OS Age Signals, Explained

Why the device layer matters — in plain language

Prepared by: Jonathan Westmoreland, Bend Privacy Alliance *A short companion to the Levy briefing memo. The full technical analysis is available as an appendix for anyone who wants the detail behind these points.*

The simple version

An operating-system age-signal law would not necessarily require a person to upload an ID or scan their face. Instead, the device or account system would ask for an age or birth date, turn that into a general age group, and let apps request that age group when the law says they need it.

That sounds simple, but it changes **where age information lives.** Instead of one website asking for your age, the age layer moves closer to the root of a person's digital life: the phone, tablet, computer, or account used to reach many different services.

One way to picture it: an OS age signal is like putting an age label at the entrance to the device, and then letting apps ask to see the label. That may sound harmless — but the real privacy question is *who gets to ask, what they keep, and whether the label later follows the person into more places than lawmakers ever intended.*

How it works, step by step

> **Person enters age or birth date → the phone or account turns it into a general age group** (like "13–15" or "18+") **→ an app asks for that age group → the app receives the signal → under an AB 1043-style law, the app may be treated as knowing the user's age group → the app changes what protections, limits, or features apply**

The important part is what happens *after* the first step: once the device or account can produce an age group, it can be asked for again and again — by more apps, and potentially, in a later law, by browsers and websites too.

Why this matters

The question is not only whether children are protected. They should be — and Oregon already has several laws aimed at student data, minors' commercial data, AI chatbots, and school-device use. The bigger question is whether Oregon would create a **reusable age layer** that can later expand from apps to browsers, websites, schools, and other services. A system built to send age signals to apps can quietly become general-purpose infrastructure for knowing — and acting on — everyone's age.

California is the live example. It enacted age signals for apps, and it is now considering a follow-on bill that would extend the same signal to browsers and websites. An Oregon law should be read as a *first step* in that direction unless it includes clear limits that prevent expansion.

What could go wrong (everyday examples)

An age signal assumes that one account belongs to one known-age person on one device. Real life is messier:

- A child uses a **parent's phone** — and the device may tell apps the user is an adult.
- A parent uses a **child's tablet** — and apps may wrongly restrict a legitimate adult.
- A student uses a **school-managed device** — and the school district can become the age authority, creating new exposure of student data.
- A **foster youth or emancipated minor** does not fit a normal parent-consent model.
- A **public-library computer** has no stable personal account, so the signal is meaningless or simply wrong.
- An app contains **advertising or analytics code** that sits right next to the age signal — which can turn a child-safety feature into a tracking tool.

These are not rare corner cases to wave away. They are exactly the situations where the system either blocks a legitimate adult or wrongly labels a child — and where a "safety" signal can leak into uses no one intended.

What safeguards Oregon should require (the red lines)

If Oregon adopts any age-signal system, these should be the floor:

- **No sharing of exact birth dates** — a general age group, at most.
- **No mandate for government ID or face scans.**
- **No central state age database.**
- **No use of age signals for advertising, profiling, school discipline, or immigration enforcement.**
- **Law-enforcement access should require a warrant or court order.**
- **No expansion from apps to browsers or websites** without separate legislation, public hearings, and a recorded legislative vote.
- **Real protections** for school-managed devices, open-source systems, and accessibility tools — and **prompt deletion** of any underlying age proof.

A short plain-language glossary

For reading alongside the technical analysis:

Technical term	What it means in plain language
Operating-system age signal	An age label created by the device or account
API	A software doorway that lets an app ask for information
Age bracket	A general age group, like 13–15 or 18+
Persistent identifier	A recurring tag that can help recognize the same user or app install over time
SDK	Outside code placed inside an app, often used for ads, analytics, or tracking
Linkability	The ability to connect the same person across apps, sessions, or devices
Actual knowledge	The law treating an app as if it knows the user's age
Scope creep	A system built for one purpose expanding into more uses later

Oregon can protect minors online without building a reusable age-surveillance layer. The job of this explainer is to make the architecture clear enough that a lawmaker can ask the right questions — not to prove every claim. The technical companion and the research archive provide the supporting detail and the primary-source citations.

Prepared by Jonathan Westmoreland, Bend Privacy Alliance. Note: the platform tools described here are new and changing, and the related litigation moves quickly; confirm current status before relying on any specific detail in a public setting.