Insights Paper:
Understanding nudify apps

August 2025

In only a few years, Artificial Intelligence (AI) has evolved from merely interpreting data to generating entirely new content. Our world has already adapted to evolve alongside it, changing language, systems and workflows to accommodate for rapid technological advancements. Entire industries such as medicine, education, and the sciences have seen capabilities expand dramatically.

Despite these positive applications, the advent of generative AI (GenAI) has also exponentially increased the capabilities of offenders in proliferating child sexual exploitation. In the past two years, this threat has taken many forms - and the child protection sector has been acutely aware of the growing dangers. ICMEC Australia's SaferAI for Children Coalition has long recognised that this heightened offender capability demands a critical, coordinated response to the threats emerging technology pose to children.

Less than a year after the SaferAI for Children Coalition's 2024 Discussion Paper exposed the risks to Australian children in the era of AI, the threat landscape has already evolved — and demands immediate attention.

ICMEC AUSTRALIA

SaferAI for Children Coalition

Artificial Intelligence and Child Protection:

A Collaborative Approach to a Safer Future

Discussion Paper

Led by ICMEC Australia, the **SaferAI for Children Coalition** is a collaborative body of Australian law enforcement, not-for-profit organisations, academics, AI experts, and other public sector stakeholders, all dedicated to creating better outcomes for children in the age of AI.

ISBN 978-1-7638997-0-4

One particularly alarming development in the past year is the emergence of "nudify apps". Previously, manipulating images of children required hours of manual editing. Now, nudify apps can transform innocent images or videos of children into child sexual abuse material (CSAM) within seconds, on demand. Access to nudification technology grows, it is fuelling the large-scale, industrialisation of image-based abuse and creates new opportunities for peer-on-peer abuse.

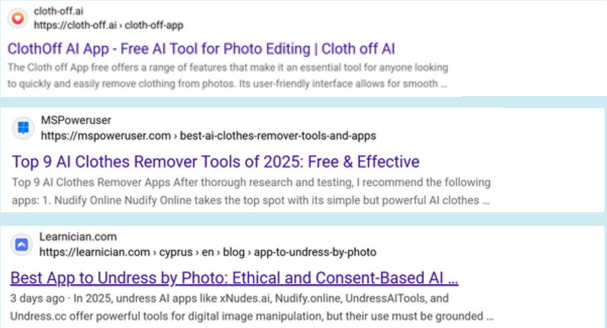
What is a 'nudify app'?

Nudify apps use AI to automatically create sexualised or 'nudified' images or video of real people. In many cases, this involves taking an innocent image of a person, and altering it to depict them without clothing. These tools are often linked to 'deepfake' technology. Whilst many nudify apps offer limited free features, most function using a pay-per-image system, with premium options enabling users to customise content to their preferences - including by age, ethnicity, and other disturbing preferences.

Recent advancements in AI mean that nudify apps can now produce hyper-realistic content which most viewers would find convincingly real. Law enforcement internationally are raising the alarm, warning that AI-generated abuse material is now nearly indistinguishable from real content.

Public awareness of nudify apps remains low, so conversations about dangers are sadly rare. Alarmingly, the top search results for 'nudify apps' on popular search engines still frame them positively, effectively promoting their use rather than cautioning against the harm they cause.

Search results at a glance



cloth-off.ai
https://cloth-off.ai › cloth-off-app
ClothOff AI App - Free AI Tool for Photo Editing | Cloth off AI
The Cloth off App free offers a range of features that make it an essential tool for anyone looking to quickly and easily remove clothing from photos. Its user-friendly interface allows for smooth ...

MSPoweruser
https://mspoweruser.com › best-ai-clothes-remover-tools-and-apps
Top 9 AI Clothes Remover Tools of 2025: Free & Effective
Top 9 AI Clothes Remover Apps After thorough research and testing, I recommend the following apps: 1. Nudify Online Nudify Online takes the top spot with its simple but powerful AI clothes ...

Learnician.com
https://learnician.com › cyprus › en › blog › app-to-undress-by-photo
Best App to Undress by Photo: Ethical and Consent-Based AI ...
3 days ago · In 2025, undress AI apps like xNudes.ai, Nudify.online, UndressAITools, and Undress.cc offer powerful tools for digital image manipulation, but their use must be grounded ...

Concerningly, in an analysis of the top 20 search results when searching the phrase 'nudify apps' in a popular search engine, ICMEC Australia found that 70% of results encouraged the use of nudify apps using language like 'free', 'ethical' and 'best' in their headlines. (August 2025)

From niche to mainstream

Nudify apps rose to prominence in 2023, when Graphika reported that in just one-month, 34 providers attracted over 24 million unique users. Since then, nudify apps have become alarmingly accessible, with thousands available in app stores and online – all with different names, but the same purpose.

Nudify apps are not only widespread – they are lucrative. Graphika (2023) describes them as a "scaled and monetised online business", often promoted through mainstream social media platforms. Many nudify apps operate on a pay-per-image basis, with optional paid add-ons that give users even greater control over the final product.

The boom in nudify apps has fuelled a sharp increase in image-based abuse and sextortion. Celebrities like Taylor Swift, Scarlett Johansson, and Kristen Bell have already been public victims of image-based or deepfake abuse – a phenomenon which has gained the attention of media globally.

In schools, the ever-increasing accessibility of nudify apps has led to a troubling rise in peer-on-peer deepfake abuse, providing easy material for sexual extortion and contributing to what law enforcement describes as a dramatic increase in AI-generated CSAM.

The tech that makes it possible

Nudify apps are not just another harmful online trend – they represent a profound and rapidly escalating threat. The technology behind these apps is key to understanding why they are so dangerous, and so difficult to regulate or shut down.

The Models

Where AI models remain 'in-house' – that is, controlled or monitored by a company like OpenAI – their owners are able to maintain control over their algorithms and enforce safeguards, often called guardrails. These may detect or deny inappropriate or illegal requests. While not foolproof, guardrails provide some level of protection for both users and the broader community.

The largest risks come from open-source models – readily available AI systems that form the backbone of most nudify apps. Once downloaded, these models sit entirely in the control of the user, where safeguards can be removed or manipulated in minutes. The base models themselves are not inherently harmful, but they can be modified using low-rank adaptations (LoRAs) – small, add-on variables that can adjust the model's capabilities for a more targeted use-case. For nudify apps, LoRAs can give users the ability to generate sexualised content and adjust for disturbing variables like age, body composition, ethnicity, position or artistic style.

The building blocks of abuse

Once created, LoRAs can be easily packaged, shared, and attached to existing base models. Online communities and online libraries dedicated to sharing LoRAs have multiplied, making it increasingly simple to create, and re-create, nudify apps. The sharing of LoRAs – even those facilitating the creation of CSAM – is not currently prohibited under Australian law.

The Datasets

A further danger lies in the data that nudify apps are trained on. To create an effective AI algorithm, it needs to be trained with as much real-world data as possible. The more examples of a 'desired' output – such as sexualised content – the more realistic results will be. For nudify apps producing CSAM, this means training on vast collections of real abuse material.

When private photos become training data

In 2024, Human Rights Watch analysed 0.0001% of the data in LAION-5B - a dataset of over 5.8 billion image-caption pairs scraped from across the internet and used to train well-known generative AI image models. Even in this small sample, the organisation found 190 photos of Australian children. Many were accompanied identifying details including the child's name, the photo's location, and a URL to the original source.

Some of these images had originally been private - posted to personal social media accounts, even those with strict privacy settings. The sheer scale of data scraped to train AI models is almost unfathomable - particularly how easily personal images can end up in these datasets. This same approach underpins the technology behind many nudify apps, meaning that, in theory, anyone's photo could be used to train tools capable of creating sexualised content.

Harm in the real world

Whilst the images nudify apps produce are manipulated and often dismissed as 'fake', they pose a significant and urgent real-world risk to the safety of children. The most obvious danger lies in their potential to create non-consensual intimate imagery - including content that meets the legal definition of child sexual abuse material (CSAM). But the harms extend far beyond the images themselves. The lifecycle of harm spans the development and training of the AI models, how material is weaponised after creation and the long-term risk of offenders becoming desensitised through repeated exposure, lowering inhibitions and normalising abuse.

The claim that 'no real child is harmed' is false: real children's images are scraped to train these tools, meaning exploitation starts the moment those images are taken and reused.

Peer-on-peer abuse

Over the past year, there has been a sharp global rise in reported peer-on-peer image-based abuse, increasingly driven by nudify apps and deepfake technology. In one high profile Melbourne case, investigators found that 50 female students at a single high school had been the victims of non-consensual sexually explicit deepfakes, created by a peer. The eSafety Commissioner, has called this an urgent crisis in school communities.

Anyone can make a report about inappropriate behaviour towards children online via the Australian Centre to Counter Child Exploitation's website: https://www.accce.gov.au/report

Please visit ICMEC Australia's website to access a list of other helplines and support services: https://icmec.org.au/help-and-reporting/

Sextortion and scaled creation of CSAM

Without sufficient guardrails, many nudify apps are capable of creating sexually explicit deepfakes of children (not just adults) - meaning they have been trained using abuse images of children. This has further enabled the industrialised production and distribution of CSAM. Offenders no longer need to obtain explicit images of their victims to extort them; the threat of releasing a convincing deepfake is often enough to coerce a child into complying with demands.

Normalisation of harm

By making sexualised content easy to create, nudify apps can contribute to desensitisation—making harmful behaviour seem more acceptable. While nudify apps are not the only cause, easy access and repeated exposure to CSAM has been linked to some people seeking more extreme content. This is especially concerning given the overall increase in AI-generated child abuse material, as online offending can often lead to contact offending.

Closing the gaps

The risks and harms posed by nudify apps require urgent action to close gaps in Australia's regulatory framework, raise awareness across communities, equip institutions to respond, and ensure the private sector plays its role in preventing harms.

Where the law stands

The training or tuning of AI algorithms for the production of CSAM is being recognised as an emerging issue worldwide. The European Union recently moved to criminalise AI-generated CSAM, as well as the development, possession and distribution of AI systems capable of producing such material. This forms part of a broader global movement to criminalise the production and distribution of AI-generated CSAM, and the technologies that enable it.

In Australia, the legal picture is fragmented. Consensual nudification - where an adult agrees to have their image altered - is not a criminal offence, meaning nudify apps themselves are not banned outright. However, sharing sexualised images of a person without their consent is illegal in all states and territories. At the federal level, there is currently no law against developing or possessing tools that can be used to generate CSAM. It is also not illegal to share information on how to adapt existing, lawful technologies so they can be used to produced CSAM.

Steps towards a safer future

To address this exact gap, Member for Curtin, Kate Chaney MP, introduced a Private Member's Bill to Federal Parliament in July 2025. The 'Criminal Code Amendment (Using Technology to Generate Child Abuse Material) Bill 2025' would make it a criminal offence to train, possess, or share technologies such as generative AI models and LoRAs designed to generate CSAM. ICMEC Australia is proud to have collaborated with Ms Chaney on this Bill.

Legislative change is essential, but it can't exist in a silo. Addressing all of the risks to children of nudify apps requires a whole-of-system response that combines law reform with prevention, education, and technology-driven safeguards.

Prevention through awareness

Community-wide education is one of the most effective ways to prevent harm from nudify apps - with schools being a critical starting point. Education programs should cover:

- The legal limits on using nudify apps;
- The real-world consequences for victims;
- How quickly and irreversibly harm can spread online; and
- The role of peers in prevention and reporting.

Why stopping harms is so hard

Private sector action, particularly from app stores, remains one of the few immediate ways to combat the harms of nudify apps. While some app stores have already removed certain nudify apps from their platforms once flagged, keeping them off is an ongoing challenge. Almost instantly, as one app is taken down, another can appear - using the same algorithm under a new name and branding.

Tracking the use of these tools is also difficult. Whilst purchases can generally be traced through financial transactions, these platforms often use cryptocurrencies or other untraceable payment methods. Encryption and the absence of sign-in requirements further protect user anonymity, creating significant barriers for law enforcement and regulators.

Act now to reduce harm

Nudify apps have moved from niche tools to an industrialised form of abuse - driving peer-on-peer exploitation, sextortion, and the creation of AI-generated CSAM. Closing legal loopholes, boosting education, and investing in stronger preventative tech tools are urgent steps to protect children from this escalating harm.

About ICMEC Australia's Insights Papers:

ICMEC Australia's Insights Papers provide clear, accessible analysis of emerging risks at the intersection of child protection and technology. Produced with input from experts, the series offers timely insights for government, industry, and the community to inform action as new threats arise.

✉ prevention@icmec.org.au   www.icmec.org.au   in ICMEC Australia

Written by ICMEC Australia authors: C. Holley, M. Jago, Dr J. Dalins