# Experts warn AI deepfakes threaten children's safety with just 20 online photos



Cybersecurity experts have issued urgent warnings regarding the alarming ease with which predators can exploit online images of children. It has been revealed that as few as 20 images are sufficient for sophisticated AI tools to create deepfake videos, raising serious concerns about the safety of sharing family photos on social media. Professor Carsten Maple, a prominent figure in the field from the University of Warwick and the Alan Turing Institute, emphasised the implications of this technology, which include identity theft, blackmail, and various forms of online exploitation.

The research, commissioned by the privacy-focused tech firm Proton, highlighted a troubling trend among UK parents, revealing that they upload an average of 63 photos each month, a significant portion of which feature their children. Alarmingly, one in five parents shares family images multiple times a week, often unaware of the risks involved. This has resulted in many children developing a digital footprint from birth, long before they can comprehend the implications of their online presence or offer consent for sharing their images.

Beyond criminal exploitation, there are additional concerns related to how major tech companies utilise these images. Professor Maple pointed out a particularly controversial policy change by Instagram, which now allows the platform to incorporate user photos to train its AI systems for various purposes. He described this move as "deeply concerning," suggesting that tech companies often harvest data to build advertising profiles and analyse user behaviours without full transparency regarding what information is being collected.

Moreover, the study revealed that over half of parents regularly back up their family photos to cloud storage, with the average parent maintaining around 185 images of their child online at any given time. However, it came to light that nearly half of parents were unaware that tech firms had access to these images and could use them for purposes beyond simple storage. Many mistakenly assumed that only basic metadata, such as timestamps and geolocation, was being shared, while a notable 11% were completely unaware of the extent of information gathered.

Experts warn that this oversharing could expose children to life-altering risks including fraud, grooming, and deepfake abuse. The permanence of digital records means that once images circulate online, they can be near impossible to delete, potentially paving the way for more sinister forms of exploitation. Professor Maple noted the gravity of the situation, stating that “we are building digital profiles of children without their consent,” underscoring the urgent need for enhanced protective measures as threats increase both in number and sophistication.

Despite growing parental anxiety—32% of parents express constant worry about potential hacking of their phones or cloud accounts—many remain unaware of the true vulnerabilities their images pose. Although 72% state that photo privacy is important, a staggering 94% believe tech companies should disclose more about their data usage practices. While some parents have implemented additional security measures, such as using Face ID or restricting app downloads, experts caution that these steps may not be sufficient to guard against the rapidly evolving landscape of AI technology and data breaches.

The reality is stark: as technology evolves, so too do the tactics employed by cybercriminals. It has become increasingly essential for parents to have open discussions with their children about these risks, equipping them with the knowledge to navigate the digital world safely. Heightened awareness and proactive strategies will play a crucial role in protecting the next generation from the unique dangers presented by the intersection of AI and social media.

## Reference Map:

* Paragraph 1 – [[1]](https://www.dailymail.co.uk/news/article-14765875/Cyber-security-experts-number-images-predators-need-make-deepfakes.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://www.mcafee.com/blogs/family-safety/why-sharing-your-kids-pics-online-is-not-a-good-idea/)
* Paragraph 2 – [[1]](https://www.dailymail.co.uk/news/article-14765875/Cyber-security-experts-number-images-predators-need-make-deepfakes.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[4]](https://www.openprivilege.com/lifestyle/technology/the-hidden-dangers-of-sharing-your-childrens-photos-online-67387fe708a6b5e9feceaace)
* Paragraph 3 – [[1]](https://www.dailymail.co.uk/news/article-14765875/Cyber-security-experts-number-images-predators-need-make-deepfakes.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[6]](https://kpmg.com/us/en/articles/2024/deepfakes-real-threat.html)
* Paragraph 4 – [[5]](https://edition.cnn.com/2025/01/02/health/deepfakes-social-media-wellness/index.html), [[3]](https://www.bitdefender.com/en-gb/blog/hotforsecurity/how-to-talk-ai-and-deepfakes-with-children)
* Paragraph 5 – [[1]](https://www.dailymail.co.uk/news/article-14765875/Cyber-security-experts-number-images-predators-need-make-deepfakes.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[6]](https://kpmg.com/us/en/articles/2024/deepfakes-real-threat.html)
* Paragraph 6 – [[1]](https://www.dailymail.co.uk/news/article-14765875/Cyber-security-experts-number-images-predators-need-make-deepfakes.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://www.mcafee.com/blogs/family-safety/why-sharing-your-kids-pics-online-is-not-a-good-idea/), [[4]](https://www.openprivilege.com/lifestyle/technology/the-hidden-dangers-of-sharing-your-childrens-photos-online-67387fe708a6b5e9feceaace)
* Paragraph 7 – [[1]](https://www.dailymail.co.uk/news/article-14765875/Cyber-security-experts-number-images-predators-need-make-deepfakes.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[3]](https://www.bitdefender.com/en-gb/blog/hotforsecurity/how-to-talk-ai-and-deepfakes-with-children), [[5]](https://edition.cnn.com/2025/01/02/health/deepfakes-social-media-wellness/index.html)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.dailymail.co.uk/news/article-14765875/Cyber-security-experts-number-images-predators-need-make-deepfakes.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.mcafee.com/blogs/family-safety/why-sharing-your-kids-pics-online-is-not-a-good-idea/> - McAfee's blog discusses the risks associated with sharing children's photos online, highlighting that cybercriminals can use these images to steal identities. The article explains that even seemingly innocent photos can reveal personal information, making children vulnerable to identity theft. It also addresses the issue of deepfakes, noting that AI technology can manipulate images to create explicit content, leading to potential exploitation. The blog advises parents to be cautious about the photos they share and to consider the long-term implications of their children's digital footprints.
3. <https://www.bitdefender.com/en-gb/blog/hotforsecurity/how-to-talk-ai-and-deepfakes-with-children> - Bitdefender's article provides guidance for parents on educating their children about the dangers of AI-generated deepfakes. It outlines specific risks, including identity theft, cyberbullying, misinformation, privacy violations, and emotional harm. The piece offers practical advice, such as limiting photo sharing to private groups, avoiding deepfake apps, and establishing safety plans. It also emphasizes the importance of open communication and using parental control tools to monitor online activity, aiming to equip children with the knowledge to navigate the digital world safely.
4. <https://www.openprivilege.com/lifestyle/technology/the-hidden-dangers-of-sharing-your-childrens-photos-online-67387fe708a6b5e9feceaace> - Open Privilege's article explores the concept of 'sharenting' and the potential dangers of sharing children's photos online. It discusses how parents inadvertently create a digital footprint for their children without consent, which can have lasting implications. The piece also highlights the risks of compromising online privacy and safety, noting that seemingly innocent photos can reveal personal information, making children vulnerable to online predators. The article urges parents to consider the long-term consequences before posting their children's images on social media.
5. <https://edition.cnn.com/2025/01/02/health/deepfakes-social-media-wellness/index.html> - CNN's article examines the impact of deepfakes on children, emphasizing the psychological and social harm they can cause. It highlights that deepfakes can lead to significant distress, anxiety, depression, and a sense of humiliation. The piece also discusses the challenges parents face in educating their children about this issue, noting that many students and teachers are aware of deepfakes associated with their schools. The article underscores the importance of open communication and teaching children to recognize and respond to deepfake threats.
6. <https://kpmg.com/us/en/articles/2024/deepfakes-real-threat.html> - KPMG's article delves into the challenges posed by deepfakes, particularly in the realm of cybersecurity. It discusses the difficulty in identifying deepfakes, noting that generative adversarial networks (GANs) can create media that is virtually undetectable. The piece also highlights the role of generative AI in facilitating the creation of deepfakes, making it accessible to a broader range of individuals. The article emphasizes the need for robust cybersecurity measures to address the threats posed by deepfakes.
7. <https://www.psychologytoday.com/us/blog/positively-media/202410/teens-and-deepfake-nudes-digital-bullying-s-new-frontier> - Psychology Today's article addresses the issue of deepfake nudes among teenagers, highlighting the role of AI in creating hyper-realistic manipulated images. It discusses how these images are often used as a form of bullying or harassment, leading to significant emotional harm for the victims. The piece emphasizes the need for parents to understand the complexities of deepfake nudes to help protect their teens, advocating for open, nonjudgmental family communication on online risks to foster safety and awareness.