12th December, 2025

Protecting Children without the privacy nightmare of Digital IDs

Mark Camilleri Gambin, General Secretary, Momentum

As governments worldwide, from Australia to the UK, legislate bans on social media for minors, the conversation shifts towards the dangers of invasive identification controls. The proposed solutions almost always involve Digital IDs or intrusive Age Verification systems requiring users to upload government documents or biometric data.

Privacy advocates raise the alarm bells. The risks from a surveillance infrastructure are too great, even when child safety is the end goal.

As a tech industry professional, I would like to outline an alternative route. From an engineering perspective, this solution is very do-able and far from "rocket science." It avoids the need for uploading passports to the cloud. It relies on a simple, privacy-preserving concept; a device-level OS signal.

The premise is simple: Children generally do not have purchasing power. They do not walk into a store and buy a €1000 or €500 smartphone. The buying process and the initial setup is typically done by the parent.

This is the control point. During the initial device setup, the operating system (iOS or Android) should offer a hard-coded option: "is this device for a minor?"

If "Yes" is selected, a flag is set deep within the OS. This flag is locked behind a parent-controlled password or biometric key. Saving it at this level means that it cannot be cleared or bypassed using a simple “factory-reset”.

The reality is that technical nuance matters. I am not talking about "stamping" every network request with a "child" label or header (which would be a privacy nightmare for ad tracking). I am talking of a simple on-demand API check, very similar to how geolocation data is accessed today (similar to navigator.geolocation for those with coding experience).

When you visit websites like Google Maps, they already execute a line of code which asks "Can I have your location?" The browser intercepts this, checks with the OS, and asks the user for permission.

Social media protection can work the same way. When a user visits Facebook, TikTok, Youtube or Instagram:

1. The site executes a request: navigator.getAgeStatus().
2. The Browser intercepts this request.
3. The Browser queries the Operating System's localised settings.
4. The OS returns a binary token: isMinor: true.

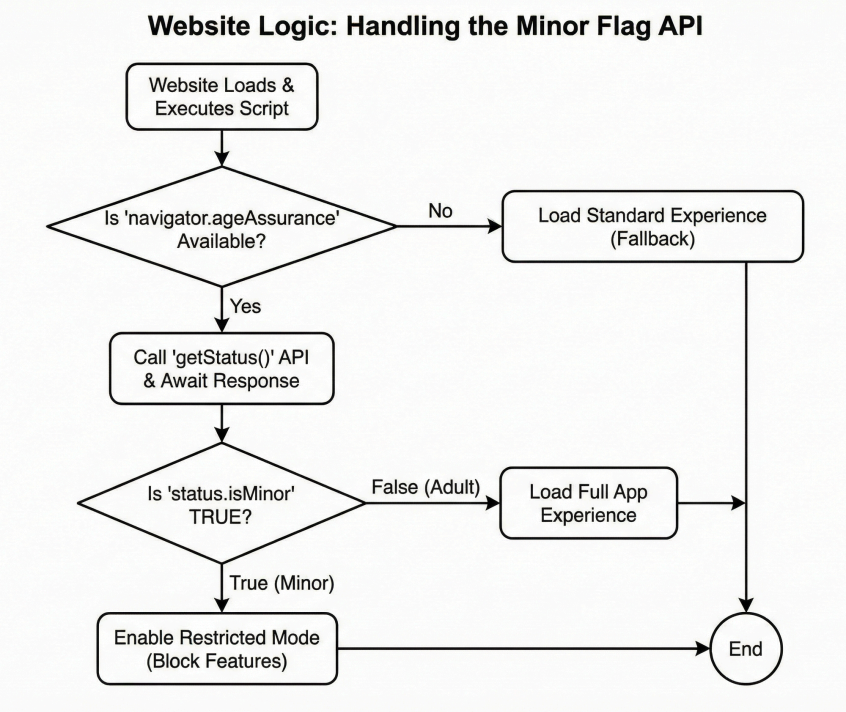
That is it. No name. No date of birth. No government ID number. Just a binary 1 or 0 processed locally on the device.

I write software for a living; therefore I am familiar with the technology behind this, and I can assure you that the infrastructure for this already exists.

- iOS has the "Screen Time" framework.
- Android has "Family Link."

Currently, these features are "walled gardens", used only by Apple and Google. The fact that they exist hints that there is some initiative to give parents some control. Legislation simply needs to force these OS giants to expose such status info via a standard API to any third-party developers or websites.

Here's a small flowchart of how the process can work:



Some may argue that waiting for the W3C (the web standards body) to agree on such an API can take years. The reality is that browser vendors like Google Chrome and Apple Safari implement powerful non-standard features all the time when it suits them or when legal compliance demands it. If the EU or Australia mandates this API, Chrome and Safari are able to roll it out in the next update. They do not need global consensus to flip a switch that can help protect children.

Because this solution relies on an active API request (like Geolocation) rather than a passive Header (which sends data automatically), privacy is preserved.

- No fingerprinting: Random blogs and news sites don't get this data unless they specifically ask for it and the browser policy allows it.
- No central databases: There is no government server holding a list of verified children.
- The "Hand-Me-Down" factor: Yes, if a parent hands their unlocked "Adult" phone to a child, the protection is bypassed. But we are solving for the majority use case: the child's own personal device. We cannot let the pursuit of a "perfect" solution prevent a highly effective solution.

What we need is commitment

The technology is constantly adding features like this. It is very doable. What is lacking is commitment.
We need to be careful. Some are already trying to use "child safety" as a Trojan Horse to weaken encryption or enforce mandatory Digital IDs for everyone. We must reject those dangerous oversteps.

Europe has the opportunity to lead here. Instead of mandating ID uploads, regulation should mandate that:

1. OS Manufacturers must expose a secure "Minor Flag" API.
2. Social Platforms must query this API before allowing account interaction.

This approach puts control back in the hands of parents at the point of purchase, where it belongs.

Mark Camilleri Gambin *mark@partitmomentum.org*
General Secretary, Momentum, Malta
Deputy Secretary-General, European Democratic Party

www.partitmomentum.org / https://democrats.eu/

Appendix: Browser “Minor Flag” API Handshake