Effectiveness of EU Age Control Legislation

An empirical analysis: can it actually reduce child abuse?

17 April 2026 · blog.opportunist.global

The political premise behind EU Age Control (AC) legislation — age verification, Chat Control/CSAR, age-gating of social media — is emotionally simple: *we are protecting children from abuse*. That premise requires empirical scrutiny. This analysis asks three questions: **who actually abuses children and where**, **which of these cases AC affects**, and **how easily AC is bypassed in practice**.

Context: what the EU is doing in April 2026

The situation has three layers. **Chat Control 1.0** died on 3 April 2026 when the European Parliament refused to extend it in a 311:228 vote. **Chat Control 2.0 (CSAR)** is still in trilogue negotiations, targeting a deal by summer 2026 — it would mandate content scanning including end-to-end encrypted services. The **EU Age Verification App** was announced on 15 April 2026 as „technically ready“ — users upload a passport or ID, platforms receive only a yes/no confirmation against an age threshold.

Pilot countries: France, Spain, Italy, Greece, Denmark, Ireland, Cyprus. The app is officially voluntary, but under the DSA platforms must demonstrate „equivalent effectiveness“ or face fines up to 6 % of global turnover — in practice mandatory. Von der Leyen's framing: „no more excuses“, „zero tolerance“. The entire legitimacy rests on AC helping children. Let's look at the data.

Who actually abuses children

This is the most important section because it fundamentally undermines the legislation's premise. The data is consistent across countries and studies over decades:

93 % of juvenile victims know their abuser — 59 % are acquaintances, 34 % family members, **only 7 % strangers** (US DOJ / RAINN). In substantiated CPS cases, **76 % of children** were abused by a parent or legal guardian. In the Netherlands only 7 % of offenders were strangers to the victim. Australian studies show similar numbers.

The risk profile is also well-established: children in single-parent households with an unrelated adult living there face risk up to **20× higher**; children with disabilities roughly 3× higher. Incest and stepfather abuse are dominant patterns of intrafamilial abuse.

The online dimension exists but is mostly a *layer* on top of offline relationships — the groomer is typically an adult known to the child through family, community, sports,

religion, school. The pure-stranger internet predator is statistically marginal.

> ***Conclusion: AC legislation is, by its very design, aimed at the minority slice of the problem that produces the fewest victims. The stepfather, coach, priest, or uncle at Christmas cannot be „stopped“ by age verification on Instagram.***

Online vectors: what AC addresses and what it doesn't

Online abuse has four distinct phenomena that political discourse routinely conflates:

1. CSAM distribution. According to IWF, 62 % of internationally identified CSAM is hosted on EU servers. But the key detail: this material is essentially not on mainstream platforms affected by AC. It circulates on the darknet, via P2P, Tor hidden services, specific encrypted channels. Age verification on Instagram affects no one trading CSAM on a hidden service.

2. Grooming of minors via platforms. Here AC superficially makes sense, but the logic fails: AC verifies age at account creation. An adult predator creates an account legally (18+). A minor also creates one (13+ or 16+). AC does not prevent adults and children from messaging each other. The actual solution — Breyer's „security by design“: default-private profiles for minors, restricted contacting by strangers, warnings when sharing contacts or nudes — requires none of the mass age verification apparatus.

3. Sextortion and self-generated content. A growing problem where a teen sends intimate content to someone who then extorts them. AC does nothing here — all parties can be legally verified.

4. Exposure to pornography. The only case where AC *theoretically* works. Empirical evidence from the UK and Australia destroys even that — see the next section.

Circumvention: what actually happened

Empirical data from countries that rolled out AC earlier is devastating:

After the UK's **Online Safety Act** took effect in summer 2025, VPN use surged **by 6 430 %**; VPN subscriptions rose 1 000 %. In **Australia**, after 9 March 2026 three VPN apps appeared in the App Store's top 15 free downloads in a single day. **Pornhub** withdrew from Australia, France, Louisiana, and Texas rather than implement verification — presenting only a block screen.

The Commission itself implicitly concedes the problem: documentation for the new EU app states that technically adept minors can bypass geographic restrictions via VPN, but the EU „considers this a limitation of any verification system rather than a fatal flaw“. Translation: we know it doesn't work, but we're doing it anyway.

Surveys: **41 %** of internet users have been asked to verify age, and **over half** attempted to bypass the process. This is not marginal resistance — this is dominant

behaviour.

Platforms respond with VPN detection, GPS correlation, deep packet inspection, IP range blacklists. But obfuscated VPNs (WireGuard over port 443, shadowsocks, Mullvad with obfuscation, I2P) remain essentially undetectable. Likewise trivial methods: shared parent account, fake ID, purchased verified account (already a functioning market), hotspot from a foreign SIM.

> ***The circumvention barrier is lower than the compliance barrier. Adults must sacrifice privacy and upload government documents; children download a free VPN.***

Effectiveness: what the data says about actual abuse reduction

There is no empirical evidence that AC legislation in any jurisdiction has led to a reduction in child abuse. No serious study. The misleading metrics used (NCMEC report counts, image takedown counts) measure *system activity*, not *child protection*. The distinction between activity and effect is the whole argument.

The European Parliament's own assessment of the original CSAR proposal was crushing: no technological solutions currently exist that can detect CSAM without a high error rate, and the regulation would undermine end-to-end encryption and digital communication security. The Council's own Legal Service warned it would breach Articles 7 and 8 of the Charter of Fundamental Rights.

Collateral damage

These are empirical, not ideological, costs of AC:

Building mass-surveillance infrastructure. Even though the current app is „privacy-preserving“ (zero-knowledge proofs, open source), it creates a centralised identity layer tied to government documents. Infrastructure built once gets repurposed — a standard pattern (COVID passports, which von der Leyen herself cited as a model).

Driving platforms out of the EU. Signal has threatened to leave. Pornhub already has. Smaller projects, decentralised services, and privacy-first operations cannot bear compliance costs — only megacorps survive. AC is an indirect tax in favour of Meta, Google, Microsoft.

Pushing children into worse environments. When minors are squeezed out of mainstream platforms they migrate to less-moderated spaces — unmoderated Discord servers, Telegram, random forums. Actual grooming venues are often smaller and less visible, not the largest platforms.

False sense of security. Parents who trust that „age verification protects“ become less vigilant about what their child is actually doing and with whom. AC can thus *worsen* outcomes by diverting attention from real prevention.

Normalising state identity for online access. Ultimately AC trends towards a model where anonymous internet access is technically impossible. That is a civilisational shift, not a technical adjustment.

Synthesis

The effectiveness of Age Control legislation in reducing child abuse is, on available data, near zero — perhaps marginally positive for exposure-to-porn among the least motivated minors. At the same time:

• **It addresses the wrong problem.** 93 % of abuse happens offline, beyond any digital control's reach.

• **It addresses the wrong minority of the online problem.** CSAM does not circulate on platforms AC affects.

• **It is trivially bypassed.** Empirical data from the UK (+6 430 % VPN) and Australia prove this in real time.

• **It builds infrastructure** with enduring costs to privacy and to the architectural freedom of the internet.

• **It is politically cheap.** It delivers strong emotional rhetoric („we protect the children“) without the political costs of measures that would actually work — resources for social services, investigative capacity against darknet CSAM networks, parental education, legislation targeting intrafamilial abuse.

Real reduction of child abuse would require: more resources for CPS and child psychologists, better detection protocols in schools and healthcare, programmes for at-risk families (single-parent households with step-partners), investigative capacity targeting darknet CSAM distribution, the „security by design“ approach for online platforms, and education for children about boundaries and communication with adults.

None of this is a priority in the current AC package. That alone is the strongest evidence that the stated goal and the actual goal have diverged.

Sources and notes

Abuse statistics: U.S. DOJ / Bureau of Justice Statistics; RAINN (Rape, Abuse & Incest National Network); National Children's Alliance; Dutch and Australian national studies. VPN circumvention data: ACS Information Age, TechRadar, Medianama, NordVPN/Proton reports March 2026. EU legislative status: Wikipedia Chat Control entry, EDRi, Patrick Breyer MEP posts, European Commission press releases, EDPS.

This analysis is descriptive and draws on publicly available data as of April 2026. It contains no legal recommendations.