

Questions for Oregon Sponsors

Before adopting OS- or app-store age verification

Prepared by Jonathan Westmoreland, Bend Privacy Alliance — a one-page leave-behind. Fuller analysis and primary-source citations available on request.

Protecting minors online is a legitimate goal, and Oregon already pursues it through several laws (student-data, consumer-privacy, AI-chatbot, breach-notification, and school-phone rules). These questions are meant to ensure any 2027 age-verification bill is necessary, narrowly drawn, and privacy-preserving — not a reusable age-signal layer that expands over time.

Questions for the bill's sponsors

1. **Which model is this** — school EdTech, app-store accountability, operating-system age signal, or proof-of-age? (These have very different privacy footprints and shouldn't be blended.)
2. **What specific harm** does it address that Oregon's existing laws — OSIPA, the Consumer Privacy Act, the AI-companion law, the school-phone order — don't already reach?
3. **Collect or only pass-through?** Must the OS *collect* age, or only relay a signal if age is already known?
4. **How broadly is age collected or inferred** — will most or all users, including adults, have to establish age?
5. **What exactly is shared** — only a coarse age bracket, or also exact birth date, verification method, supervision status, or a parent-child link?
6. **Who may request the signal** — first-party covered services only, or also browsers, websites, school apps, AI companions, and in-app advertising/analytics code?
7. **Scope lock:** does the bill bar expansion from apps to browsers/websites without separate legislation, public hearings, and a recorded vote? (California's AB 1856 is the warning.)
8. **Reuse ban:** are advertising, profiling, school discipline, and immigration uses prohibited, and is law-enforcement access gated behind a warrant or court order?
9. **Persistence:** is the signal queried in real time and promptly deleted, with no linkage to persistent tracking identifiers?
10. **Devices and schools:** which devices are covered, and how does it interact with school-managed devices, OSIPA, and FERPA?
11. **Enforcement and process:** who enforces (AG, private right of action, or both), and will a privacy impact assessment and independent technical review come *before* drafting?

Minimum safeguards (the red lines)

- No sharing of exact birth dates — a coarse age bracket, at most; no government-ID or biometric/face-scan mandate; no central state age database.
- No use of age signals for advertising, profiling, school discipline, or immigration enforcement; law-enforcement access only by 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.
- Strict purpose limitation, prompt deletion of underlying proof, transparency reporting, independent security audits, and a sunset / legislative-review clause.

Bend Privacy Alliance is not opposed to child-safety legislation; our ask is that Oregon prove any age-signal architecture is necessary, proportionate, technically workable, and privacy-preserving before it is built. Related litigation moves quickly — confirm current status before relying on specific details.