



"One day this could happen to me"

Children, nudification tools and sexually explicit deepfakes

April 2025







Table of contents

Content warning	4
Foreword from Dame Rachel de Souza	5
Glossary	8
Executive Summary	10
Introduction	13
1. Children's views on nudification tools and sexually explicit deepfakes	14
1.1 What the online world looks like to children	14
1.2 Prevalence of AI tools and products	16
1.3 Gendered harm	17
1.5 What children want	19
2. What we know about children's exposure to sexually explicit deepfakes	21
2.1 The technology	21
2.1.1 Nudification tools	21
2.1.2 Who are the targets of nudification tools?	22
2.1.3 The impact on girls and young women	24
2.2 Children's exposure and use of this technology	24
2.2.1 Children are increasingly being exposed to sexually explicit deepfakes	24
2.2.2 Young people are more at risk than adults	25
2.2.3 Children can be perpetrators of deepfake sexual abuse	25
2.3 The high risk of harm to children	26
2.3.1 Sexually explicit deepfakes present a high risk of harm to children	26
3. The deepfake economy	27
3.1 Open-source Al models	27
3.2 The deepfake economy	28
3.2.1 Bespoke nudification apps	
3.2.2 Other image editing apps	30
3.3 Accessing nudification tools	32



3	3.3.1 Search engines	32
	3.3.2 Social media sites	
3	3.3.3 App stores	35
4. Wh	nat needs to happen now?	37
4.1 \	What the law currently says	37
4.2	The Children's Commissioner's recommendations for change	37
4	4.2.1 Outlaw nudification tools	37
4	4.2.2 Short term solutions	39
5. Me	thodology	. 41
Refer	rences	43



Content warning

This report is not intended to be read by children, but by researchers and policy makers interested in making children safer. It contains details about the harmful material children encounter in the online world, including descriptions of sexual abuse, harmful depictions of women and sexually explicit content. This content may be difficult and upsetting to read. However, we think it is important to highlight the nature of the content children are exposed to online, so that we may better protect all children.

If you, or any child you know of, are affected by the issues discussed, the following organisations can provide you with expert information, advice and support.



Report Remove is here to help young people under 18 in the UK to confidentially report sexual images and videos of themselves and remove them from the internet. www.childline.org.uk | Call 0800 1111



Childline is a free and confidential service for under-19s living in the UK:

www.childline.org.uk | Call 0800 1111



Shout provides 24/7 urgent mental health support via text:

www.giveusashout.org | text SHOUT to 85258

Stop It Now helpline is for anyone worried about child sexual abuse, including their own thoughts or behaviour.



www.stopitnow.org.uk | Call 0808 1000 900



Foreword from Dame Rachel de Souza



The growth of the online world is a technological revolution, the likes of which hasn't been witnessed in centuries.

The internet has enhanced our lives immeasurably, by opening up education, communication and research in ways those of us who are now well into our adulthoods might never have imagined. For children growing up in 2025, who are among the first generations to have never known a solely analogue life, being online is second nature.

It is an incredible asset in our daily lives, but it has also fundamentally changed the nature of how we interact with each other, how we stay safe, and how we maintain privacy. For most children, if not all, it has introduced a darker side. They are forever in their digital playgrounds.

Every day, children tell me about the violent, upsetting or degrading things that are shown to them online by algorithms designed to capture their attention. That's why, as Children's Commissioner, I have been relentlessly focused on driving for greater safety online. It's also been driven by what I saw in children's changing behaviour during my years as a teacher and headteacher, as they learned to navigate a life through a digital lens.



But the subject of this report – sexually explicit 'deepfakes' – is not one I was familiar with until more recently, despite having worked with children every day of my professional life. Of all the worrying trends in online activity children have spoken to me about – from seeing hardcore porn on X to cosmetics and vapes being advertised to them through TikTok – the evolution of 'nudifying' apps to become tools that aid in the abuse and exploitation of children is perhaps the most mind-boggling.

The technology used by these tools to create sexually explicit images is complex. It is designed to distort reality, to fixate and fascinate the user – and it confronts children with concepts they cannot yet understand. The evolution of these tools is happening at such scale and speed that it can be overwhelming to try and get a grip on the danger they present.

I have heard from a million children in my four years as Children's Commissioner. As I enter my fifth and penultimate year, I also have a bank of data from almost 90% of schools in England in my toolkit on the most pressing issues facing their children – that's evidence from around 19,000 safeguarding leads, headteachers, and senior leaders.

It is rare for children and adults to hold the same position on a subject. On this issue, however, they agree: the risks posed by children's unfettered access to harmful content is a constant and growing worry – and one on which children's experiences cannot be sidelined.

On this subject, there is little nuanced debate required. There is no good reason for tools that create naked images of children. They have no value in a society where we value the safety and sanctity childhood. Their existence is a scandal.

As one 16-year-old girl asked during the research phase of this report: "Do you know what the purpose of deepfake is? Because I don't see any positives."

The act of making such an image is rightly illegal – the technology enabling it should also be. Any individual or organisation motivated by the idea of making profit by creating a tool that supports the exploitation of a child must be held to account.

The Government has set an admirable and ambitious mission to halve incidences of violence against women and girls within this Parliament. Getting rid of these exploitative apps and tackling this emerging threat to children would be a significant step towards this mission. Women and girls are almost



exclusively the subjects of these sexually explicit deepfakes: 99% of these images online are of women and girls. Chillingly, evidence suggests that many of the tools designed to create them only work on female images because they have been trained to do so.

The risks to boys are different but equally harmful – studies have shown that teenage boys are predominantly at risk from the influence of Artificial Intelligence and online communities of extremist material, including sexual.

When we talk about children's rights, we mean the 'always' and the 'nevers': the things children should always have, and the things that should never happen to them. This report offers a stark example of the latter. Children are growing up fearing that a smartphone might, at any point, be used as a way of manipulating them.

We owe it to our children, and the generations of children to come, to tackle this now, instead of accepting it as just one more restriction placed on their freedom, and one more risk to their mental wellbeing.

In my *Big Ambition* survey last year, just one in five children told me that politicians and leaders listen to their views. It is time to prove otherwise. Children growing up today are paying the price of our inaction.



Glossary

Age verification - Age verification is a process that confirms a person's age before granting them access to age-restricted goods, services, or content.

Artificial Intelligence (AI) - Technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy.

CSAM – Child Sexual Abuse Material

Clear web: The side of the World Wide Web that is publicly accessible.

Dark web – Web pages that require specific configuration, software, or authorization to access, allowing users and website operators to remain anonymous or untraceable.

Deepfake – Audio-visual media that has been generated or manipulated using AI, which misrepresents someone or something.

Deepfake economy – An ecosystem that enables a wide group of actors to create and trade in deepfakes, including sexually explicit deepfakes.

Fine-tuning - An additional training process that can be applied to pre-trained AI models to add specific capabilities by leveraging particular datasets.

Gen AI – A type of AI that uses generative models to produce media in response to prompts.

Large Language Model (LLM) - A type of AI that is trained on a large amount of data to process, understand, and respond to human languages and text.

Nudification or nudify tools - Apps and websites that produce deepfake nude images of real people.

Open-source (or Open-release) AI models – Models in which the underlying code, or at least parts of the algorithm, are permanently and freely available for other actors to copy, fine-tune, and use as they see fit.



Sextortion – Sextortion is a type of online blackmail. It's when criminals threaten to share sexual pictures, videos, or information about you unless you pay money or do something else you don't want to.

Synthetic media – Synthetic media refers to content partially or entirely generated using AI or machine learning, including images, video, and audio.

Pseudo image – A pseudo-photograph is an image made by computer-graphics or otherwise which appears to be a photograph.



Executive Summary

"Maybe young girls will not post what they want to post or do something they would like to do just in case there's this fear of 'Oh I might be abused, this might be turned into a bit of sexual content' when it shouldn't have been."—Girl, 17, focus group

Generative Artificial Intelligence (GenAl) is transforming the online world. All models can generate text, images, videos, and hold conversations in response to a handful of prompts and are rightly being seen as a development with huge potential for the enhancement of people's lives. However, these tools are also being misused at an alarming cost to children's online and offline safety.

'Nudification' tools are apps and websites that create sexually explicit deepfake images of real people, and at the time of writing, this technology is legal in the UK. GenAI, which is often free to use and easy to programme, has supercharged the growth of these tools. Despite this being a relatively new technology, the high risk of harm it presents to children is increasingly evident.

Children told the Children's Commissioner's Office (CCo) team that the very existence of technology, that could strip people of their clothes, frightened them. In a series of focus groups held with children in their schools (quoted throughout this report), the team heard girls describe how they were trying to reduce the chance of featuring in a sexually explicit deepfake by limiting their participation in the online world- a space which could enhance their social lives, play and learning, if it were safe for them.

This report identifies the threat that sexually explicit deepfake technology presents to children. Currently, it is illegal to create a sexually explicit image of a child. Yet, the technology that is used to do so remains legal and accessible through the most popular parts of the online world, including large social media platforms and search engines.

After analysing what is known about this new technological threat, assessing what it looks like in the online landscape, and speaking to children about what it means for them, this report has found:



• Nudification tools and sexually explicit deepfake technologies present a high risk of harm to children:

- Nudification tools target women and girls in particular, and many only work on female bodies. This is contributing to a culture of misogyny both online and offline.
- The presence of nudification technology is having a chilling effect on girls' participation in the online world. Girls are taking preventative steps to keep themselves safe from being victimised by nudification tools, in the same way that girls follow other rules to keep themselves safe in the offline world – like not walking home alone at night.
- Children want action to be taken to tackle the misuse of AI technology. One girl questioned what the point of it was, if it only seemed to be used for bad intentions: "Do you know why deepfake was created? Like, what was the purpose of it? Because I don't see any positives" Girl, 16.

• Nudification tools and sexually explicit deepfake technologies are easily accessible through popular online platforms

- Search engines and social media platforms are the most common way that users access nudification apps and technologies.
- o GenAl has made the development of nudification technology easy and cheap.
- Open-source Al models that are not primarily designed to create overtly sexually explicit images or videos still present a risk of harm to children and young people

The Children's Commissioner wants GenAl technology, and future Al technology, to be made safe for children, and calls on the Government to:

- 1. Ban bespoke nudification apps.
- 2. Bring in specific legal responsibilities for the companies developing GenAl tools to screen their tools for nudifying risks to children and mitigate them.



- 3. Provide children with an effective route to have sexually explicit deepfake images of themselves removed from the internet.
- 4. Commit to making the online world safer for girls, by recognising sexually explicit deepfake abuse and bespoke services used to carry this out as acts of violence against women and girls.



Introduction

"I feel like girls would be scared [...] I'm somewhat worried that, like, one day this could happen to me. Like, it could happen to anyone around you and like with how good AI is getting, they wouldn't know whether it's real or not. It's kind of scary." – Girl, 16

Children are growing up in a world where anyone - a classmate, a friend, a stranger on the street - can hold a smartphone up at any moment and create a fake image of them naked. Digital tools that can sexualise or digitally remove clothes are no longer niche programmes lurking on the dark web. They are available on the most common app stores and promoted on some of the biggest search engines and social media platforms in the world.

Bespoke tools that create sexually explicit deepfakes have become businesses, and they are making money off the non-consensual doctoring of images. They even have a name: 'nudifying' tools. Nudification tools are bespoke apps and websites that produce deepfake nude images of real people, often using GenAI models. At a time that is seeing high prevalence of misogyny online, it is alarming but perhaps unsurprising, that these nudification tools overwhelmingly target women and girls specifically. Evidence in this report suggests that they often only work on female bodies.

It is illegal to create indecent or prohibited images of children. Nudification tools, though, are not. In this report, the Children's Commissioner sets out the high risk that these tools pose to children, which are currently not prohibited by any law or regulation. The report will:

- 1. Present children's feelings about the existence of nudifying technology.
- 2. Demonstrate the high risk of harm this technology presents to children.
- 3. Highlight how easily these tools can be built and accessed.
- 4. Issue an urgent call for bespoke nudification tools to be banned.



1. Children's views on nudification tools and sexually explicit deepfakes

The team held focus groups with children and young people to find out how much they knew about the existence of nudification tools and sexually explicit deepfakes, and how it made them feel. Their view was one that should be shared by everyone: fear of this technology and concern about what it meant for their safety. This section analyses children's views on four key topics and sets out what children want to be done to keep them safe.

1.1 What the online world looks like to children

As an introduction to the focus group discussions, children were asked about what their online world looked like: the platforms they used, the types of content they see and interact with, and their perception of how people interact and treat one another in online communities. Children shared that they regularly see a wide range of hateful content online, often targeted at women and girls in particular.

"In the comment... a lot of obviously young men, are talking about 'bop'. Which is just a new for way for saying, like, slag. And I think it's become so normalised, like so normalised." – Girl, 16

"Recently one of my friends sent me a TikTok. And it was just a bunch of people hating on this one girl that [...] a video with 1000 views, but every single comment was just hateful." – Boy, 16

Girls also gave details of indirect hate, which takes the form of social media posts that reinforce existing harmful stereotypes, including instances where girls felt women were being pitted against a standard set by men:

"People make like stereotypical jokes about women. Like 'go back to the kitchen, make me a sandwich'. I feel like people think it's light-hearted, but sometimes it's just like unnecessary and like, not even funny." – Girl, 16



"I think it's really disrespectful when you see celebrities in their like 40s on the red carpet and they're like 'Oh, she doesn't look like 40. What's she been drinking, blah blah.' Like, do people think that women just turn into shrivelled up monsters after the age of 30?" – Girl, 17

Notably, girls were able to share more in answer to this question than boys. While boys shared awareness of some of the issues raised by female participants, male participants perceived some of the attention girls experienced online as positive.

"I feel like there's more compliments coming to girls rather than boys." - Boy, 16

Some boys also agreed that they felt online hate was not always gender specific.

"I think it works both ways, but there's always fake accounts hating on them... both genders." - Boy, 16

Children also had lots to share about the presence of hateful content more generally. They indicated that hate is common across some of the most popular social media platforms used by children:

"So this person is being quite horribly racist - what's new? It's kind of become a casual conversation on social media." – Girl, 18

"I think most toxic social media app is two thousand percent TikTok. I think with Snapchat and stuff, there is obviously the physical violence to do with the messages you may be receiving. But when it's like women posting stuff and then backlash they receive, it's just on TikTok. Well, it's not just on TikTok, but I think the majority of the time it's on TikTok." – Girl, 16

"Now on TikTok the guidelines - I don't know what what's going on - but there's videos up there that that's not meant to be up there." – Boy, 16

"I just use Snapchat and unfortunately, TikTok and Instagram. There's no sense of community." – Girl, 17



1.2 Prevalence of AI tools and products

Children are increasingly encountering AI, and media created using AI, including deepfakes, as part of their day-to-day online lives. Children were asked if they had seen deepfake media on social media. Some children said they had on platforms such as Instagram, TikTok and X.

Many of the children's comments about their exposure to deepfakes indicated that the fake images or videos were intended to be playful, and were not sexually explicit.

"I see lots of deepfakes, especially on like TikTok, just like memes in general. Like something with a caption can be quite funny." – Boy, 16

However, some of the tools children had seen being used to create synthetic media intentionally sexualised the subject.

"I've seen one before, it like, makes two people kiss." - Boy, 17

"There was some trend on TikTok where girls... had a picture of their boyfriend and they was making it like dance to some song. And then they were making the actual picture dance." – Girl, 16

Most children the office spoke to had not come across a specific nudifying app before. However, it transpired that nudifying apps were being advertised to children on popular social media apps.

"I've seen some advert I believe on TikTok, where it's like basically showing someone with their phone, like recording someone, and then they're showing like [...] they're wearing like a dress or something, then underneath they're showing them in pants after." – Boy, 16

Al tools are becoming increasingly prevalent on online platforms, but children indicated that they often found it difficult to identify content created using it.

"I sometimes struggle to pick out what's truly AI because it just keeps getting better." – Girl, 17

"I think AI is developing, deepfake is increasing and I've seen it more social media. And before, like a few years ago, I wouldn't really see it online. But now, like there's a lot of edits of like national leaders getting mocked by deepfaking." – Boy, 16



1.3 Gendered harm

Girls fear nudification technology in much the same way as they would fear the threat of sexual assault in public places. For girls, the threat is just there. Boys, on the other hand, explained that they would only feel worried about it if they could justify why it would happen to them in some way, for example, as a retaliation in a conflict.

For girls, harm lay in the possibility of sexually explicit deepfakes being produced, and also how these deepfakes contributed to an existing culture of misogyny online.

"I feel like that the immediate one is fake pornography [...] so many female celebrities are now having their face like copy pasted onto these like revealing photos. And it's just like damaging to their reputation." – Girl, 16

"I think having a sexualised image of young people, it's kind of saying, 'Oh no...we're men and we're better than you and we're stronger than you so we can take these images of you and you should just be fine with it, because we're the dominant ones'." – Girl, 18

"The narrative like Andrew Tate and influencers like that... backed by a quite violent and becoming more influential porn industry is making it seem that AI is something that you can use so that you can always pressure people into going out with you or doing sexual acts with you..." – Girl, 18

These children have made the link between online content and offline threats to their safety. Such a worry taps into the growing concern about the impact this harmful content has on boys and young men's attitude towards women and girls. Girls also expressed concern that deepfakes could be used against women and girls to coerce or blackmail them into acts they would otherwise not consent to.

"God-forbid they go to that length, they could like slander your person, your character... simply because they didn't like you as a person." – Girl, 17

"Like revenge porn - you might have like publicly rejected them or something, they might try and do that." – Girl, 16



"So like if you say 'no, I don't like you' I think it's now becoming more commonplace for them to say, 'OK, well, I'm going to make a deep fake of you and ruin your life because you rejected me'." – Girl, 18

When asked specifically about what risks nudification tools would present to women and girls, girls set out that the technology made it easier to commission acts of violence against women and girls, of which the creation of sexually explicit deepfakes is one.

"It's so easily accessible that anyone could just make those photos, put them on the Internet and just like ... create a big controversy just because they like clicked a few buttons on a mobile app." – Girl, 16

Girls reported withdrawing from their online and offline lives out of fear that they will be victimised by nudification technology. This chilling effect is causing them to take steps to keep themselves safe, which often requires them to limit their behaviour in some way. This pattern of behaviour is similar to girls avoiding walking home alone at night, or not going to certain public places alone.

"I feel like girls would be scared [...] I'm somewhat worried that, like, one day this could happen to me. Like, it could happen to anyone around you and like with how good is like AI is getting, they wouldn't know whether it's real or not. It's kind of scary." – Girl, 16

"That risk that people can just get a photo of you from the Internet and make it - it's more and more worrying." – Girl, 16

"Maybe young girls will not post what they want to post or do something they would like to do just in case there's this fear of 'Oh I might be abused, this might be turned into a bit of sexual content' when it shouldn't have been." – Girl, 17

Girls also explained what steps they were already taking to keep themselves safe online. Many of them involved reducing their presence in the online world. This consideration was not brought up by the boys the office spoke with, suggesting that this is not something they think about in the same way.

"Because my accounts are private and I don't reveal my face online, I feel somewhat safe. But also like, even without my face being like on social media if like ... kind of outlandish scenario, like one day like a close friend, someone I trusted, took an image [of me]... and made it into something and put it onto the



Internet for everyone to see, I would feel unsafe. There's always kind of that in the back of my mind. Like, what if?" – Girl, 16

Finally, girls did not see many benefits to this technology, they were consumed by the risks:

"Even before any controversy came out, I could already tell what it was going to be used for, and it was not going to be good things. I could already tell it was gonna be a technological wonder that's going to be abused." – Girl, 16

In the focus groups, one girl asked a member of the CCo staff what the point of the technology was, because they couldn't understand what good it could bring: "Do you know why deepfake was created? Like, what was the purpose of it? Because I don't see any positives." – Girl, 16

Boys, overall, did not view deepfake technology in the same way as girls. In contrast to the threat of the mere existence of this technology, boys viewed the personal risk from deepfakes as conditional. Boys felt that there would need to be a reason for a perpetrator to create these images, as opposed to them doing so simply because they were able to.

"I don't think anyone hates me enough to." – Boy, 17

"It depends on the intention of the deepfaker. Because like someone might be doing it to set someone up, or some might be doing it to joke along with their friends?" – Boy, 17

"I feel like if it's a deepfake of someone famous, then there's going to be some sort of like political motive to it. If it's someone that's like, normal, I'd say more likely to be likely to be blackmail because realistically, what else would you get out of it? Apart from blackmail."— Boy, 16

1.5 What children want

Children want the risks of AI and deepfake technology to be tackled. Children had different views on how deepfake technology specifically should be addressed, with some advocating for the technology to be banned outright. Their suggestions echo their requests for how other online harms should be tackled in other research carried out by the CCo³ – including age checks, better reporting mechanisms, and content moderation.



"Restricting heavily or even banning like these AI generated images and content because they're very misleading, I think just restricting them would be better for social media as a whole." – Girl, 16

"Obviously it's complicated to put that in place quickly, but that doesn't affect the fact that it still should be put in place and having those strict regulations isn't like affecting freedoms of social media. It's protecting people." – Girl, 18

Some children asked for technology companies and the government to take less restrictive steps to protect them. Some suggestions included:

"It's just an app where you can do things like can be compared to any other editing app. But I think at the same time there should be restrictions on what kind of images you can create on these apps like stuff like this, like nudity and stuff I think should be just taken off." – Girl, 16

"[...] to confirm your age they should be able to use ID. Because most people on the internet they lie about their age and it could be harmful." – Boy, 17

Children also made technical suggestions to social media companies, who they viewed as having responsibility for this issue:

"Technology can detect certain things and images right? So it should be able to detect what images people are uploading." – Girl, 17

"There should be like regulation on the tools you can use to make the deepfakes, and let's say on TikTok and Instagram, if you are posting something, to check if it's like a deepfake or not." – Boy, 16

"I think they need to do a better job of looking at the videos and actually taking the reports seriously, because I know some reports are getting ignored." – Boy, 16

Children also wanted to highlight that they noticed the positive impact of some types of content regulation that already exists on some specific online platforms.

"The moderators are definitely much more on it. So it feels as though the worst thing you'll get will be a passive aggressive comment, but you will never see something really aggressive on the app for long because it'll get deleted." – Girl, 17 – Reddit in comparison to TikTok



2. What we know about children's exposure to sexually explicit deepfakes

As well as children's own awareness and experiences of nudifying technology, there is a growing body of evidence that children are being directly impacted by deepfake nudification services.

2.1 The technology

2.1.1 Nudification tools

Nudification tools are bespoke apps and websites that produce deepfake nude images of real people. They are often created by fine-tuning GenAl models.

Nudification tools, including nudification apps and websites, are in scope of pornography provisions in the Online Safety Act, which requires services that provide pornographic content⁴ to ensure, by use of age estimation or age verification, that children are not normally able to access pornographic content in relation to the service.⁵

The growth of these user-friendly apps has been attributed to the emergence of what is now being called the 'deepfake economy' – an ecosystem that facilitates the creation and distribution of sexually explicit deepfakes between users for profit. Last year, Ofcom assessed that bespoke apps make up one of the three main pillars of deepfake economy, alongside individual creators and hosting sites.⁶

THE LAW

It is illegal to possess AI-generated sexual content featuring children, but the AI models that create these images are not illegal.



2.1.2 Who are the targets of nudification tools?

Women and girls are almost exclusively the subjects of sexually explicit deepfakes. 99% of sexually explicit deepfakes accessible online are of women and girls, and the tools that are used to create them often do not work on men and boys. One plausible explanation for this is that these tools are typically trained on large datasets of sexually explicit imagery. All tools create images by learning from, and replicating elements of, existing images. This means that these tools are likely to only work on female bodies because they have been trained largely on images of female bodies.

There is a high and an ever-increasing demand for sexually explicit deepfakes. Content on the most visited bespoke websites for sexually explicit deepfakes received 40 million views in the month of January 2024. Google searches for the term 'deepfakes' increased by 76% between 2019 and 2023, with the related search terms almost exclusively being female celebrities. Typically, these are of adult celebrities, but analysis of the most popular deepfake websites and providers has found that underage women, 'teen' celebrities, and children's characters are also being created and sold.⁹

Despite the demand for pseudo images of high-profile women, it is ordinary women who have been identified as the most targeted group for nudifying apps.¹⁰ Analysis shows an exponential increase in the volume of sexually explicit deepfakes online.¹¹



Table 1: Top 10 most targeted persons on leading deepfake porn website. 12

Name	Age (2025)	Age at time of career breakthrough	No. of videos on a leading deepfake porn website (2024)
Emma Watson	34	11	1052
Scarlett Johansson	40	13	904
IU	31	15	859
Gal Gadot	39	19	623
Natalie Portman	43	13	589
Margot Robbie	34	18	559
Elizabeth Olsen	36	22	517
Wonyoung	20	14	482
Irene	34	22	458
Millie Bobby Brown	21	12	456



2.1.3 The impact on girls and young women

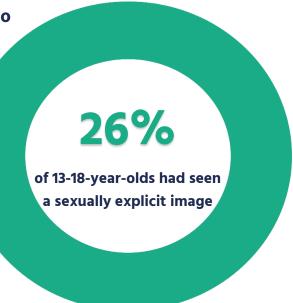
The wider evidence supports what children told CCo: that the negative impact of this technology being used and available disproportionately affects girls and young women. A 2023 study by Internet Matters found that 38% of girls strongly agreed that featuring in a nude deepfake would be worse than in a real nude image, in comparison to 27% of boys.¹³ This suggests that the additional burden of an image being non-consensual, and fake, adds to the negative impact of sexually explicit images being made or shared of women and girls. This impact has been detailed in the Children's Commissioner's report on harmful sexual behaviour.¹⁴

2.2 Children's exposure and use of this technology

The high risk of harm presented by nudification technology has been set out in the section above. The following will present what is known about children's exposure to it. The challenge here is that, as this technology is relatively new, evidence is relatively scarce. Nonetheless, what does exist, builds a case to say there should be an indictment against nudification tools.

2.2.1 Children are increasingly being exposed to sexually explicit deepfakes

A 2024 survey by Internet Matters found that 13% of teenagers have had an experience with a deepfake nude. This might be seeing, receiving, or sending one. A similar survey carried out earlier this year by Girlguiding suggests that children's exposure is rising: it found that 26% of 13-18-year-old respondents had seen a sexually explicit deepfake image of a celebrity, a friend, a teacher, or themselves.





2.2.2 Young people are more at risk than adults

Studies into young people's exposure to sexually explicit deepfakes have also found that children are most at risk of exposure to this material. Young people aged 16-24 were more likely to be exposed to sexually explicit deepfakes than adults aged 55+ (20% v 6%).¹⁷

2.2.3 Children can be perpetrators of deepfake sexual abuse

In the UK, the National Crime Agency has recently identified online communities of teenage boys sharing extreme and sadistic material, including sexual material, as an emerging threat to radicalisation and extremism. The report found that AI was expediting offences, and the offenders were predominantly teenage boys. The Children's Commissioner has previously highlighted that children feel that exposure to, and normalisation of, pornography is influencing harmful sexual behaviour among children. Sexually explicit deepfakes should be considered in the context of these emerging patterns and regarded as an additional factor in harmful behaviours among children.



2.3 The high risk of harm to children

2.3.1 Sexually explicit deepfakes present a high risk of harm to children.

Some children are more vulnerable than others

25% of children with SEN status, children with EHCPs and children with diagnoses of physical or mental health conditions reported seeing, receiving or sending sexually explicit deepfake media. This is a higher figure than the 11% of children without these markers of vulnerability.

Internet Matters, The New Face of Digital Abuse: Children's experiences of nude deepfakes, October 2024, Link

Nudification tools are entirely harmful to children. There are no positives to children being exposed to them or their products. Children come to harm as a result of direct exposure to nudification tools. Internet Matters identified the three ways this harm occurs: through child-on-child sexual abuse, adult-perpetrated child sexual abuse, and sextortion.²⁰

It is illegal to possess AI-generated sexual content featuring children. Crucially, the AI models that create these images are not illegal. This includes AI models that are trained on child sexual abuse material. This has left a loophole in legal safeguards that a number of organisations have said is facilitating paedophilic offences²¹ and the creation of Child Sexual Abuse Material (CSAM).

Beyond facilitating paedophilic behaviour, sexually explicit deepfake material and technologies have a direct impact on the wellbeing of victims. Adult victims of deepfake sexual abuse, where perpetrators create sexually explicit deepfakes without a persons' knowledge or consent, have reported experiencing PTSD and the onset of suicidal ideation.²² Children can never consent to their image being manipulated or taken in this way, and the act of doing so is already illegal.²³ Yet, the evidence shows that children are being exposed to this material, and are being victimised using this technology. Child victims have died by suicide as a result of deepfake abuse, including Mia Janin who died in March 2021.²⁴

Nudification tools also cause harm to children indirectly. Some human rights organisations have highlighted that the growing culture of misogyny online is having a silencing effect on women and



girls,²⁵ and the Children's Commissioner's findings set out in section 1 of this report confirms that the existence of these tools are indeed frightening girls into reducing their participation in the online world.

3. The deepfake economy

Ofcom has highlighted that an increasing user base of nudification tools, coupled with accessible tools and transactions between users and developers, has created a 'deepfake economy'. The CCo carried out a review of what nudification apps look like in this economy in order to understand just how easy it is for children to get caught up in it.

Tools require parts. Before this report sets out what some of the bespoke nudification tools look like, or how they are accessed, it is important to understand how these tools are built in the first place.

3.1 Open-source AI models

Open-source AI models are software in which the underlying code (such as Stability AI's Stable Diffusion), or at least parts of the algorithm (such as Meta's Llama 3), are permanently and freely available for other actors to copy, fine-tune, and use as they see fit. It means that users are theoretically able to use models to create content that was not its original purpose.

The Internet Watch Foundation has identified open-source AI models to be the tool of choice for paedophiles to create AI generated Child Sexual Abuse Material (CSAM) and named it as the main threat in the AI CSAM landscape. The organisation has found that perpetrators can legally fine-tune open-source AI models to create this material.²⁷ These models are not marketed for the purposes of nudification, but they provide the tools for individuals who wish to build bespoke tools. A social media analytics firm, Graphika, found that the quick and low-cost nature of open-source generative AI models was the primary driver of the growth of the creation and dissemination of non-consensual intimate image abuse of adults, including the growth of nudification apps.²⁸

In making the assessment that open-source AI models present the biggest CSAM threat, the Internet Watch Foundation did not name the open-source AI models they encountered on CSAM forums or in any of the material they analysed. They indicated that some of the more well-known providers were

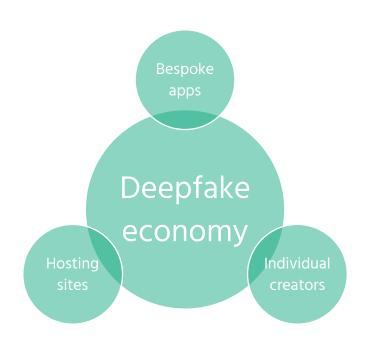


aware of the risk they presented, and were taking steps to mitigate the misuse of their models to create illegal material.

Despite the documented increase in AI CSAM images being available on both the dark and clear web, it remains unclear just how far these open-source AI models are capable of being used to create CSAM image generators and nudification services. AI providers are not required to make the AI's training data public, meaning there is no independent oversight of the appropriateness or legality of AI's learning curriculum.

3.2 The deepfake economy

The deepfake economy is made up of three parts: websites, individual users, and bespoke apps.



Analysis by a social media analytics firm, Graphika, found that nudification and sexually explicit deepfake providers have progressed from occupying niche corners of the internet to being fully-fledged online businesses. ²⁹ As businesses, these providers have monetised the demand for sexually explicit deepfake images and are profiting from their creation - which this report has identified as an act of violence against women and girls.

3.2.1 Bespoke nudification apps

Nudification apps and tools are developed and launched frequently. Industry assessments now show that deepfake non-consensual intimate image providers "operate as a fully-fledged online industry". Unlike the general GenAl image editing apps described in the section below, which are marketed for general image editing purposes, bespoke nudifying apps have the sole purpose of creating



sexually explicit deepfakes. The CCo encountered a number of apps that offered services to, for example, "hotify every body you wanted to but were afraid to" (see Figure 1 for example).

The CCo carried out a search for commonly used nudifying apps both on app stores and social media platforms. Of the results that were generated, the office considered it notable that the descriptions and images used to promote the apps explicitly presented female subjects as the targets.



Figure 1

Figure 1 depicts one of the top search returns for the search term 'undressai' on a popular social media site. The images depict a before and after picture of a woman who has had her clothes digitally removed. The caption invites users to "undress any woman with this new Al". The title image itself is of a woman's face, which emerged as a pattern with other results for other nudifying apps being advertised on that social media site.

As an entry point to the process of creating sexually explicit deepfakes without requiring the knowledge or consent of the subject, these apps present a high risk of harm to children, not only because they present criminals with a method of preying on them, but because they normalise representing women in this way



3.2.2 Other image editing apps

There are a range of media editing apps available to download and use to create or alter images. Most of these are marketed for that purpose, and they have a high level of creative potential, which children have told the team they find fun and inspiring. However, these apps can be used for the purposes of sexualising images if they are not designed with mechanisms against it. The CCo has learned that there are some AI image editing apps that can change images into videos. These AI tools display great sophistication, but the Commissioner is concerned that these seemingly innocuous tools could be used to sexualise children.

Case Study: ViggleAl

"There was some trend on TikTok where like girls were making like, they had a picture of their boyfriend and they was making it like dance to some song. And then they were making the actual picture dance. So like, I saw that and that was ViggleAI." – Girl, 16

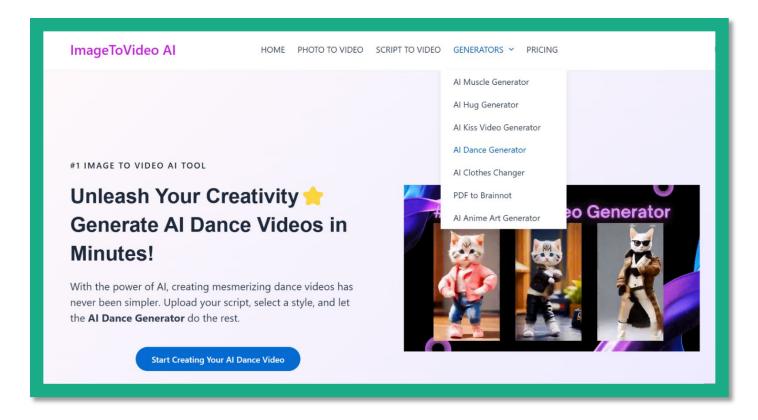
One child in the Children's Commissioner's discussion group, carried out for this study, named Viggle AI as an app they had encountered which made images of people they knew dance.

The Office is aware that whilst most dancing is harmless and fun, there are some styles of dancing that risk sexualising the dancer. The Office is concerned that unregulated apps like this one may be trained on data featuring sexualised dancing, and that it is this that the AI model recreates when generating a video from the image uploaded – regardless of whether or not it is a child. Like many image generating and editing tools, Viggle AI's terms and conditions mandate users to not use the tool for illegal purposes and that the company had the discretion but not the obligation to remove or disable content as it sees fit.

For ViggleAl's Terms of Service, follow this link.



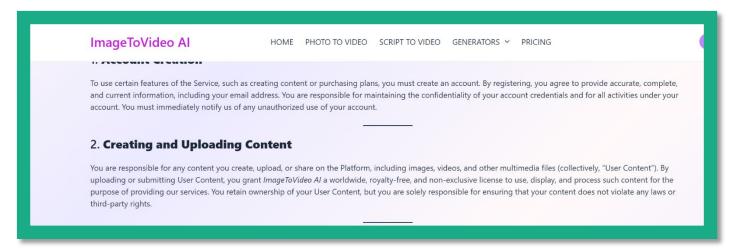
Figure 2 shows the options users can choose to turn an image into a video.



Like ViggleAl, ImagetoVideo Al gives users a tool to make an image dance. It also gives users a tool to generate an Al Hug, an Al Kiss, Al Anime and Al Muscle. There is also a tool for Al Clothes Changer, which allows users to replace the clothes of a user with a selection of options. There is no age verification for this tool, which means children could upload their own pictures and dress them in clothes designed for adults, or adults could upload images of children without any barriers. The company itself, like many of the other image editing tools the CCo found, retained no responsibility for legality of the content that is created (see Figure 3 for terms of service).



Figure 3



ImagetoVideo AI is an example of a GenAI tool that is not marketed for the primary purpose of creating sexually explicit deepfakes but would have the capacity to create problematic or illegal content. If a user were to be looking for a bespoke nudification app, the CCo found that searches for known nudification apps returned results for image editing apps that did not feature nudification in their descriptions.

3.3 Accessing nudification tools

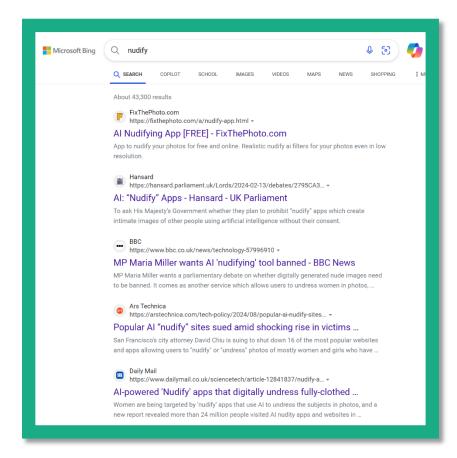
Nudification tools are no longer a reserve of the dark web. Websites, apps, and providers are accessible through common and popular parts of the online world, including through search engines and social media sites that are most commonly used by children. Ofcom has suggested that instances of children being exposed to these tools are being driven up because they are so accessible and easy to use.³⁰ The following section of this report will set out just how easy it is for child users to be exposed to these tools.

3.3.1 Search engines

A large-scale piece of analysis of the deepfake landscape found that 68% of web traffic to specialised deepfake pornography sites came through Google search. ³¹ The research also found that simply searching for the term 'deepfake' and a celebrity's name returned results for sexually explicit deepfake websites on the first page of search results 99.7% of the time.



Figure 4



When the CCo carried out a simple search on Microsoft Bing, a nudification tool made its way to the top of the search results (see Figure 4).

Search engines are notable points of access for these tools, and their use for this purpose has been rising steadily since January 2023. Google trends show that searches for 'undress app', 'deep nude ai' and 'deep nude' searches increase from that month, and peak in the first quarter of 2024. This coincides with the circulation of a nude deepfake of a high-profile female singer, Taylor Swift.³²

It is notable that despite being identified as key points of access, and the growing attention on this issue especially around the time a high-profile female celebrity was victimised using this technology, the CCo was still served links to these sites on the first page. This presents a question about how effective the platforms' downranking of these results are, if at all. Search engines are not required to age-gate their services or search terms, which is additionally concerning as child users could be served similar results as adult ones.



3.3.2 Social media sites

Recent industry analysis has found that users encountered nudifying services on social media sites, before being referred onto specialised deepfake websites or mobile stores to download specific apps.³³ Instagram, Telegram and X were some of the social media platforms named in Graphika's *Revealing Reality* report, which is especially concerning given that the CCo's previous research has shown that

children as young as 8 are accessing these platforms.³⁴ Social media platforms have also been identified as the main platforms used by children to share sexually explicit deepfake images.³⁵

The CCo searched for well-known nudification apps on X, after one of the Office's ambassadors named this site as the most likely place they felt they would be exposed to inappropriate pornographic material. The Children's Commissioner's Office Ambassadors are young people selected to represent young people and inform the work of the CCo. The Office found that accounts had been created on that site to promote nudification apps and tools. Most of the account descriptors specified that their tools could be used on girls, and the majority of the accounts that had profile images featured sexualised images of girls. Concerningly, some of the accounts were X Premium accounts.

X PREMIUM ACCOUNTS

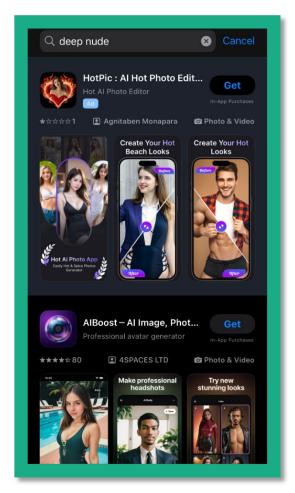
X accounts that feature a blue tick are called X Premium accounts. Before a change in ownership of X, when the site was known as Twitter, the blue tick was only featured on accounts that were verified and notable. They were symbols of status and designed to instil trust in particular accounts. This changed in 2023, when Twitter became X and blue ticks were used to instead signify that an account was a paying subscriber to X. At the time of writing, an X Premium account costs £2.50 a month.



3.3.3 App stores

Finally, the CCo has found that searches for nudification apps on Apple's app store returned results for nudification tools.

Figure 5



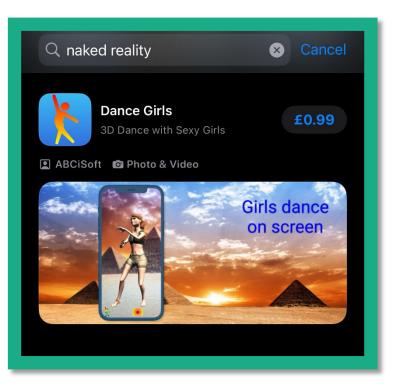


Figure 5 shows the search results for "deep nude" and "naked reality" on Apple's app store in January 2025. Deepnude was one of the first nudification apps that used an AI model to remove clothes from subjects in images, and it was removed from app stores shortly after it was released in 2019.³⁶ It is notable that the top two items returned for this search include one overtly sexualising AI tool ('Hotpic'), and the other was an otherwise generic image editing tool ('AIBoost'). As has already been explained in the



earlier part of this report, generic image editing tools can have the capacity to create sexually explicit images.

This report has gathered evidence to justify calling for a ban of bespoke nudification technology, regardless of whether they are intended to be used on children or not. The next part of the report will set out what the law currently says, and then present recommendations that will fix the legal loopholes that have left children exposed to the harms of this technology.



4. What needs to happen now?

There is no good reason for bespoke nudification tools to exist. While AI technology presents policy makers with a number of hugely difficult decisions, what to do about nudification tools isn't one of them. The Children's Commissioner is calling for these tools to be banned, and for the UK to create a regulatory environment that would make technology being misused in this way impossible. Technology companies should be responsible for the way their AI tools are used, and these recommendations for Government will set that responsibility down in law and in practice.

4.1 What the law currently says

In early 2025, the UK Government announced it would be extending some of this protection against the creation of sexually explicit AI content to adults in the Data Use and Access Bill.³⁷ It has also brought forward the creation of purported intimate images of adults in the Crime and Policing Bill.³⁸ At the time of writing, both of these laws are still undergoing parliamentary process. Both these laws place criminal responsibility on individuals, but they will not make the AI models that create this material illegal.

The Online Safety Act 2023 puts legal responsibility on online platforms operating in the UK to prevent UK users from encountering illegal content online, including child sexual abuse material.³⁹ The Act also mandates technology companies to prevent children from coming to harm from content that is harmful to them, including pornographic content.⁴⁰

Ofcom's new Children Codes, which will come into force in July 2025, will improve protection of children from services designed for adults and from seeing some harmful content. They don't make the provision of nudifying services illegal.⁴¹

4.2 The Children's Commissioner's recommendations for change

4.2.1 Outlaw nudification tools

The Children's Commissioner's desired outcome is for bespoke nudifying apps to be outlawed in the UK. This is something children specifically requested when talking to the team writing this report. That should include two distinct legislative measures:



- 1. **Legislation:** the Government should legislate to explicitly ban AI tools that are designed or marketed as nudification services. This could be achieved in a number of ways, for instance:
 - An amendment to the **Product Safety and Metrology Bill:** to ensure that providers of products or digital products that rely on a Gen AI system carry out risk assessments for illegal and harmful activity and take reasonable steps to design that risk out of the product.

This will: mean that tools developed using Gen AI models have to be risk assessed for illegal and harmful activity before they are available in the UK. Bespoke nudification apps in their current form will not prove themselves safe against illegal activity and will not be certified to be available in the UK.

- 2. **Legislation:** for the Government to introduce an **AI Bill** in this parliamentary session. The AI Bill must make it the responsibility of providers of GenAI models to prevent their use for nudifying children. For example:
 - Make it a legal requirement for technology companies to test their products against whether they can be used to nudify children prior to launching them in the UK market;
 - For the compliance of this statutory risk assessment to be outcomes based. This means that
 the providers of GenAI models that are used by individuals to nudify children would be held
 accountable for that.

This will: mean that LAI firms will be held responsible if their products are used to create explicit deepfake images of children in the UK.

The risk to children from bespoke nudification apps, and the misuse of GenAI tools to create sexually explicit deepfakes, is deeply concerning and must be urgently addressed.

Outside of legislation, there are a number of interim actions that policy makers should take to protect children. The Commissioner makes these further recommendations to provide protection to children in the interim:



4.2.2 Short term solutions

While the legislation set out in recommendations 1 and 2 passes through parliament, the Children's Commissioner is calling for:

3. **Regulation**: for Ofcom to fully enforce the Online Safety Act, including ensuring that the safety duties held by **Part 5 services** are fulfilled effectively. Nudification services, as providers of sexually explicit or pornographic material, are in scope of this.

This will: mean that nudification services will be required to verify that users are over 18 before allowing them access to content.

This will not: in isolation provide sufficient protection to children from the high risk of harm presented by these apps. As this report has shown, children are frightened by the very existence of these apps. Making these apps available only to adults will not remove the threat to children. This recommendation is a short-term and partial solution while the legislative recommendations 1-2 are put in place to provide children with more long-term protection.

4. **Regulation:** for Ofcom to strengthen the **Children Codes** to ensure its risk assessment process is proactive against emerging harms. Nudification apps are an example of a harm that has emerged as a result of a new technology. The risk assessment that social media companies are required to carry out in order to comply with the Online Safety Act should be outcomes based, and include proactive inputs to assess the risk of children encountering harmful content, such as pornographic material.

This will: mean that more popular technology platforms, like social media platforms, will be required to identify and mitigate the risk to children of content produced by sexually explicit deepfake tools, including content used to proactively market them. This means platforms will be seeking out the harm before it gets to the child.

This will not: remove the threat of these apps to children because they will still be available to adults. It will only make them harder for children to find.



5. **Support:** The Government should provide the necessary support for children to report an intimate image – including false ones that have been created using AI - that has been shared in a public online space, and to get it removed. Examples of services that already exist include Report Remove, a service run by Childline and the Internet Watch Foundation.

This will: provide children with a reactive solution on an individual level.

This will not: prevent these images being created or uploaded in the first place. This recommendation is a short-term solution while the legislative recommendations 1-2 are put in place to provide children with more long-term protection.

6. **Regulation:** The Government should ask Ofcom to require technology companies in scope of the Online Safety Act to embed the **Report Remove** tool into their services. This requirement should be specified in the Illegal Harms safety measures set out in the regulator's Illegal Harms Codes.

This will: mean a reactive solution is easily accessible to children who need it on an individual basis.

This will not: be enough alone to signal technology companies' compliance with the Online Safety Act's illegal harms duties.

The above legislative and regulatory changes are necessary to safeguard children in the short and long term. In addition to these, the Commissioner recommends:

7. **Education:** for sexually explicit deepfake technology to be included on PSHE curriculums.

This will: give children the vocabulary, knowledge, and confidence to talk about this topic

This will not: absolve responsibility from Government, Ofcom and technology companies to keep children safe from the harms of this technology. Children are not responsible for keeping themselves safe online when the technology itself is fundamentally unsafe.

8. **Recognition:** for the Government to call the use of technology to create nonconsensual sexually explicit deepfakes an act of violence against women and girls, and to commit to tackling it in the Government's VAWG strategy to be released later this year.



This will: give this problem the weight and attention it warrants.

This will not: be effective without targeted legislative measures, highlighted above, that demonstrate a commitment to solving this problem.

5. Methodology

Focus groups

The CCo hosted focus groups with 22 children aged 16-17 in January 2025. This comprised of three separate groups, from two different schools: one in London and one in Bristol. Groups were split by gender to encourage more open conversation: one group of 7 boys, one with 7 girls, and one with 8 girls. Each group was facilitated by two CCo researchers and was audio-recorded and later transcribed. The questions prepared for the discussion covered their perceptions of how people, particularly women and girls, are treated in online spaces, their familiarity with and understanding of deepfake images, the impact that these images have on their online and offline lives, and what should be done about the images and the tools used to create them.

Notes and transcripts from these discussions were reviewed and analysed to identify common themes, and to bring out illustrative anonymised quotes used throughout this report.

Market review

The CCo carried out a review of organic searches to establish how accessible the sexually explicit deepfake economy was.

The Office selected names of known nudification apps to use as search terms. These were chosen after a media analysis was carried out of the online articles published about nudification apps or technology between 2019 and 2024. In the case of one search term, 'naked reality', this was chosen after it was suggested as a result on an app store in response to another search term. The Office carried out organic searches of the terms 'nudify', 'undressai', 'undress ai', 'deepnude', 'deep nude', 'clothoff' and 'naked reality', on:



- Search engine: Microsoft Bing

- Social media platforms: X and Instagram

- App stores: Apple

The CCo then gathered screenshots of the suggestions on the first 3 pages of the search engine, first 10 suggestions on the app store, and first 10 suggestions on the social media platforms. The CCo then carried out a literature review to trace if the apps or accounts had been discovered on these sites before.

The devices used were a Department for Education laptop and an iPhone.



References

1 Graphika, A revealing picture: Al-generated 'undressing' images move from niche pornography discussion forums to a scaled and monetized online business, December 2023, Link, accessed 24th March 2025

2 Savanta for Amnesty UK, Gen Z in the UK: Perceptions and experiences of misogyny on social media, March 2025, Link, accessed 9th April 2025

3 The Children's Commissioner for England, I've seen horrible things: children's experiences of the online world, October 2024, Link, accessed 9th April 2025

- 4 Online Safety Act 2023, Part 5 section 80 (2)
- 5 Online Safety Act, Part 5 section 81
- 6 Ofcom, Deepfake Defences: mitigating the harms of deceptive deepfakes, July 2024, Link, accessed 24th March 2025
- 7 Internet Matters, The New Face of Digital Abuse: childrens experiences of nude deepfakes, October 2024, Link
- 8 International Union of Sex Workers, What are 'Nudify' apps? Link, accessed 24th March 2025
- 9 My Image My Choice, Deepfake Abuse: Landscape Analysis, 2024, Link, accessed 24th March 2025
- 10 My Image My Choice, Deepfake Abuse: Landscape Analysis, 2024, Link, accessed 24th March 2025
- 11 My Image My Choice, Deepfake Abuse: Landscape Analysis, 2024, Link, accessed 24th March 2025
- 12 Mrdeepfakes.com is the leading deepfake porn website. Data from My Image My Choice, Deepfake Abuse: Landscape Analysis, 2024, Link, accessed 24th March 2025. Note that some of these women were at the height of their fame when they were children, for example Emma Watson, who starred in Harry Potter and the Philosopher's Stone when she was 11.
- 13 Internet Matters, The New Face of Digital Abuse: childrens experiences of nude deepfakes, October 2024, Link
- 14 The Children's Commissioner for England, "A lot of it is actually just abuse": Young people and pornography, January 2023, Link, accessed 24th March 2025
- 15 Internet Matters, The New Face of Digital Abuse: childrens experiences of nude deepfakes, October 2024, Link
- 16 Girlguiding, 'One in four teens have seen pornographic deepfakes online' Girlguiding, February 2025, Link, accessed 25th March 2025
- 17 Ofcom, Online Nation 2024, November 2024, Link, accessed 24th March
- 18 The Guardian, 'Online gangs of teenage boys sharing extreme material are 'emerging threat' in UK', March 2025, The Guardian, Link, accessed 31st March 2025
- 19 The Children's Commissioner for England, "A lot of it is actually just abuse": Young people and pornography, January 2023, Link, accessed 24th March 2025



- 20 Internet Matters, The New Face of Digital Abuse: childrens experiences of nude deepfakes, October 2024, Link
- 21 Internet Watch Foundation, How AI is being abused to create child sexual abuse imagery, October 2023, Link, accessed 24th March 2025
- 22 Professor Clare McGlynn, 'Deepfake porn: why we need to make it a crime to create it, not just share it', The Conversation, April 2024, Link, accessed 24th March 2025
- 23 Protection of Children Act 1978 and section 62 Coroners and Justice Act 2009; section 160 Criminal Justice Act
- 24 Sarah Hooper, 'Girl killed herself when bullies shared fake nudes of her', Metro, January 2024, Link, accessed 24th March 2025
- 25 Amnesty International, #toxictwitter: violence and abuse against women online, 2017, Link, accessed 24th March 2025
- 26 Ofcom, Deepfake Defences: mitigating the harms of deceptive deepfakes, July 2024, Link, accessed 24th March 2025
- 27 Internet Watch Foundation, What has changed in the AI CSAM landscape? July 2024, Link, accessed 9th April 2025
- 28 Graphika, A revealing picture: Al-generated 'undressing' images move from niche pornography discussion forums to a scaled and monetized online business, December 2023, Link, accessed 24th March 2025
- 29 Graphika, A revealing picture: Al-generated 'undressing' images move from niche pornography discussion forums to a scaled and monetized online business, December 2023, Link, accessed 24th March 2025
- 30 Ofcom, Deepfake Defences: mitigating the harms of deceptive deepfakes, July 2024, Link, accessed 24th March 2025
- 31 My Image My Choice, Deepfake Abuse: Landscape Analysis, 2024, Link, accessed 24th March 2025
- 32 Sky News, 'Why is viral Taylor Swift deep fake so alarming?' January 2024, Link, accessed 24th March 2025
- 33 Graphika, A revealing picture: Al-generated 'undressing' images move from niche pornography discussion forums to a scaled and monetized online business, December 2023, Link, accessed 24th March 2025
- 34 Children's Commissioner, Digital childhoods: a survey of children and parents, 2022, Link
- 35 Center for Democracy and Technology, In Deep Trouble: Surfacing Tech-Powered Sexual Harassment in K-12 Schools, September 2024, Link, accessed 24th March 2025
- 36 BBC News, 'App that can remove women's clothes from images shut down', BBC News, June 2019, Link, accessed 24th March 2025
- 37 UK Government Ministry of Justice, 'Better protection for victims thanks to new law on sexually explicit deepfakes', January 2025, Link, accessed 24th March 2025
- 38 UK Government Ministry of Justice, 'Government crackdown on explicit deepfakes', January 2025, Link, accessed 24th March 2025
- 39 Online Safety Act 2023, Schedule 6
- 40 Online Safety Act 2023, Section 60
- 41 Ofcom, Statement: Protecting children from harms online, April 2024



CHILDREN'S COMMISSIONER

Sanctuary Buildings, 20 Great Smith Street London, SW1P 3BT

020 7783 8330

www.childrenscommissioner.gov.uk

- @childrenscommissioner
- @ChildrensComm
- **f** @childrenscommissionersoffice