Evolution of AI in child sexual abuse material

Published on 22 May 2025 Written by Beckie Rackham, Media Office Team Leader, Greater Manchester Police

How artificial intelligence (AI) and 3D programming is being used to create ‘deepfake’ indecent images

Going equipped 10 mins read

Sadly, both indecent images and prohibited images of children are nothing new to investigators. Over the past few years, the online world and technology has continued to grow and develop. But with that, the very worst in society have evolved their offending behaviour in new and terrifying ways.

Issues such as ‘deepfakes’ have been covered extensively in popular culture. But now, with the expansion of readily accessible 3D programmes and artificial intelligence (AI), offenders are expanding their horizons even further. At Greater Manchester Police (GMP), we recently saw this with the case of Hugh Nelson, which this article will delve into in more detail.

Investigations involving AI programmes in the child sexual abuse space are still the outlier compared with the ‘traditional’ indecent images that are typically found. However, we are starting to uncover a shift in criminal behaviour. AI, or computer programmes, are being used more and more to create new material. In research commissioned by the Internet Watch Foundation (IWF), they confirmed a 380% rise in AI-generated child sexual abuse – with 245 reports in 2024 compared with 51 in 2023 (IWF, 2025).

Forensic services are already stretched due to the shift towards online offending that started many years ago. AI/child sexual abuse material (CSAM) is proven to be more likely to increase addiction to this type of content. It’s possible therefore, that investigators could become overwhelmed. It is now so much quicker and easier to create than the material we have become used to seeing up to now.

In this investigation, and what will likely be the case in many others to follow, despite the seemingly ‘cartoon’ and unrealistic nature of this content, real victims are behind it. They face an even greater risk of being repeatedly victimised online, or the even more serious issue of being missed entirely, if this space becomes more saturated and difficult to manage.

Background

Hugh Nelson, a now 28-year-old from Bolton, was convicted in August 2024 of several offences relating to the online abuse of children. This followed an investigation by our dedicated Online Child Abuse Investigation team. He had originally come to our attention via the National Crime Agency, which had been conducting a proactive investigation into AI being used in the online child exploitation field. We identified Nelson, whose online persona was ‘SweetDemons’, to be the offender through his financial data, tracing the money his ‘customers’ were paying for his creations.

Nelson was jailed for over 20 years in October 2024, with the charges he pleaded guilty to including the production, distribution and possession of indecent images of children (IIoC).

What made this case particularly unique and deeply horrifying is that Nelson was using a computer programme with an AI face-transformation function within it. This turned normal everyday photographs of real children into indecent child sexual abuse imagery. He was then selling or publishing albums of those images across various chat rooms on the clean web.

The software

Ultimately, coming across new applications happens all the time and can create challenges in gaining forensic evidence. However, it is important that the digital forensic investigator uses their existing skills, knowledge and investigative mindset to locate the evidence and display this appropriately. This ensures that the bigger picture of the investigation is made clear.

In this particular case, it was the first time a GMP investigation had discovered 3D modelling software of any nature being used in such a way. Those handling the case had no hands-on experience in dealing with this type of content and the new types of forensic artefacts they would be looking for.

The software package provides a wide range of 3D assets for users to create scenes and characters. Typically, it is used for genuine purposes such as video game creation and animations. The software comes with tools that allow users to manipulate their models in several ways, including changing their posture, expressions, putting them in poses and adding animations.

In the case of Hugh Nelson, he was looking to create a model that appeared to resemble the commissioned victim as closely as possible.

Nelson's 'customers' were predominantly the fathers, uncles, family friends or neighbours of the victims, and lived all across the globe. They would send him regular photos such as holiday or school photographs to use as the basis for the models. Before starting this venture, he did not have any graphic design or illustration experience. It shows how quickly and easily someone with no creative background is now able to create this kind of content. The emergence of AI and computer software is taking away the need to have a particular skill.

The developers at the software company assisted the investigation by signposting us to what we should be looking for in the code to determine whether an AI face transfer plugin had been used. This in turn helped us to figure out which creations originated from photographs of real children, even if we couldn't find the original image.

This investigation was very much a case of learning on the job. Investigating the software live on the platform and working with the developers was absolutely key to ensuring that we were on the right track. It is something that would be recommended should other investigators find themselves in the same position with this platform or others of a similar nature.

What will also be useful to investigators looking particularly at AI cases is grading software plugins. At GMP, we have plugins which look at Exif data – markers within a file – that allow us to find specific things in the data and image.

We know there are limitations to this method. You will not always be analysing the original version of an image so the data attached is not the data you are looking for. However, these plugins can be useful when the original data is recovered from a suspect's device.

In this case, however, the main data of importance was the chat data, through which we could derive the start point for Nelson's creations. Without this, the most important part of this investigation, the safeguarding of the real children impacted, could not have been done.

Legislation and grading

When we began investigating this case, legislation already existed to say that images which are created by AI can be graded as photographs (Categories A to C). However, guidance from the Crown Prosecution Service (CPS) contains the following caveat.

‘High-quality computer-generated indecent images/AI-generated images can pass as photographs and it is possible to prosecute on the basis of quality computer-generated images as pseudo-photographs.’

The images created by Hugh Nelson didn’t reach this criteria. They were cartoon-looking rather than images designed to look realistic and would have typically fallen into the prohibited images category.

We felt that to charge him with prohibited images offences only would have been a disservice to the victims. This is especially the case when you consider the extremity of the content and the fact that the material had a real source image of a victim at the centre.

Given this, when looking at **section 7 of the Protection of Children Act 1978**, specifically with regard to ‘tracing’ and how these can be classified as photographs:

(4A) References to a photograph also include

- a tracing or other image, whether made by electronic or other means (of whatever nature)
  - which is not itself a photograph or pseudo-photograph, but
  - which is derived from the whole or part of a photograph or pseudo-photograph (or a combination of either or both)’.

This applies to offences under **section 160 of the Criminal Justice Act 1988**, meaning indecent photographs of children.

During discussions with the CPS, it was agreed that criteria would be used to determine how an image is graded.

We were able to satisfy the following.

- Where we have good provenance of images (continuity of real image to final product) we should proceed with indecent photographs.
- Where there is a digital footprint or any related chat that could show that the final product was traced from another image (that we don't have) we should proceed with indecent photographs.
- Remaining images will need to be checked to satisfy that they look like photographs rather than purely computer-generated images (Do not fit into the above criteria). The former should be graded as IIoC and the latter as prohibited. Therefore, cartoon-style images with no provenance linking them to a real child, or a photograph, are categorised as prohibited images.

From our investigation, we could identify 119 images we could classify as indecent rather than prohibited in terms of distribution from eight chats he was in, and 1,807 images he had made. In total 1,391 other images located on his devices still had to be classified as prohibited images as they didn't have a traceable source photograph they had derived from.

Summary

This was a landmark ruling not just for GMP but for forces nationally, as this is now stated case law. We can now say that computer-generated images, even non-realistic and cartoon-style images, which derive from real photographs of children can be charged as indecent images of children, rather than prohibited images of children.

This is significant for the grading of indecent images of children and will ultimately change the results of grading going forwards when applied against R v Nelson.

It is clear that the law still has some catching up to do when it comes to the AI space. But it is expected that some AI child sexual abuse offending – but not all – will be covered in the upcoming Crime and Policing Bill. We must continually expand our horizons to ensure we can keep track of new platforms, technology and the ways offenders continue to evolve. This is particularly the case for digital forensic investigators, whose decision-making ultimately has some of the biggest impact on these cases.

We have helped to set up a national pilot to test AI detection tools. A variety of tools in development have already been tested on existing, finalised cases, to see if they could identify whether content is AI generated or real. The results of these tests are mixed and there is still much to do to bring the

evolution of these tools in line with the escalation of offending behaviour. But this could be an area which makes a positive difference on cases in the future.

While this work continues, the art of visual interpretation is still key to ensuring positive outcomes. Deepening understanding of issues such as shadow placement and alignment in photography, for example, may assist investigators in identifying where AI has been used.

Overall, roughly 98% of AI-generated child sexual abuse material is of girls (IWF, 2025). If we can successfully tackle the problem and those involved, we could go a long way towards addressing the wider issue of violence against women and girls.

- This article was peer reviewed by Dylan Alldridge, Head of Innovation, Office of the Police Chief Scientific Advisor

References

- Internet Watch Foundation. (2025). **New AI child sexual abuse laws announced following IWF campaign**
- Internet Watch Foundation. (2025). **Global leaders and AI developers can act now to prioritise child safety**

Download Going equipped

This article is from the 10th issue of Going equipped.

- **Going equipped: Issue 10 Spring/Summer 2025 (pdf) 2.78 MB**

Tags

Going equipped