCIAL MEDIA

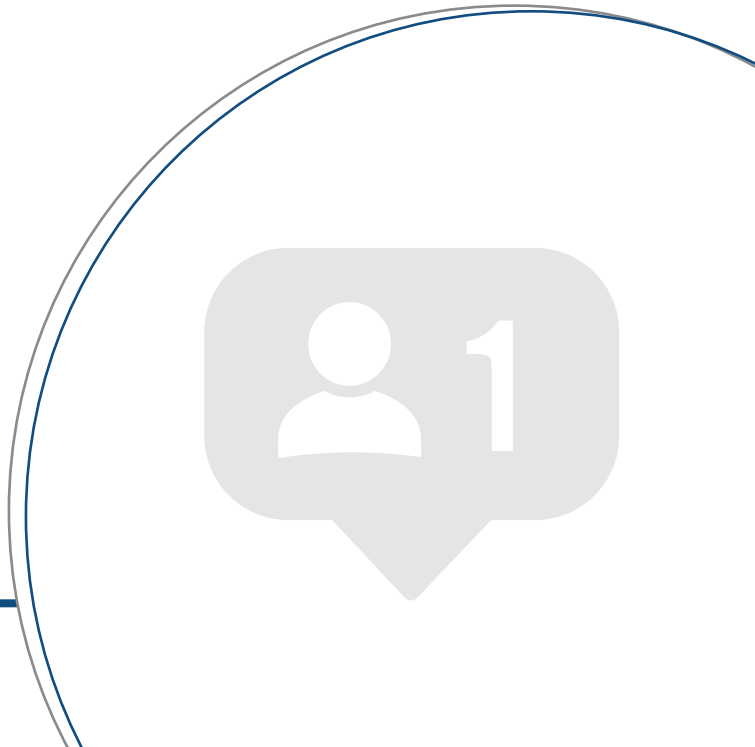
The All-Party Parliamentary Group (APPG) on Social Media was established in March 2018 and is a cross-party group of UK Parliamentarians. The UK Safer Internet Centre (UKSIC) has provided the secretariat for the group since November 2020.

Officers of the APPG on Social Media

- Chris Elmore (Chair), MP for Ogmore, Labour Party
- Aaron Bell (Secretary), MP for Newcastle-Under-Lyme, Conservative Party
- David Linden (Treasurer), MP for Glasgow East, SNP
- Lord Waverley (Vice Chair), Crossbench
- Bambos Charalambous (Vice Chair), MP for Enfield, Southgate, Labour Party
- Baroness Karren Brady (Vice Chair), Conservative Party
- Dr Lisa Cameron (Vice Chair), MP for East Kilbride, Strathaven and Lesmahagow, SNP

Other attendees who provided key input

- Sir Paul Beresford, MP for Mole Valley, Conservative Party
- Catherine McKinnell, MP for Newcastle upon Tyne North, Labour Party
- Baroness Ludford, Liberal Democrats
- Lady Masham, Crossbench
- Maria Miller, MP for Basingstoke, Conservative Party
- Baroness Newlove, Conservative Party
- Baroness Featherstone, Liberal Democrats
- Lord Blunkett, Labour Party
- Lord Kirkhope of Harrogate, Conservative Party
- Debbie Abrahams, MP for Oldham East and Saddleworth, Labour Party
- John Nicolson, MP for Ochil and South Perthshire, SNP
- Siobhan Bailie, MP for Stroud, Conservative Party
- Henry Smith, MP for Crawley, Conservative Party
- Sarah Champion, MP for Rotherham, Labour Party
- Saqib Bhatti, MP for Meriden, Conservative Party



1. BACKGROUND TO THE INQUIRY

In the first six months of 2021, the Internet Watch Foundation (IWF) recorded a 117% increase in "self-generated" child sexual abuse material that has been created using webcams or smartphones often when a child is alone. The child may or may not be aware that they've been recorded or photographed. In some cases, children are groomed, deceived or extorted into producing and sharing a sexual image or video of themselves. Other times it might be created and shared by a child consensually. This report will discuss the terminology used to describe this issue later on.

Much of this content takes place in the child's bedroom or other domestic setting, and it is often clear that the child's parents are unaware of what is happening in their home. This has been an emerging trend over the past couple of years; the IWF also saw a 77% increase in this type of content from 2019 to 2020 and it is those increases that helped to form the background to this inquiry.

Data from other sources provided to the inquiry, also confirm that online sexual activity and sharing "self-generated" content has become a 'normal' part of many young people's lives.

For instance, research from the NSPCC shows that:

- **More than one in seven children aged 11-18 (15%) have been asked to send self-generated images and sexual messages.**
- **7% of 11-16-year-olds have been asked to share a naked or semi-naked image of themselves.**
- **On average, one child per primary class has been sent or shown a naked or semi-naked image online by an adult.**

A recent Ofsted report into sexual harassment in schools in England provides further background of the "normalisation" of these issues within schools. Nine in 10 girls that spoke to the Inspectorate told them that sexist name calling and being sent unwanted explicit pictures or videos happened "a lot" or "sometimes."

This is also an issue in Wales and Scotland too. Wales' education watchdog is planning to hold a review into sexual harassment in schools following Everyone's Invited, where 91 Welsh schools were named[3]. In 2018, Girlguiding Scotland found that over 21% of girls and young women in Scotland aged 13 to 25 experienced sexual harassment at school, college or university[4].

1 IN 7 CHILDREN

aged 11-18 (15%) have been asked to send self-generated images and sexual messages.

3. https://gov.wales/written-statement-sexual-harassment-and-abuse-education-settings
4. https://www.girlguidingscotland.org.uk/girls-taking-action/our-campaign-work/ending-sexual-harassment-in-schools/

1. BACKGROUND TO THE INQUIRY

1.1 Impact of COVID-19

This is a trend which seems to have been exacerbated by the COVID-19 crisis. In March 2020, many child protection organisations and law enforcement agencies warned of a potential increase in online harm to children due to the COVID-19 pandemic and lockdowns. With both young people and potential offenders spending more time online, there was a concern that this would create the conditions for an increase in child sexual abuse using the internet.

Unfortunately, this proved to be the case. The NSPCC has found that since lockdown:

1. **Childline has seen an 11% increase in the number of counselling sessions about online sexual abuse.**
2. **The NSPCC helpline has had a 60% increase in contacts from people with concerns about children experiencing online sexual abuse.**

Whilst this has clearly been an issue during the pandemic, it is thought that there will also be an impact beyond COVID-19. A Europol report in June 2020 suggested that:

"There have been significant increases in activity relating to child sexual abuse and exploitation on both the surface web and dark web during the COVID-19 lockdown period... An increase in the number of offenders exchanging CSAM online during lockdown may have an impact on and stimulate demand for this type of material online beyond the lockdown."

Given the widespread impact that online harm and self-generated abuse issue seems to be having on children and young people, and the recent publication of the Online Safety Bill for pre-legislative scrutiny, the APPG wanted to know what more could be done to better protect children online.

That is why, on 9 November 2020, the inquiry: "Selfie Generation: What's behind the rise of Self-Generated Indecent Images of Children online?" was launched.

The inquiry ran until 24 June 2021 and had two stages: a call for written evidence which closed on 31 January 2021, followed by four oral evidence sessions with academics, children's charities, law enforcement and industry.

The inquiry received written evidence from 18 individuals and organisations and additionally, other research reports and documents were provided to the APPG to support this report. A full list is provided at the end of the report.

We are extremely grateful to all those who provided evidence, insights and contributions to support this important inquiry.

1. BACKGROUND TO THE INQUIRY

1.2 Witnesses who provided written evidence

- Emma James, Senior Policy and Research Officer, Barnardo's
- Maeve Walsh, Carnegie Trust
- Dr Abhilash Nair, Aston University
- Euan Fraser and Hannah Bondi, International Justice Mission UK
- Mark Donkersley, eSafe Global
- Caroline Allams, Natterhub
- Emily Setty, University of Surrey
- Dave Miles, Facebook
- Jack Perry, PA Consulting Group
- Jon Needham, Oasis UK
- Hannah Ruschen, NSPCC
- Emma Davies and Vicki Shotbolt, ParentZone
- Professor Andy Phippen and Professor Emma Bond
- Professor Lorna Woods
- Sarah Whitehead, West Yorkshire Police
- Henry Turnbull, Snap Inc.
- Niamh McDade, Twitter
- Ben Bradley, TikTok

1.3 Witnesses who provided oral evidence

Session: Monday 22 March 2021

- Dr Abhilash Nair, Aston University
- Professor Lorna Woods, Carnegie Trust and University of Essex
- Professor Emma Bond, University of Suffolk
- Professor Andy Phippen, Bournemouth University

Session: Monday 26 April 2021

- Will Gardner OBE, CEO, Childnet International
- David Wright, Director, South West Grid for Learning (SWGfL)
- Olivia Robey, Child Abuse and Exploitation Lead, Centre for Social Justice
- Claire Levens, Policy Director, Internet Matters
- Andy Burrows, Head of Online Safety, NSPCC
- Emma James, Senior Policy Advisor, Barnardo's

Session: Wednesday 19 May 2021

- Rob Jones, Director of Threat Leadership, National Crime Agency
- Chief Constable Simon Bailey QPM, National Police Chiefs' Council lead for Child Protection
- Tom Squire, Clinical Manager, Lucy Faithfull Foundation

Session: Thursday 24 June 2021

- Becky Foreman, UK Corporate Affairs Director, Microsoft
- Dave Miles, Head of Safety for Europe, Middle East, and Africa (EMEA), Facebook

The All-Party Parliamentary Group on Social Media would like to thank the UK Safer Internet Centre for the provision of secretariat since November 2020.

For any additional information or questions, please contact Michael Tunks, Senior Policy and Public Affairs Manager at the Internet Watch Foundation and UK Safer Internet Centre, on mike@iwf.org.uk or Abigail Fedorovsky, Policy and Public Affairs Assistant at the Internet Watch Foundation and UK Safer Internet Centre, on abigail@iwf.org.uk

2. INTRODUCTION

Technology is increasingly playing a significant role in children and young people's lives from a very young age. Whilst the internet can be a valuable source of learning and connection, the digital environment also has the potential to facilitate harm. This APPG inquiry report aims to make recommendations that will help maximise the benefits of social media, whilst mitigating the negative consequences.

According to Ofcom's latest Online Nation report, more than half of 12-15-year-olds surveyed said they had a negative experience online in 2020. On mobile phones the most common of these experiences was 'being contacted online by someone you don't know who wants to be your friend' (cited by 30% overall) and a significant minority had seen something scary or troubling (18%) or seen something of a sexual nature that made them feel uncomfortable (17%)[5].

It is vitally important that there is no further delay in the scrutiny and preparation of the Online Safety Bill. We owe it to our children to ensure the highest possible protections are in place both online and in the community to ensure that their online experience is a safe one.

This requires a multi-stakeholder approach and requires everyone to play their part. Government, law enforcement, parents, teachers and professionals working with children and the technology industry all have a responsibility to keep children safe online.

The APPG welcomes the inclusion of a Duty of Care within the Online Safety Bill. It is encouraging to see that the protections for children already prioritised by the child protection and education sectors are now being brought to the attention of the technology sector too.

However, it became clear throughout the course of the inquiry that there was still more to be done collectively to improve the response to children. We believe it is crucial that this focus is not lost in the forthcoming scrutiny of the Bill and that the regime works in children's interests and is effective from day one. This issue is simply too important for it not to be.

[5] https://www.ofcom.org.uk/__data/assets/pdf_file/0013/220414/online-nation-2021-report.pdf

3. DEFINING "SELF-GENERATED" INDECENT IMAGERY

3.1 Importance of Terminology

One of the key issues that arose from this inquiry was the importance of the language being used, particularly the vital need to avoid placing any blame on the child for sexual activity and the need for clear definitions that ensure children can have this content removed from the internet as easily as possible.

In the UK, images of children are assessed using the Sentencing Council's 2014 Guidelines[6] to determine whether they are illegal:

Category	Description
A	Images involving sexual penetrative activity, images involving sexual activity with an animal or sadism.
B	Images involving sexual, non-penetrative sexual activity.
C	Other indecent images not falling under Category A or B.
Not Illegal	The image is not deemed to be illegal.

For this inquiry, the APPG also set out to use the internationally recognised Luxembourg Guidelines[7] terminology to define self-generated sexual content/material involving children.

However, multiple witnesses challenged the term "self-generated" because of the implication that children are to blame for their sexual activity. A recent report from the Tech Coalition has suggested that the current terminology could be softened to avoid inadvertent victim blaming and should be referred to as ***"first person produced imagery"***[8].

The report also recommends that this new term has the following definition:

"Sexual visualised depictions of a child that are generated without the full knowledge, consent, and participation (for example, grooming, blackmail and coercion) of the child and without the physical presence of an instigator AND/OR that may have been originally voluntarily produced by the minor child, but then is distributed to or shared with others without the child's full knowledge or consent."

The report also crucially said that consent should not be limited to legal capacity to consent but should reflect the age-appropriate state of mind of the subject and should take into account if the generation was coerced.

6 https://www.sentencingcouncil.org.uk/offences/magistrates-court/item/possession-of-indecent-photograph-of-child/_

7 http://luxembourgguidelines.org/english-version/

8 https://www.technologycoalition.org/wp-content/uploads/2021/06/MSF-Summary-FINAL-FINAL-FINAL.pdf

3. DEFINING "SELF-GENERATED" INDECENT IMAGERY

3.2 Understanding Motivations for Sharing Imagery

Many witnesses also pointed out that there are a variety of very different situations that can come under the broader term of "self-generated" indecent imagery. It is important to understand the specific contexts and motivations for sharing imagery, and the different terminology relevant to these situations, to better design appropriate interventions.

In their written evidence, NetClean suggested five distinct categories of self-produced images that speak about the different motivating factors for sharing content:

1. **Innocent Images.**
2. **Voluntarily self-produced material.**
3. **Images produced as a result of grooming.**
4. **Images produced as a result of sexual extortion.**
5. **Images produced as a result of trafficking.**

When looking at these distinct categories, NetClean found that the most common type of self-produced material they recorded was voluntarily self-produced material (57.5%), followed by images as a result of grooming (22%.)

This is a helpful breakdown as it is clear that there is a significant difference in the type of intervention needed in a situation where a child voluntarily shares an intimate image with a peer than in a situation where the child has been groomed by a sexual predator or is being blackmailed. These are each serious situations and need appropriate and proportionate responses, but it is important to consider the nuance within the broader term "self-generated" indecent imagery to safeguard the child appropriately.

In a similar vein, in his evidence, Dr Nair also proposed three categories of sexting images:

1. **Consensual sharing between partners**
2. **Images that are initially created consensually but are redistributed without agreement.**
3. **Images that are created through coercion or bullying, or by predators.**

These, again, give an indication as to the varying motivations that a child might have when sharing an image. Having said that, these categories are all somewhat interlinked too, and this nuance needs to be carefully considered. For instance, it is important for children to understand that whatever their original motivations for sharing the imagery, there is always a risk that it can be sent on to other people beyond their control and could be shared as child sexual abuse material.

3.3 Age

Whilst typically we think of online sexual activity as primarily affecting older teenagers, the inquiry has shown that younger children also need to be targeted with interventions. Childnet explained how when they first launched Project deSHAME they focused on 13-18-year-olds, however they more recently extended this to include 9-12-year-olds too as young people expressed that this issue was relevant to that age group.

In 2020, the Internet Watch Foundation found that 81% of images or videos of self-generated content showed a child aged 11 to 13 years old. In a further 15% of cases, the image or video showed a child aged 10 or under[8].

The APPG therefore recommends that interventions are targeted at primary aged children, as well as older teenagers[10].

9 https://www.sentencingcouncil.org.uk/offences/magistrates-court/item/possession-of-indecent-photograph-of-child/_

10. Years 3 to 6.

4. DISCLOSURE AND REMOVAL

4.1 Shame

The APPG heard that a major reason why children do not want to disclose abuse is because they feel ashamed. For instance, Childnet's Project deSHAME has found that the top five barriers for young people seeking help when it comes to online harm are:

- Too embarrassed: 52%
- Worried about what would happen next: 42%
- Worried about being targeted by those involved: 42%
- Worried that they are to blame: 39%
- Would rather sort it out for themselves: 39%

When Childnet launched their resources, one teenage girl said that young people see these things happening, but no one talks about them, so this creates shame for the young people around these topics. Childnet has found that if schools, parents or carers bring up these issues, children feel more confident in talking about them. It is important that as a society we have open conversations about these often-taboo topics, so that young people feel comfortable disclosing what has happened to them.

In order to bridge this gap, the IWF has recently launched a campaign aimed at parents and carers, in partnership with the Home Office and Microsoft, that helps adults to have open conversations with their children about online abuse and social media use. This encourages adults to T.A.L.K. to their children:

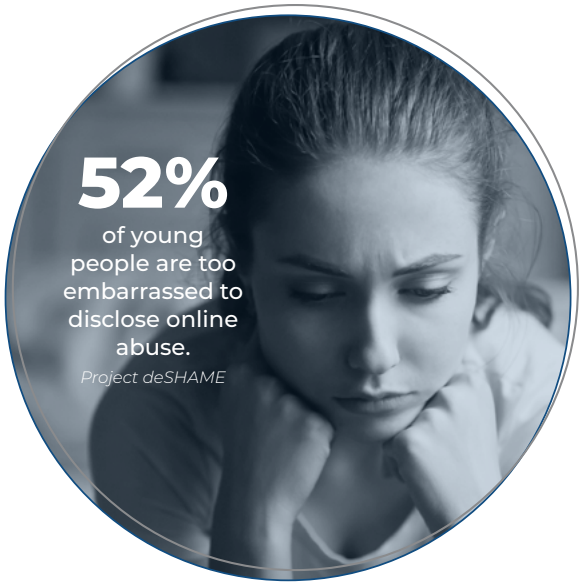
- Talk to your child about online sexual abuse.
- Agree digital boundaries.
- Learn about online platforms your child loves.
- Know how to use tools and safety settings.

In their joint written evidence Professor Phippen and Professor Bond spoke about their experience talking to young people who generally believe disclosure will be met with an unsupportive and potentially harmful response. In particular, they referenced how educational materials tend to focus on the legal issues surrounding the sharing of an intimate image by a minor. Children are taught that if they do share an image, they are breaking the law and can be arrested.

As a result of these educational messages, many young people believe that once an image has been shared further, there is nothing they can do to rectify the situation: "once its online its always online," "you've only got yourselves to blame" and "if you don't take the image, no one can share it".

It is essential that children receive constructive educational messages that avoid blaming or shaming the victims, and that they have certainty that something will happen if they report their abuse.

The Department for Education and devolved Education Departments must ensure that schools are well-resourced and teachers receive appropriate training to facilitate these messages.



4. DISCLOSURE AND REMOVAL

4.2 Reporting

Currently one of the main reasons why young people do not disclose abuse is that they do not think that social media companies will do anything once an issue is reported. For instance, Childnet's Project deSHAME found that the top reason among children for not reporting on social media was not thinking it would help (43%.)

Claire Levens from Internet Matters gave evidence that social media companies need to demonstrate to children that they are listening to them by acting swiftly on any concerns and communicating effectively why a particular decision has been made when it comes to removing content. Children need to be able to understand the reporting process, the timelines and the likely roots of redress.

One positive example of this is a new tool, Report Remove, launched by the IWF, the NSPCC and the UK Government in partnership with tech companies where minors can report sexually explicit, self-generated images to have them taken down. Facebook also assisted by collaborating to support the technical development and piloting of Report Remove. Report Remove encourages a child-centric approach and gives children somewhere to turn if something does go wrong, aiming to empower them. This also enables the NSPCC to safeguard vulnerable children appropriately.

Report Remove is currently strictly limited to removing illegal content according to the Sentencing Council Guidelines and relies on children having to verify their age. Professor Bond pointed out that help is currently simpler for over 18s than under 18s who have access to the Revenge Porn helpline which assists adults seeking to get their intimate images removed from the internet under the intimate image-based laws. With disclosure already being incredibly difficult for children and connected to strong feelings of shame, it is essential to remove as many barriers as possible and streamline reporting processes.

The APPG recommends that the Home Office reviews all relevant legislation to ensure it is as easy as possible for children to have their images removed from the internet and ensure that the children are appropriately safeguarded, and offenders brought to justice.

Platforms should also ensure children can have their images removed as easily as possible, for instance through having effective response mechanisms to requests to take down images by child users.

The Department for Education and devolved Education Departments should ensure that teachers and all of the schools workforce know how to appropriately handle disclosure.

Report Remove by the IWF and the NSPCC

4. DISCLOSURE AND REMOVAL

4.3 Legislation

When it comes to disclosing abuse, children need to have confidence in the law that they will be safeguarded and supported, and not criminalised for creating a potentially illegal image.

The Protection of Children Act (1978) and the Children's Act (1989), laws that created the offences of creating, making, sharing and distributing indecent images of children were designed before the current digital age and currently do not differentiate between the involvement of an adult or a child. These laws were not designed for, and could not have foreseen a time when there would be, such large-scale use of camera enabled devices which allow imagery to be created, uploaded and shared in such vast quantities as happens today.

Chief Constable Bailey provided evidence to the inquiry about how law enforcement has had to adapt to this new world and provide workable solutions to the current legal structures and modern-day technological challenges.

He explained how policing had successfully worked alongside the Home Office to create a pragmatic solution called Outcome 21. Outcome 21 gives law enforcement the ability to shut down an investigation on the basis that it is not in the public interest to pursue a prosecution when it has been established that a child created the image. Law enforcement then works alongside the Disclosure and Barring Service (DBS) to ensure that this does not adversely affect the life chances of children and young people in securing future work.

Despite this, other evidence submitted to the inquiry suggests that the application of Outcome 21 is currently inconsistent across England and Wales and, as it is left up to police discretion, there is a level of uncertainty about what is acceptable.

There is also currently no Outcome 21 in Scotland or Northern Ireland.

The APPG recommends that the College of Policing reviews its current Outcome 21 Guidance and ensures there are clearer, more consistent guidelines established for police throughout the UK so that they use Outcome 21 appropriately and ensures synergies wherever possible with the devolved administrations.

5. TECH RESPONSIBILITY AND DESIGN

5.1 Current steps taken by companies

It is important the Government, industry, and civil society continue to work in partnership to maximise the benefits of the internet whilst minimising harm to children. Many witnesses pointed out the multitude of benefits that social media and the internet provide for young people, for instance Professor Bond who talked about the internet often being a place for people to find understanding and belonging.

The APPG also heard about some of the innovative initiatives from social media companies to ensure the fast removal of illegal content from their platforms. For instance, companies like Facebook, Twitter, TikTok, Microsoft and Snap say that they do not allow illegal activity such as child sexual exploitation, sexualisation of children, child nudity or inappropriate interactions with children on their platforms.

Facebook stated in their evidence that 99% of the reports they act on are removed before consumers have seen the content. TikTok's most recent transparency report for the first quarter of 2021 makes a similar claim that 81.8% of the videos that they removed for violating its Terms and Conditions were removed before anyone had seen them.

Companies also have some preventative tools in place, for instance Twitter has a range of *#ThereIsHelp* prompts, including a dedicated prompt designed to intervene when users look up terms associated with child sexual exploitation. The prompt is also intended to connect users to local partners that offer intervention and prevention programmes.

Photo DNA

Tech companies collaborate with law enforcement and hotlines like the IWF to identify and remove illegal images of children from their platforms. For example, Microsoft explained how they have heavily invested tools, research and data into dealing with the issue of CSE/A online. Microsoft explained how they developed PhotoDNA technology after a direct request from a Toronto Police Chief to Bill Gates and how that was furthered in 2009 through work with Dartmouth College in the US. PhotoDNA enables any company, charity or law enforcement agency using the tool to find copies of that image even though it has been digitally altered. Some have called it the most important technical development to date in the field of child protection in the past decade. Microsoft now shares this technology with smaller providers, charities and NGOs and is now open sourced to over 130 technology organisations and companies.

Microsoft has also funded research into the issue of self-generated indecent images of children by partnering with the Internet Watch Foundation (IWF) which examined the impact of captures of livestreamed child sexual abuse (2018) and online produced content (2015).

Many tech companies are already partnering with civil society and Government to produce educational initiatives aimed at their child users. For instance, TikTok has worked alongside Thorn to launch an in-app campaign called This is NoFltr to facilitate a conversation between young people and adults about sharing nude images and consent.

5. TECH RESPONSIBILITY AND DESIGN

5.2 Safety by Design

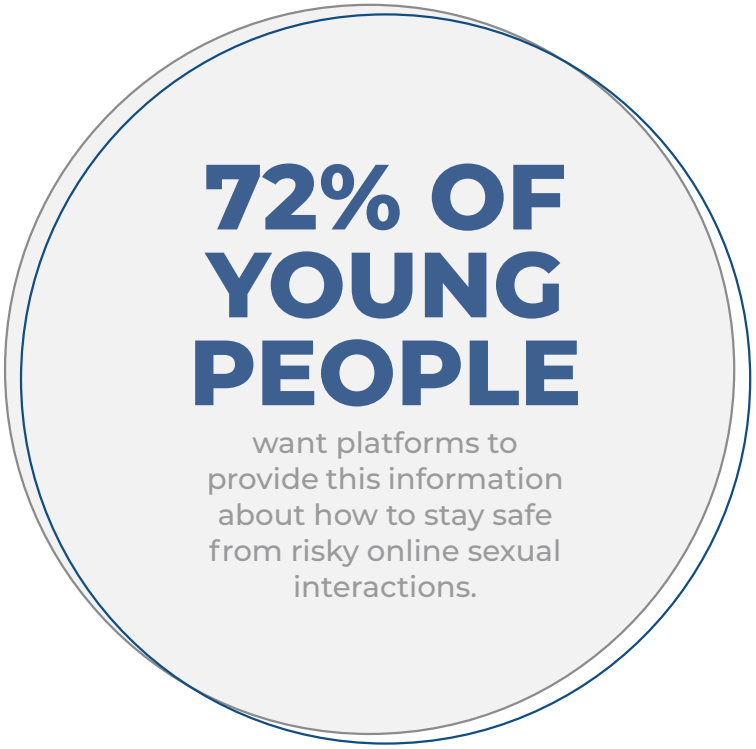
The APPG heard evidence about the importance of platforms being designed with safety in mind. Professor Woods highlighted the need for platforms to have a systemic focus, to not just look at whether content is harmful, but to consider how safe their design is, i.e., to what extent it can be used deliberately for harmful risks and behaviours. She mentioned Instagram as a positive example of a company who has recently made changes so that adults can only message children who already follow their account.

It is important that social media providers are seen as responsible for the public space they have created, much as property owners or operators are in the physical world. Everything that happens on a social media service is a result of corporate decisions. There are already some positive examples of this happening, for instance, on Snapchat the default setting is that users cannot receive messages from someone who is not their friend on the app.

A safety by design approach would enable parents and carers to be supported in protecting their children. For instance, Barnardo's stated in their evidence that parents and carers often feel that they are made to feel responsible for monitoring their child's online life 24/7 which is unrealistic as their children become older.

Finally, the APPG suggests that social media platforms provide educational messages for children about how they can stay safe from abuse. Research from Thorn found that 72% of young people want platforms to provide this information about how to stay safe from risky online sexual interactions. A positive example of this is a new campaign that the IWF has worked in partnership with Microsoft and the Home Office to produce, for young girls and their parents specifically aimed at educating them about online abuse and the methods offenders use to coerce children into producing "self-generated" content.

Platforms should ensure there are clear ways for users to raise complaints and request images are taken down.



5. TECH RESPONSIBILITY AND DESIGN

5.3 Age Verification

Throughout the inquiry, witnesses provided evidence about the potential detrimental impact that accessing pornography from a young age can have on children and their ability to form healthy relationships. For instance, Barnardo's have found that children's understanding of sex, including what they perceive as healthy and normal, often comes from viewing pornography online. This influence can be highly significant in how they navigate the online world.

NCA CEOP Director, Rob Jones, explained that if children progress in the wrong way in their browsing of adult pornography, they will end up viewing child sexual abuse imagery. Whilst it is essential that schools and parents talk to children about pornography, it is concerning that there is such a high level of unfettered access to adult websites. In the offline world, it is not possible for a child to walk into a newsagent and just be confronted with hardcore pornography. The magazines are usually located on the top shelf and their covers are obscured from view. As the Government has consistently said, the same rules that apply to the offline world should apply to the online world.

Dr Nair talked about his recent EU-funded research on age verification. He highlighted that currently most platforms just have a tick box for age, even though it is a requirement under GDPR that parental consent is needed when processing data of children under 13.

The APPG recommends that the Online Safety Bill and other appropriate legislation, such as the Audio-Visual Media Services Directive (AVMSD) includes measures to age verify users of adult websites that do not host user generated content.

5. TECH RESPONSIBILITY AND DESIGN

5.4 Encryption

Various witnesses raised the issue of encryption of popular apps which have large numbers of child users. It is well known that Facebook intends to encrypt its messenger platform, and many witnesses raised very real concerns about the impact this would have for child protection, including Olivia Robey from the Centre for Social Justice, Andy Burrows from the NSPCC and in particular Rob Jones, NCA and Chief Constable Simon Bailey.

An article from Professor Hany Farid submitted to the inquiry says that:

"Broader adoption of end-to-end encryption would cripple the efficacy of programs like PhotoDNA, significantly increasing the risk and harm to children around the world. It would also make it much harder to counter other illegal and dangerous activities on Facebook's services. This move also doesn't provide users with as much privacy as Zuckerberg suggests. Even without the ability to read the contents of your messages, Facebook will still know with whom you are communicating, from where you are communicating, and a trove of information about your other online activities. This is a far cry from real privacy."

The APPG is keen to stress that our response to the issue of encryption is not to demonise the technology. We understand the importance of encryption to securing global bank systems and other sensitive information for example. However, we believe that before a platform encrypts it must ensure that the same safeguards and co-operation with law enforcement is in place in the encrypted channel as currently exists in the unencrypted environment.

Facebook defended the plan to encrypt messenger by explaining that they were working closely with the European Internet Forum to look at what the potential technical encryption solutions could be to deal with CSE/A content in those channels. It was explained there was a lot that could be done to mitigate this, however, there will undoubtedly be a loss of visibility of this sort of content.

Despite these issues, law enforcement is still yet to receive assurances from Facebook that it will not encrypt messenger until a solution has been found.

The APPG believes it is completely unacceptable for a company to encrypt a service that has many child users. Doing this would do so much damage to child protection. We recommend that technology companies do not encrypt their services until a workable solution can be found that ensures equivalency with the current arrangements for the detection of this imagery.

We recommend that platforms, hardware providers and others work together to identify potential solutions to encryption and other technical challenges.

5. TECH RESPONSIBILITY AND DESIGN

5.5 Regulation

i. Ofcom's Role

The APPG heard evidence about Ofcom's vital role in tackling self-generated indecent imagery online as the new Regulator under the Online Safety Bill. It is important for Ofcom to work in partnership with civil society, users, victims, and tech companies to be as effective as possible. There are existing organisations that are experts in this sector, and Ofcom should prioritise working alongside them. For instance, the IWF was mentioned by almost all witnesses as an organisation removing millions of illegal images and videos each year and developing innovative solutions to online abuse.

Witnesses from Facebook and Microsoft highlighted that much of the Online Safety Bill will be determined through secondary legislation and would mean there are many decisions which will fall to either Ofcom or the Secretary of State. Whilst larger companies have the resources and legal teams to prepare in advance, smaller companies do not have access to this.

There should be clarity in the Online Safety Bill about illegal content and legal- but-harmful content. There are legal behaviours linked to the grooming of children and it is important for there to be clarity about how this will be treated, for example if there is an online group sharing information about how to groom.

The Government should publish more information on the Online Safety Bill as soon as possible. This should include information about how Ofcom will designate expert co-regulators, and the criteria involved in selecting which organisations this will be.

ii. Duty of Care

All platforms, regardless of their size, must be fulfilling a duty of care to their users and ensuring that offending is as difficult as possible.

Witnesses from law enforcement spoke about their concerns of the extremely low bar to offending on the open web and that mainstream search engines are regularly returning Category A images within three clicks.

Simon Bailey: *I was quoted in a national newspaper recently about the fact that Registered Sex Offenders were using Instagram profiles. A newspaper discovered 100 registered sex offenders using the platform. If this were a shop on the high street, it wouldn't be possible for 100 sex offenders to gather at a store where children are.*

Platforms should take all possible measures to tackle harmful fake accounts, particularly those held by sex offenders.

6. EDUCATION AND PREVENTION

6.1 Relationships and Sex Education (RSE) Curriculum

Whilst technology companies have a key role to play, this must also be complemented by educational messages for young people. It is essential to have effective educational initiatives in schools to address the normalisation of young people sharing explicit images. For instance, research from Thorn shows that 40% of young people surveyed agreed that "it's normal for people my age to share nudes with each other".

Some evidence showed that the existing educational messages are too focused simply on the idea that children should not share images in the first place. Professor Phippen and Professor Bond ran a pilot study in 2008 looking at sexting which found that there was a massive gulf between young people's attitudes and those of adults. They pointed out that nothing has changed since then, but highlighted that the "best in class," resource – certainly in the view of young people they have spoken to – is the "So You Got Naked Online" resource by SWGfL. It takes a pragmatic and supportive approach, which offers support to the young person rather than patronises or punishes them.

Many witnesses talked about the role that the RSE curriculum can have in facilitating open discussions with young people about healthy relationships. For instance, Olivia Robey from the Centre for Social Justice spoke about how the RSE curriculum provides a good opportunity to have conversations with young people about the online aspects of peer relationships and associated risks.

Andy Burrows from the NSPCC said that it is vital to have high-quality nuanced interventions that start at the points that children and young people are at, for instance the RSE is an opportunity to teach young people about what healthy relationships look like, how to recognise abusive dynamics in behaviour and how to disclose abuse. This must be informed by high-quality research.

If the RSE curriculum is to be effective, teachers and schools' professionals must be well-equipped to deliver lessons about online safety and abuse. Unfortunately, at the moment this is not always the case. David Wright from SWGfL shared an example of an assessment they have made of 15,000 schools. In over 40% of cases, the schools do not have any professional development for staff about online safety. The Government should invest in the schools' workforce to be able to deliver digital education effectively.

6. EDUCATION AND PREVENTION

6.2 Prevention

It is essential to prioritise preventing online abuse from happening in the first place, not only through educational initiatives, but also through direct intervention with potential offenders. In 2021 the NCA's Annual Threat Assessment estimated that between 550,000 and 850,000 people in the UK pose a sexual threat to children, either through offline or online offending. International Justice Mission UK provided written evidence about the considerable number of UK users who pay to watch livestreamed abuse that might be taking place in another country, e.g. the Philippines – the UK is currently the third largest consumer of livestreamed abuse.

The Lucy Faithfull Foundation set up the Stop It Now helpline in 2002 and which now deals with around 1,400 contacts per month from around 800 individuals. 50% of those people are directly concerned about their behaviour and 1 in 5 have solicited indecent images from a minor. The majority call about viewing indecent images, but some call regarding their behaviour related to online grooming. Lucy Faithfull have developed an online chat service and online self-help guides. Over 170,000 people have clicked through to these self-help services. Independent evaluations show that a number of these people change their behaviours as a result of seeking help, with many stopping viewing images at all. However, Lucy Faithfull does not currently have the resources they need for the demand. The Foundation deals with 1,000 calls every month but is currently missing almost 2,000 per month. They helped 7,000 people in the last year, but unfortunately could have helped an additional 2,000. The Foundation would be able to answer these calls if they had an additional £180,000 per year.

It is vital that organisations that do this preventative work are well-resourced by the Government to cope with the demand, particularly given the increasing reports of online abuse during the COVID-19 crisis.

It is important to understand why offending happens and what the most appropriate response should be. For instance, Tom Squire from the Lucy Faithfull Foundation provided evidence about the different offending profiles that they see. These offenders have different starting points, and their progression differs, which is important to understand as it informs the different interventions needed.

There are also many children and young people who commit sexual offences against their peers, but the majority of the strategies designed in response focus on adult offenders only. When abuse is perpetrated by another child, there should be specialist safeguarding and support in place.

Olivia Robey from the Centre for Social Justice raised the issue of offenders migrating between platforms, for instance if the offender connects with a young person on Snapchat and then migrates to WhatsApp. Platforms should work more closely together to understand these pathways and avoid high-risk design features.

7. RECOMMENDATIONS

1. Tech companies should not introduce encryption unless they can guarantee that they can still remove illegal content and cooperate with law enforcement in the same way they do now.

2. The RSE curriculum should facilitate constructive conversations about healthy relationships in a digital age, that avoid blaming children. The Department for Education and devolved Education Departments must ensure that schools are well-resourced, and teachers receive appropriate training to facilitate these messages. The APPG recommends that interventions are targeted at primary aged children, as well as older teenagers.

3. The Home Office should review all relevant legislation to ensure it is as easy as possible for children to have their images removed from the internet and ensure that they can have confidence in the removal process.

4. Tech companies should be proactive in taking responsibility for ensuring they act with a duty of care towards their users. They should cooperate constructively with Government and other stakeholders. Platforms should ensure there are clear ways for users to raise complaints and request images are taken down.

5. "Self-generated" indecent imagery should be referred to as "first person produced imagery".

6. There should be clearer guidelines established for policing throughout England, Wales, Scotland and Northern Ireland relating to Outcome 21[1] to ensure a more consistent outcome that does not blame or criminalise children unnecessarily.

7. The Online Safety Bill and other relevant legislation such as the Audio-Visual Media Services Directive should encourage age verification of adult websites to prevent children from accessing them.

8. The Government should publish more information about the requirements in the Online Safety Bill as soon as possible, including how Ofcom will designate expert co-regulators in priority areas such as child sexual abuse.

9. The Government should ensure that organisations working to remove illegal content or preventing offending are well-funded and resourced, particularly areas that were previously EU-funded.

10. Platforms should take all possible measures to tackle harmful fake accounts, particularly those held by sex offenders.

8. HOW CAN I GET HELP?

As a young person

- Gurls out Loud
Information to help you if an adult asks you for nude images

gurlsoutloud.com

- Report Remove
Remove a nude image shared online

childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/remove-nude-image-shared-online

- So You Got Naked Online
A resource that offers children and young people advice and strategies to support the issues resulting from sexting incidents.

swgfl.org.uk/resources/so-you-got-naked-online

- Childline
A free, private and confidential service where you can talk about anything.

childline.org.uk

As a parent or carer

- Home Truths
Information about how to keep your safe from online grooming

talk.iwf.org.uk

- Childnet International
Online Sexual Harassment: Advice for Parents and Carers of 13–17-year-olds

childnet.com/resources/online-sexual-harassment-advice-for-parents-and-carers-of-13-17-year-olds

- Stop It Now Helpline
Confidential help and support if you're concerned about the behaviour of another adult.

stopitnow.org.uk

9. REFERENCES

Click for more

» Department for Education. (2018.) Sexual violence and sexual harassment between children in schools and colleges. May 2018.

» ECPAT France and ECPAT Luxembourg. (2017.) Online Child Sexual Abuse and Exploitation: Current forms and good practice for prevention and protection. June 2017.

» Europol. (2020.) Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse during the COVID-19 Pandemic. June 2020.

» Internet Watch Foundation Annual Report 2020.

» NatCen. (2017.) Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation. October 2017.

» NetClean. (2018.) Eight insights into child sexual abuse crime.

» Ofcom. (2021.) Online Nation: 2021 Report. June 2021.

» Project deSHAME. (2017.) Young people's experiences of online sexual harassment. December 2017.

» Scottish Government. (2021.) Engaging in risky online behaviour: Initial findings on prevalence and associated factors at age 12 from the Growing Up in Scotland survey. June 2021.

» Technology Coalition. (2021.) Multi-Stakeholder Forum: Charting a Collective Path Forward. June 2021.

» Thorn. (2021.) Self-Generated Child Sexual Abuse Material: Attitudes and Experiences. August 2020.

» Thorn. (2021.) Responding to Online Threats: Minors' perspectives on disclosing, reporting, and blocking. May 2021.

» University of Bedfordshire, Safer Young Lives Research Centre, and Association for Young People's Health. (March 2021.) Learning from the Experts: Young people's views on their mental health and emotional wellbeing needs following sexual abuse in adolescence. March 2021.

» VoiceBox. (2021.) OnlyFans and young people: exploitation or empowerment? April 2021.

SELFIE GENERATION

What's behind the rise of self-generated indecent images of children online?

APPG on Social Media

appg

UK Safer Internet Centre

© 2021 - APPG on Social Media