AI FORENSICS

# Technical Report:

## AgeGO Age Verification on Pornographic Platforms

### Background

To protect minors online, the Digital Services Act (DSA), in action since August 2023, requires online platforms accessible to children to implement safeguards that mitigate the risks of exposure to harmful or inappropriate content. In France, these provisions are reinforced by the law SREN[1] of May 2024, which empowers the national Digital Services Coordinator, Arcom, to enforce age verification obligations on pornographic websites accessible in the country.

In October 2024, Arcom adopted technical guidelines[2] on age verification systems for pornographic websites. On 4 August 2025, it issued formal notices[3] to five platforms established in the European Union and accessible in France, urging them to deploy compliant age verification mechanisms.

On August 28th, 2025, six pornographic platforms implemented[4] age verification systems. Among them, tnaflix.com, xvideos.com, and xnxx.com relied on the solution that AgeGO[5] developed.

Users seeking to access explicit material distributed on these sites from France (without resorting to VPNs) must now consent to the proposed age verification measures before proceeding.

**This technical report reviews the age verification system currently implemented, focusing on its alignment with Arcom's technical guidelines and raises potential privacy concerns for users.**

***Disclaimer:*** *This technical report is based on information publicly available as of September 1st, 2025. We acknowledge that manual errors may have occurred, and we do not claim to have carried out an exhaustive analysis of all existing age verification mechanisms. Finally, at no point does this report provide, attempt to provide, or purport to offer an assessment of non-compliance with applicable regulations.*

[1] https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047533100/
[2] https://www.arcom.fr/se-documenter/espace-juridique/textes-juridiques/referentiel-technique-sur-la-verification-de-lage-pour-la-protection-des-mineurs-contre-la-pornographie-en-ligne
[3] https://www.arcom.fr/presse/protection-des-mineurs-en-ligne-larcom-met-en-demeure-cinq-sites-pornographiques-etablis-dans-lue
[4] https://www.arcom.fr/presse/protection-des-mineurs-en-ligne-larcom-constate-la-mise-en-place-de-dispositifs-de-verification-de-lage-par-six-nouveaux-sites-pornographiques
[5] https://www.agego.com/

## AgeGO's system

The age verification process is identical for all three platforms. Upon clicking on blurred sexually explicit material[6], an age verification pop-up appears, as shown in Figure 1.

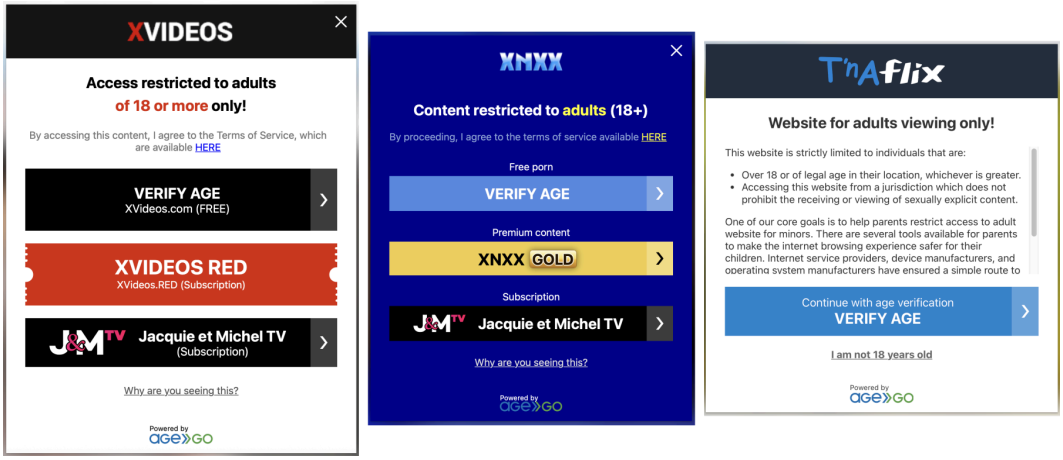


*Figure 1: Age verification pop-up blocking access to sexually explicit content*

Upon clicking on "Verify Age", users are offered three options:

- log in with their AgeGO account,
- undergo a selfie-based facial age estimation (with a fallback option requiring a government-issued ID), or
- log in using the Yoti app, another age verification provider.


*Figure 2: Diagram of AgeGO age verification process*

[6] We observe that the xnxx's subdomain distributing pornographic images and GIFs (multi.xnxx.com), remains accessible, as of September 1st, 2025 without age verification.

Our observations show that, prior to selecting a verification option and prior to consenting AgeGO's Privacy Policy,, the user's browser sends a request to AgeGO's server disclosing:

- **the website currently visited** (encoded as *siteId: 75* for xvideos.com, *73* for xnxx.com, and *153* for tnaflix.com), and
- **the exact video the user is attempting to access** (field *"returnto" e.g. https://www.xnxx.com/video-tdng7c8/perfect_step…*).

In response, AgeGO issues a cookie (`x-ag-sid`) encoding this information. This cookie is subsequently included in all further requests to AgeGO.

As highlighted in Figure 2, both the Selfie and Yoti options are presented to users as "*double anonymity*" solutions.

Arcom's October 2024 technical guidelines define **"*double anonymity*"** as an option in which the age verification provider—in this case, AgeGO—must not know for which service (i.e. which pornographic website) the verification is performed.

In practice, AgeGO receives information about the specific platform requesting verification and the exact videos users attempt to view, even before they select an age verification method, particularly one presented as "*double anonymity*".

When selecting the "selfie facial age estimation" method, users are prompted to accept AgeGO's Terms & Conditions and Privacy Policy (see Figure 3).

As of 1 September 2025, AgeGO states that the video stream captured from the user's device is uploaded directly to a third-party provider. This provider is not named in their Privacy Policy[7] nor in their Terms & Conditions[8]. The only indication provided is that it operates under the EU–U.S. Data Privacy Framework.

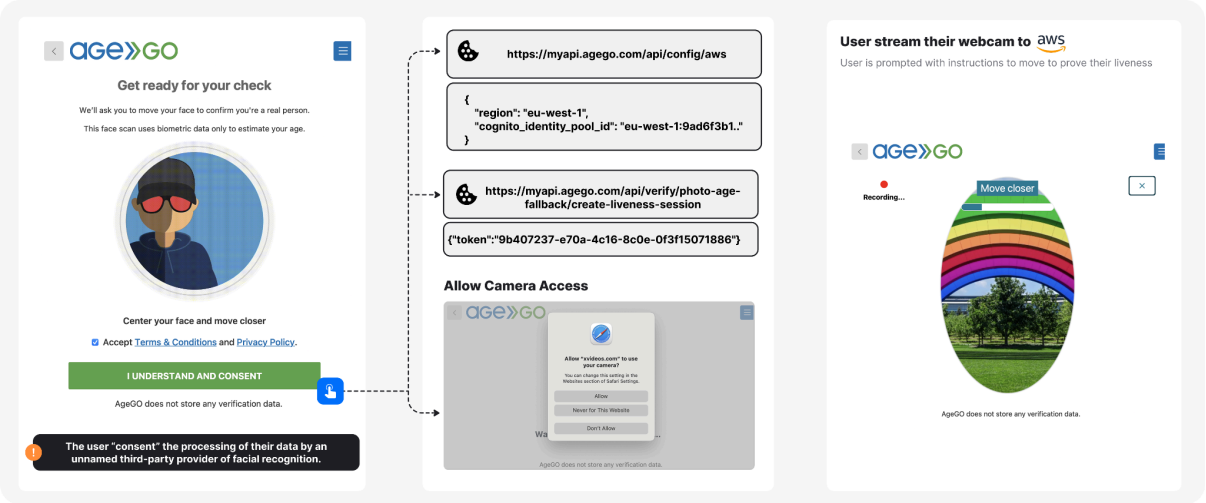


*Figure 3: Diagram of AgeGO age verification process using the "selfie" option*

[7] Archived at https://perma.cc/9CEF-2Y2M
[8] Archived at https://perma.cc/8W47-B48R

**Upon inspecting network traffic, we observed that the video stream captured from the user's webcam is sent directly to Amazon Web Services (AWS) "Rekognition"[9].**

In particular, rather than transiting through AgeGO's servers, the WebSocket stream is established directly from the user's browser to: streaming-rekognition.eu-west-1 .amazonaws[.]com.

As a result, AgeGO's selfie verification method not only transmits to AWS the user's webcam feed but also exposes their IP address, user agent, and the fact that they are accessing an 18+ website via AgeGO (the "origin" field of the requests being set as https://my.agego.com). While the exact platform among those using AgeGO is not transmitted, this may appear to constitute a significant disclosure.

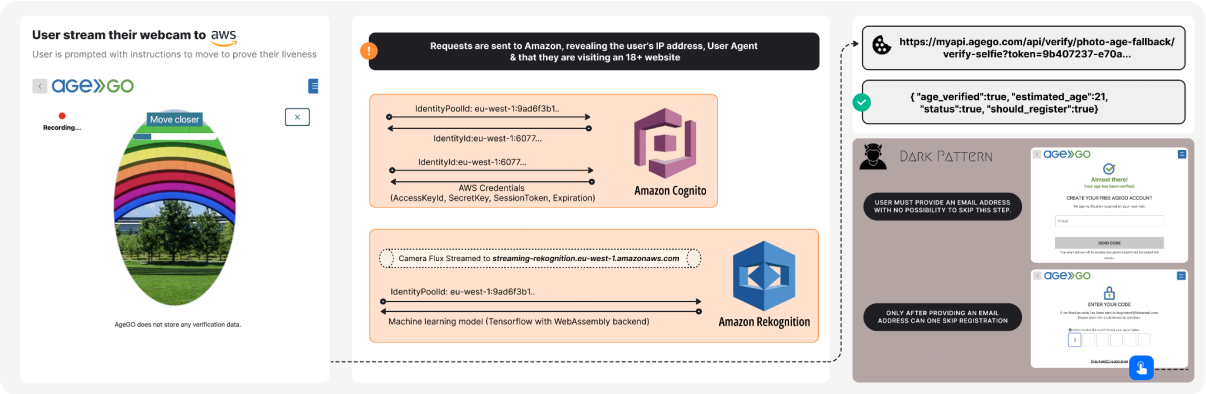


*Figure 4: Diagram of AgeGO Selfie age verification process - relying on AWS*

Upon successful age verification, users are required to provide an email address. This step is mandatory and cannot be skipped. Only after entering an email address—even a false one—can users complete the verification process by creating an AgeGO account or skipping it. This appears to constitute a **dark pattern**, as defined in EU regulations, by pressuring users to disclose more personal information than is necessary for age verification purposes.

Ultimately, the user is redirected to the sexually explicit content. This redirection occurs through a request to https://myapi.agego.com/api/session/return, which includes as its sole customized parameter: "`x-ag-sid`". The platform responds with —among other parameters— the original URL of the video the user sought to access.

[9] https://aws.amazon.com/rekognition/

## Conclusion

The AgeGO age verification system, implemented on xnxx.com, xvideos.com, and tnaflix.com, collects both the website and the exact URL of the content users seek to watch, and fails to inform users that their webcam stream will be shared with Amazon Web Services if they opt for the "Selfie" verification method.

AgeGO presents its 'Selfie' verification method as guaranteeing "double anonymity". Arcom specifies that such a verification system should ensure that:

I. The provider of the verification cannot know for which service the age verification has been performed—a requirement that is, by all accounts, breached by AgeGO's data collection;
II. No third party involved in the process should be able to recognize a user who has already used the age verification system. Yet, by establishing a direct stream between the user's device and Amazon Web Services, AgeGO reveals to AWS that the user's IP address is engaging with the agego.com system. As a result, AWS could, in theory, recognize a returning user. However, we do not have information on whether metadata is stored by AWS in a way that would enable such identification in practice.

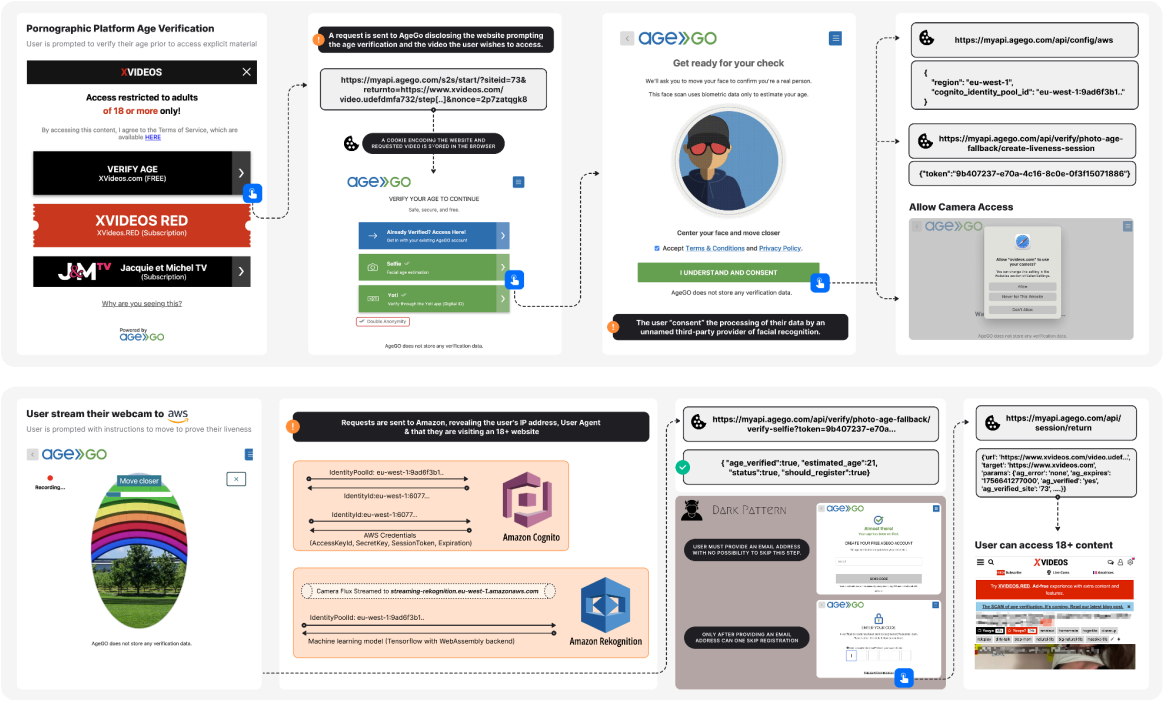


*Figure 5: Overall diagram of AgeGO Selfie age verification process*