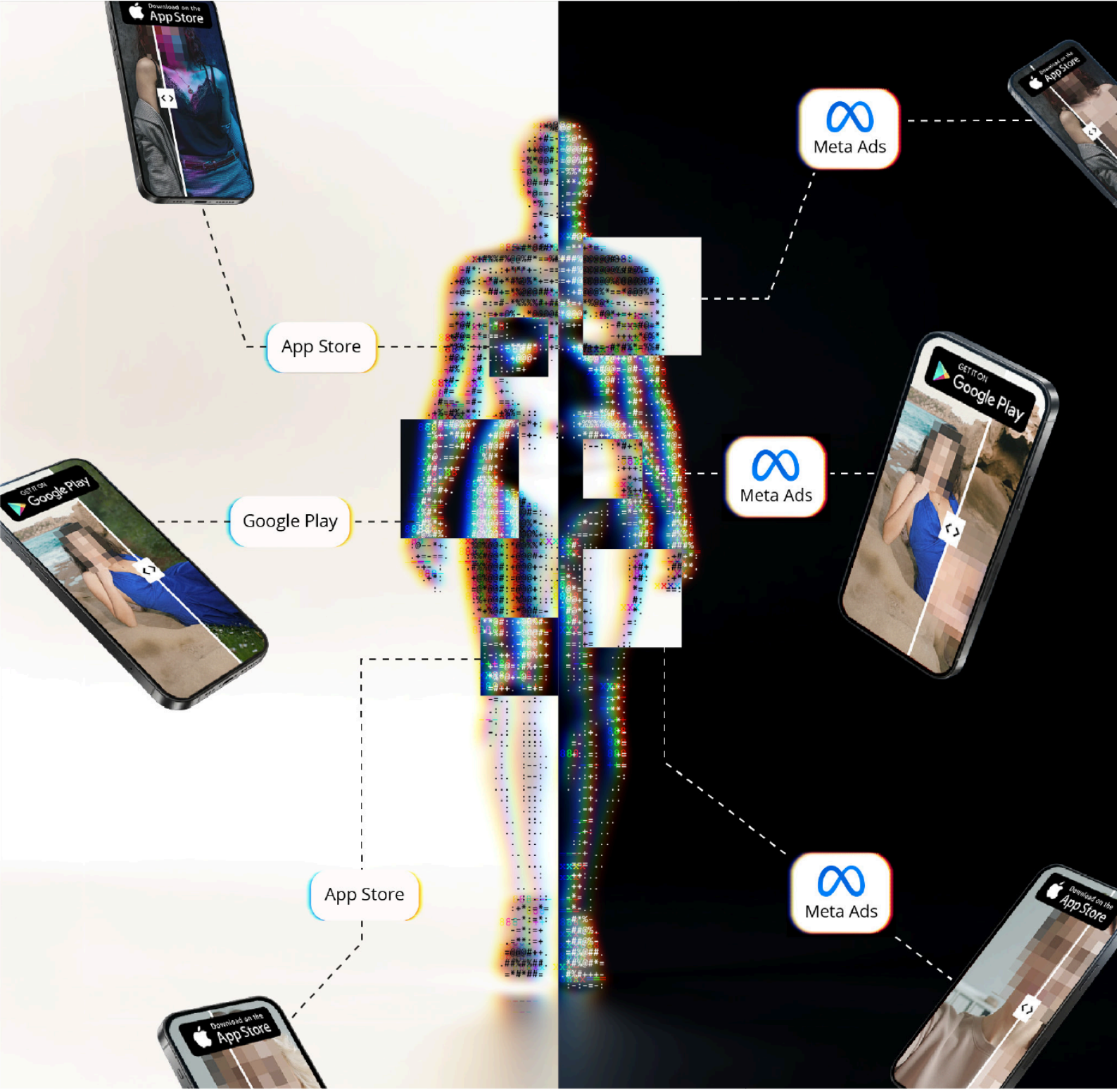


ADVERTISED BY DESIGN

Nudify Apps on Meta, Google Play and the App Store

AI FORENSICS

Credits:

Research & report: Dr. Paul Bouchaud
Cover: Nele Schwesig

All other content © AI Forensics 2026 | http://aiforensics.org

Email: info@aiforensics.org
Social media: LinkedIn | Bluesky

Disclaimer:

This report contains screenshots of (blurred) sexually explicit content. *The report presents analyses drawn from our own research and publicly available data as of September 2026 and offers a non-exhaustive overview of a specific research period. Manual or automated errors may have occurred. No legal conclusions are drawn from this work, and nothing herein should be read as a legal accusation.*

Executive summary

As the EU moves toward banning "nudifier" apps[1], we explore the technical infrastructure and distribution of a network that has published hundreds of such apps, promoted by tens of thousands of ads on Meta.

- **A particular danger for women and children.** A nudifier app creates images, videos, and audio depicting an identifiable person's intimate parts, or sexually explicit activities, without their consent.
- **A single operation is behind hundreds of seemingly unrelated nudifier apps.** We identified over **444 applications,** typically published on Google Play and Apple's App Store by seemingly different developers.
- **Since January 1, 2026, over 84k ads** matching the network pattern, **have been distributed on Meta.** These ads have been paid for under self-declared and plainly fictitious payer names such as "123456". Despite being "reviewed" before publication, the ads are typically illustrated with pornographic content, which violates Meta's policy.
- **Cloaking by design.** Analysis of the apps reveals there are two versions: when a user installs it organically, they see a benign hair salon and outfit-change app, while a user arriving from a Meta ad is served an explicit version.
- **Dependence on mainstream AI and cloud infrastructure.** These apps rely on third-party inference providers such as ClothOff's, Tencent's, and Shengshu Technology's models.
- **AI-generated coercion.** Among the ready-made video templates provided by these apps, we found "Bedroom Rape", "Lock Her Up", and "Captive Cum Bag".
- **Continued availability.** As of September 11, 2026, 27 apps remained live on Google Play, and 21 remained live on Apple's App Store.

Table of contents

Executive summary 3
Context 4
Case study 6
Unweaving the web 9

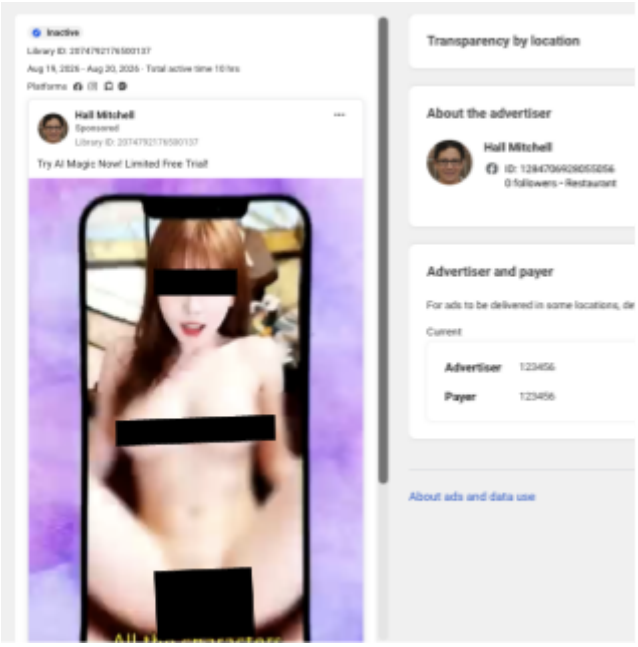
[1] https://www.europarl.europa.eu/news/en/press-room/20260611IPR45207/ai-act-ep-approves-simplification-measures-and-nudifier-app-ban

Context

Under the European Digital Services Act (DSA), very large online platforms must maintain a public repository of the advertisements they distribute in the European Union, including the content of each ad and the name of the person on whose behalf it is presented. On Meta, both the payer and the beneficiary names are **self-declared**. **No systematic identity check is performed**, and in its current formulation, the DSA does not explicitly require it.

Searching the ad library for implausible advertiser names showcases the limits of this permissive design: hundreds of thousands of ads are paid by “1”, “111”, etc. Meta’s “state-of-the-art” integrity systems appear not to have found these remarkable.

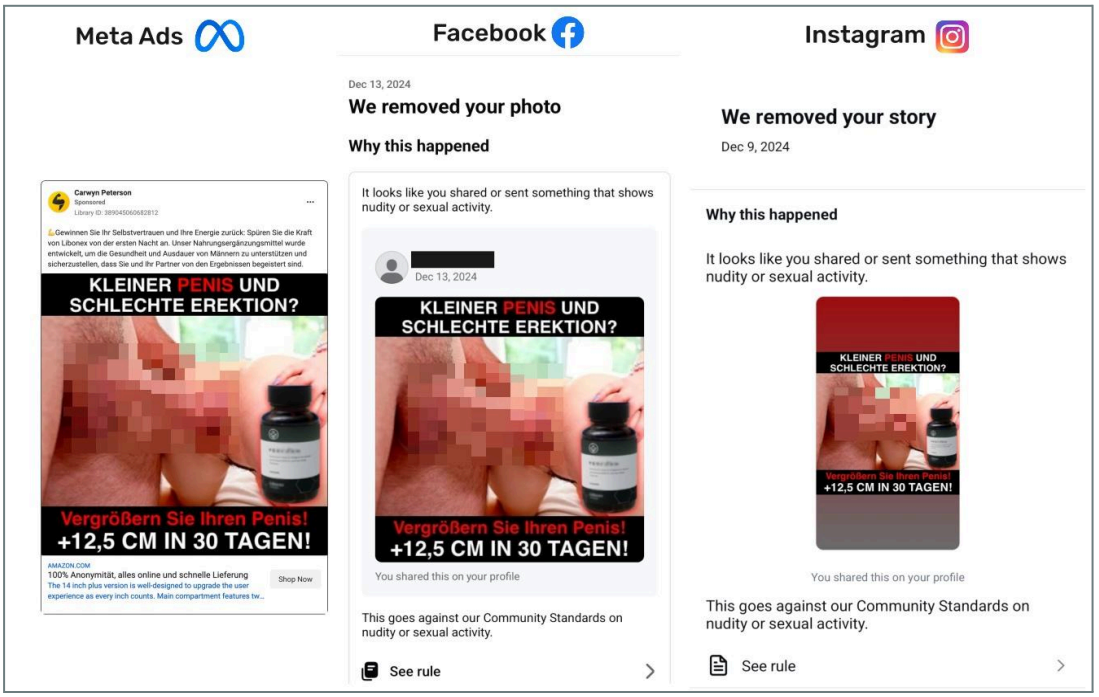
In this report, we focus in particular on a cluster of advertisements promoting **nudifier** apps and paid for by fictitious payers such as “123456”. The ads themselves typically **display pornographic content** (see below) and are created by pages whose profile pictures are AI faces generated by the infamous website thispersondoesnotexist[2], as evidenced by the watermark.



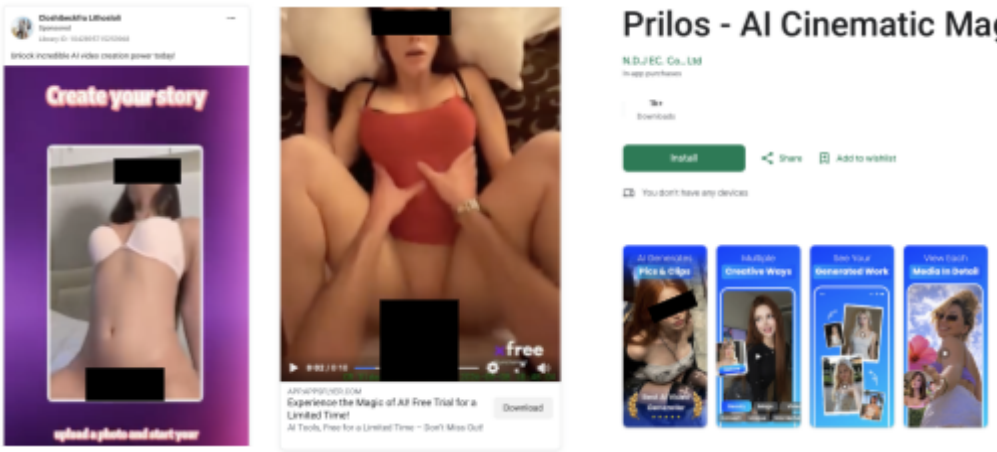


[2] https://thispersondoesnotexist.com/

In January 2025, we documented[3] the presence of thousands of pornographic ads distributed by Meta, while the exact same visual, posted organically on Instagram, was taken down shortly after. The limiting factor appears not to be the technology but the governance.



Similarly, in January 2026, the Tech Transparency Project[4] documented that nudifier apps, distributed through Google Play and Apple's App Store, surfaced in Meta's ads ecosystem. This remains the case in September 2026.

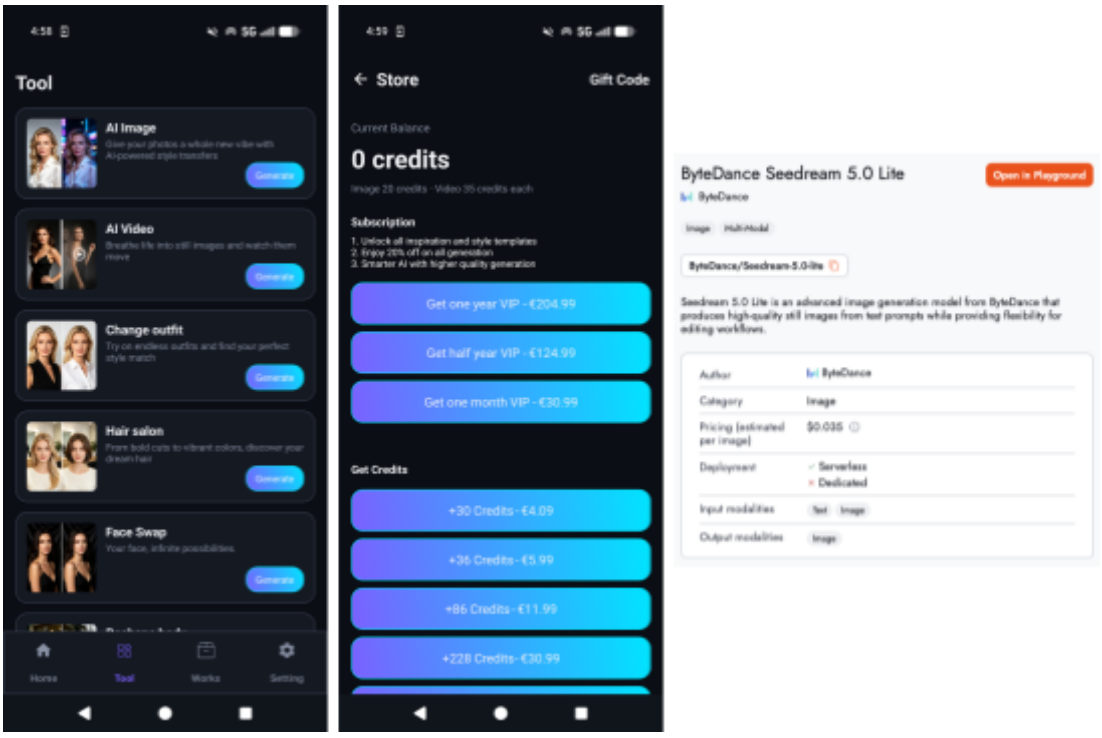


[3] https://aiforensics.org/work/meta-porn-ads
[4]https://www.techtransparencyproject.org/articles/metas-chinese-partner-behind-deluge-of-nudify-ads

Case study

To understand how these applications operate, we downloaded one of them, Prilos, directly from Google Play and examined its code alongside its public facing interface.

Interestingly, at first we only found an AI-powered hair salon and outfit-change app: a user can, after purchasing credits, generate images and videos. To this end, the application uses a third-party service, **Together AI,** which processes the images for a fee. By inspecting the code, we observed that Prilos relies on ByteDance's model Seedream 5.0 Lite for images and Alibaba's HappyHorse 1.1 R2V for video.



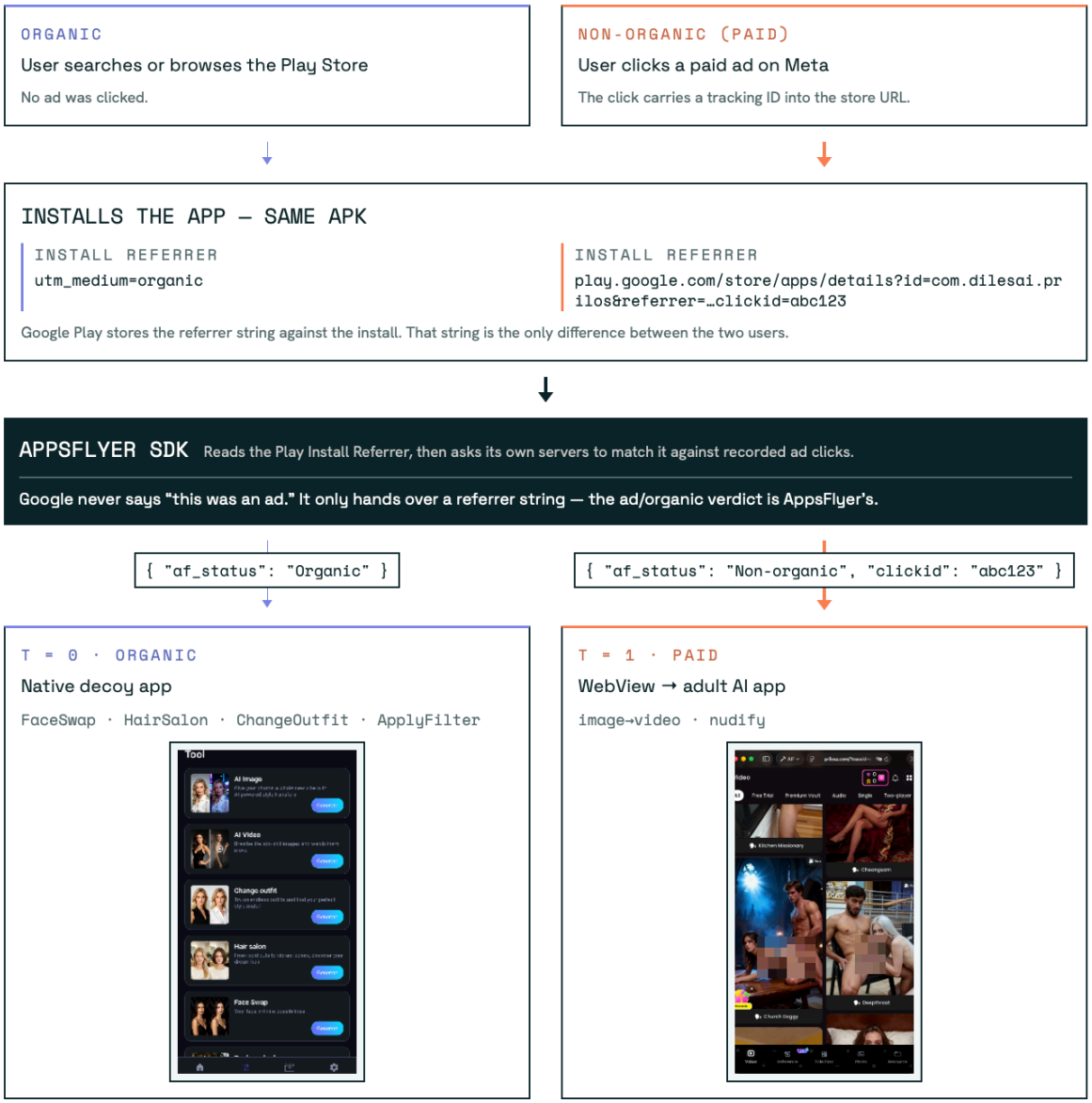
Screenshots, September 10, 2026. Left: Prilos mobile application. Right: Together AI pricing.

The resulting economics are worth stating plainly. An image generated with Seedream 5.0 Lite costs the developer **$0.035** at Together AI's published rate. The user pays between **$2.60 and $3.20** per image, depending on the credit pack purchased (see above): a markup of **roughly x75 to x90 times.**

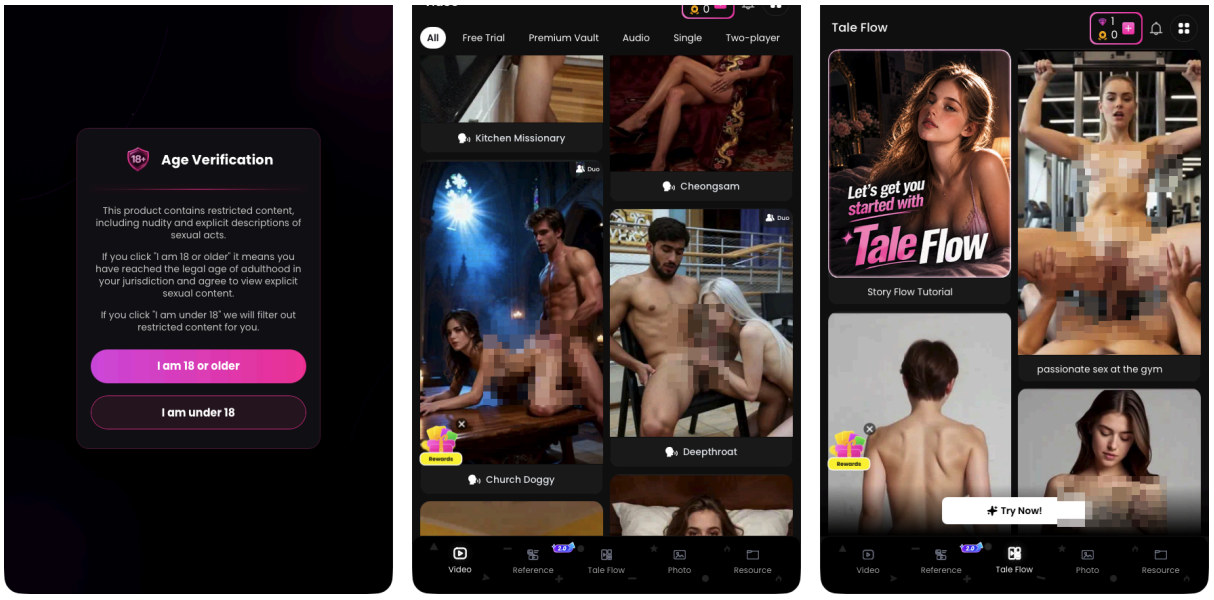
While the underlying Seedream 5.0 Lite model can edit the image to produce some sexualized content, we remain far from the "no restriction" pornographic promises made in the ads.

This is because the application **hides its true purpose**. We downloaded the application ourselves from the app store; we did not click install directly from a Meta ad.

In the code we observe a **"gate"**:

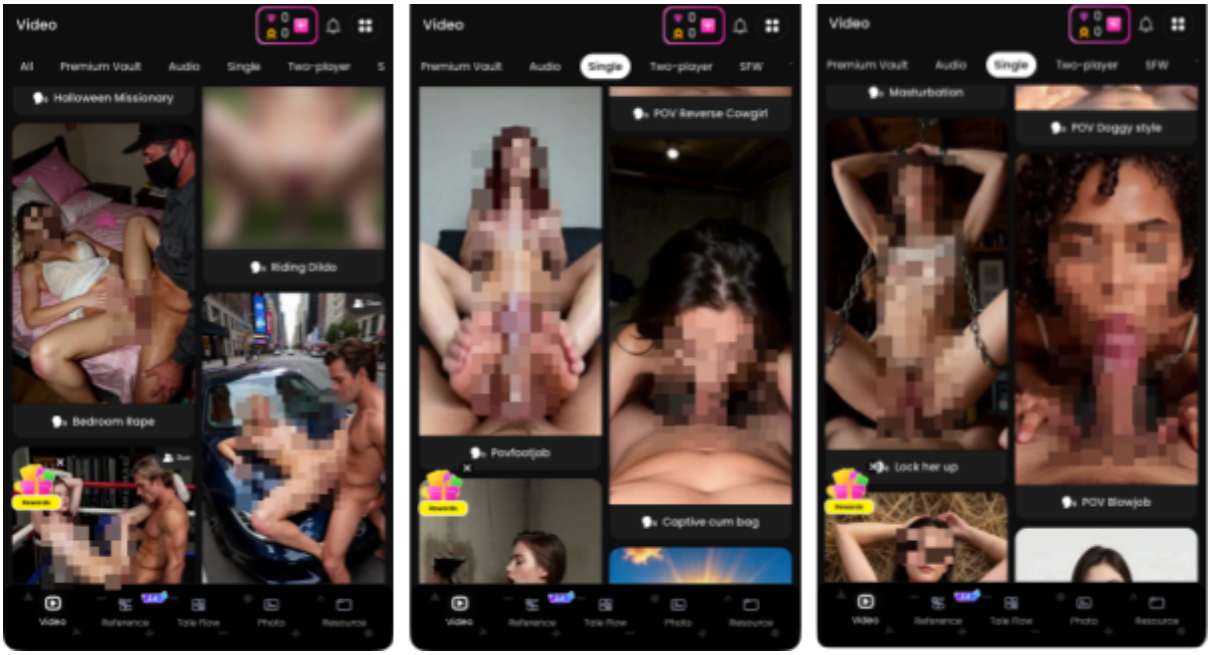


When the user downloads the app "organically", i.e., without going through an ad, the "safe" version shown above appears. When it comes **from a Meta ad**, a completely different **explicit version is displayed** (see below), loading a webpage embedded inside the app.



Screenshots, September 11, 2026. "Ungated" Prilos application.

In this "real", explicit, version of the app, one can generate pornographic, non-consensual content by uploading an arbitrary input image and producing explicit images and videos with over a thousand ready-made templates. Among those, we found **"Bedroom Rape", "Lock Her Up", and "Captive Cum Bag".**



We observed various solutions integrated into the application: the images of the users, as well as the app resources, are hosted on Amazon's AWS CloudFront. The code mentions Tencent's and Shengshu Technology's Vidu AI solution, as well as ClothOff, a provider of nudifier and AI-generated pornographic content.

A user can purchase a "diamond" for $0.11. A typical video costs between 20 and 24 "diamonds", amounting to over $2 per video. We have no breakdown of the inference cost for the app provider.

Unweaving the web

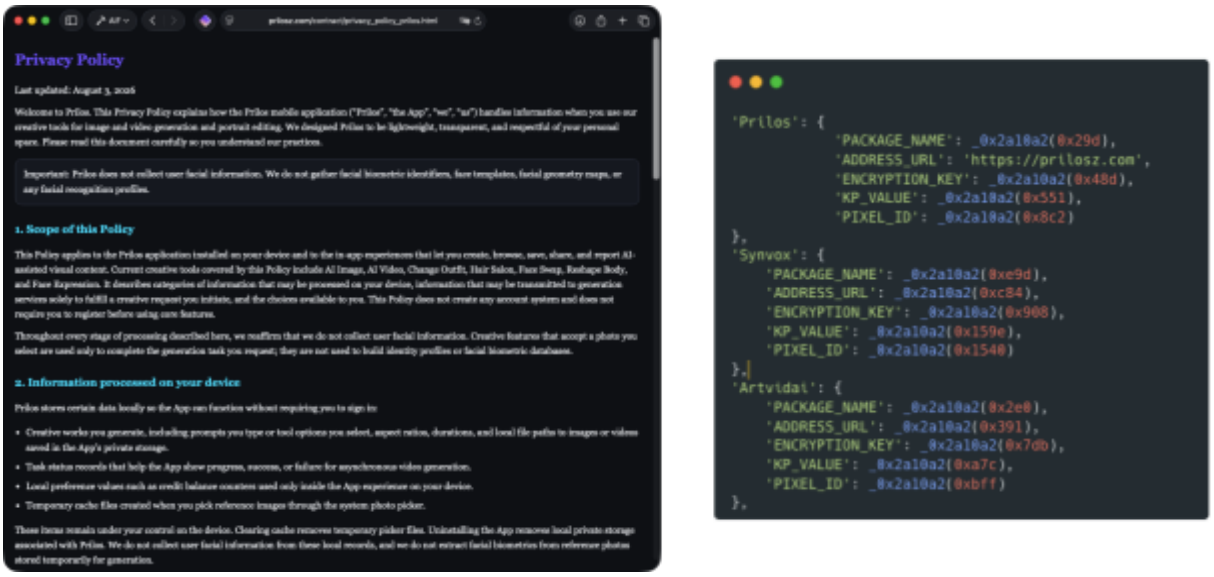
Prilos is one example of an app. In the Meta Ad Library alone, we found **dozens of distinct applications** running near-identical creatives behind the same fictitious payer names.

Importantly, all those apps **have different names** and are run by **different developers** on the store, which makes attribution to a single operation challenging. However, the developers apparently slipped up, allowing us to discover a connection between these apps.

Google Play requires every listing to link a privacy policy hosted on the public web, reachable without installing the app. That single compliance requirement obliges the operator of each nudifier app to run a website.

A visit to the Prilos policy reveals nothing of interest: a boilerplate privacy policy, competently unremarkable. A visit to the homepage reveals even less: a black screen. The page is an empty single-page application that renders nothing at all.

The interesting part is in the background. Behind that blank page sits a JavaScript bundle, and inside it, under a layer of obfuscation, a dictionary keyed by application name.

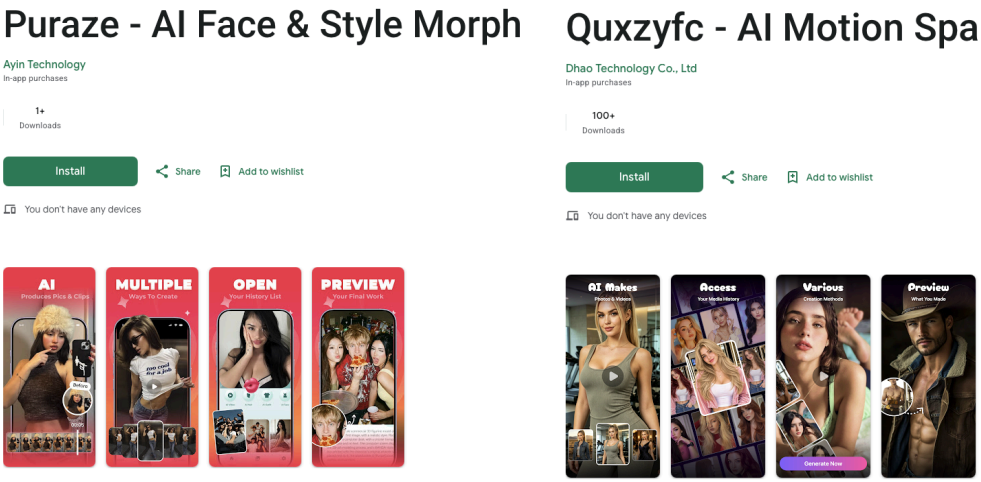


Screenshots, September 11, 2026. Left: Prilos' privacy policy. Right: Snippet of the JS bundle.

Each entry holds an app's package identifier, its domain, its API encryption key, its internal channel code, and its Pixel ID. For instance, alongside "Prilos" sit entries with names such as:

`com.purplesunaze.puraze` and `com.obseamply.quxzyfc`.

These are **Android package identifiers**, and they resolve[5] to recently published applications closely resembling the first.



Screenshots, September 10, 2026. Google Play listing.

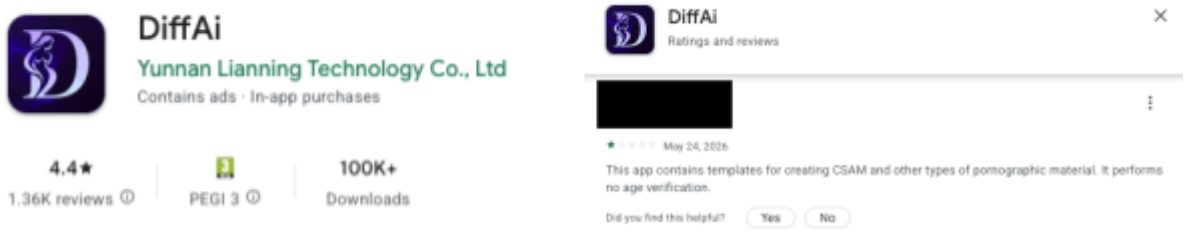
[5] play.google.com/store/apps/details?id=com.obseamply.quxzyfc

This is a build artifact; the operator likely maintains one codebase and one configuration table covering their portfolio, and likely compiles the whole table into every site rather than only the row that site needs. Each app's website therefore publishes the credentials and identifiers of the others.

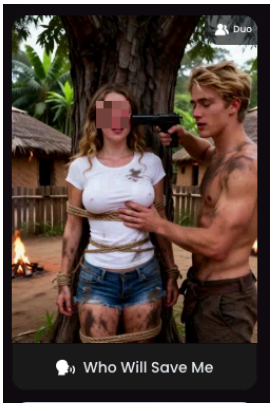
Starting from the applications we had flagged manually, we visited each homepage and extracted its embedded dictionary. Through this process we identified **444 applications**. Of these, 46% carry an ios tag in their bundle identifier and appear intended for Apple's App Store; the remainder appear to target Google Play.

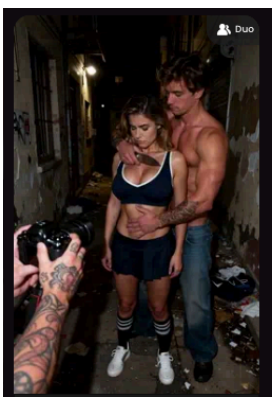
As of September 11, 2026, 27 apps are still live on Google Play (including 20 of which are rated PEGI 3, i.e., deemed suitable for children), collecting over 352k downloads, and 21 are live on Apple's App Store.

While most of the apps are short-lived, DiffAi, created in December 2025, was still accessible in September 2026 and has had over 105k downloads, we note in the review a user complaining for the app facilitating the creation of CSAM.



It also has ready-made templates showcasing coercion:





To understand the dynamics of the operation, we collected the registration date of each domain associated with the apps.

We also searched for ads distributed on Meta, run from January 1, 2026 onward, that contain one of the following expressions:

'Unleash Next-gen AI Magic 🪄', 'Experience stunning AI video capabilities instantly!', 'Unlock incredible AI video creation power today!', 'Don't Miss Out! Try AI Magic Now with a Free Trial!', 'AI Tools, Free for a Limited Time - Don't Miss Out!', 'Turn ordinary moments into unforgettable fantasies with AI Face Swap.', '🔥 Come on baby Unleash the Fun in Your Pics', 'Try AI Magic Now! Limited Free Trial!', 'AI photo to video that actually works'

Putting the two in parallel, we observed a similar rise in activity in spring 2026 between the domain registrations and the over 84k ads distributed on Meta.

