A PRIVACY BRIEFING · OREGON 2027

Who has to prove their age to use the internet?

Operating-system age verification, app-store accountability, and the surveillance infrastructure being assembled in the name of child safety — and what Oregon should ask before it joins in.

Research brief · compiled by Bend Privacy Alliance
For privacy-minded Oregonians shaping policy

Tracks A–D · Sections 1–20
24 slides

THE SETUP

A 2027 bill is coming — but the architecture isn't settled.

01 At a virtual town hall — *"What's Next: AI, Social Media, and EdTech"* — Oregon lawmakers announced plans to introduce **operating-system age-verification** legislation in the **2027 session**.

02 The event opened from a **healthy-tech / child-protection** posture — framing the debate around screen time and social-media harm, not a worked-out verification architecture.

03 By sponsors' own account, the **technical, privacy, data-storage, and implementation** questions have not yet been fully worked through.

IN THE ROOM

Rep. Emerson Levy	D–Bend
Sen. Lisa Reynolds	D–Portland
Rep. April Dobson	D–Clackamas
Rep. Kim Wallan	R–Medford
Ami Formica	wellwired.org

THE WORKING FRAME

Protecting minors online is important — but Oregon should not create a statewide age-data infrastructure without first proving the approach is *necessary, effective, privacy-preserving, narrowly tailored, technically workable,* and *resistant to repurposing.*

THE CORE DISTINCTION

"Age verification" is four different things.

Do not let them collapse into one bill. Each has a different data architecture, privacy risk, and constitutional posture.

A School technology / EdTech

Screen limits, device opt-outs, an EdTech registry, student-data rules. About **schools and procurement** — not the open internet.

B App-store accountability

Stores verify age, assign categories, broker parental consent to developers. The **Texas / Utah / Louisiana** model.

C Operating-system age signals

HIGHEST PRIORITY

The OS collects age at setup and transmits an age-bracket signal to apps. Closest to **California AB 1043** — and the likely 2027 template.

D Proof-of-age credential

Prove you're over a threshold (18+) **without disclosing** birthdate or identity. The EU counter-model.

THE QUESTION THAT DECIDES EVERYTHING

When a lawmaker says *"operating-system age verification,"* which of the four models do they actually mean?

A single answer determines the privacy risk, the constitutional exposure, and who is forced to prove their age.

Section 14 · Q1 — Which model is being considered?

B APP-STORE ACCOUNTABILITY

Contested in court — but operating right now.

App stores verify age, assign categories (<13 / 13–15 / 16–17 / 18+), and pass an **age and parental-consent signal** to developers before a minor downloads or uses an app.

Oregon's own attempt, **HB 3696 (2025)**, died in committee. The model lives on in Texas, Utah, Louisiana, and Alabama.

> **The pattern to convey:** district courts keep blocking these laws on First Amendment grounds — then appellate courts stay the injunctions and let them run.

TEXAS SB 2420 — THE CAUTIONARY TIMELINE

May 2025	Signed by Gov. Abbott.
Dec 2025	Enjoined in full — content-based, fails strict scrutiny.
May 2026	District court refuses to lift the injunction.
Jun 2026	**5th Circuit stays it — SB 2420 takes effect. Merits unresolved.**

C OPERATING-SYSTEM AGE SIGNALS · CALIFORNIA AB 1043

The operating system becomes an age broker.

Enacted, unanimous, effective **Jan 1, 2027** — and the closest match to what Oregon reportedly named.

01 · COLLECT

OS prompts for birthdate / age at device or account setup.

→

02 · DERIVE

Stored as a coarse bracket — never the exact date downstream.

→

03 · SIGNAL

App requests it; OS returns the bracket via a real-time API.

→

04 · LEGAL EFFECT

Developer is deemed to have **"actual knowledge"** of the user's age.

Self-report

No government ID, no biometric. Lighter-touch than Texas — yet it builds the deeper infrastructure.

4 brackets

<13 · 13–15 · 16–17 · 18+. A coarse signal — but a persistent one.

$2.5k–7.5k

Per affected child, per violation. Enforced by the California AG.

Section 1A · AB 1043 — Civil Code Sections 1798.500 et seq.

INSIDE THE SIGNAL · HOW THE ARCHITECTURE ACTUALLY WORKS

An OS age signal is like putting an *age label at the entrance to the device* — then letting apps ask to see it.

That can sound harmless. 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.

Technical companion · prepared by Bend Privacy Alliance

C THE SIX-STAGE ARCHITECTURE

Where age data goes — and where it can be misused.

Collection and derivation are settled by the platform. The privacy outcome is decided in **stages 4–5.**

STAGE	WHAT HAPPENS	WHO CONTROLS	KEY RISK INTRODUCED
1	**Collection**	OS / account provider	Adults pressured to self-identify; is the real birthdate kept?
2	**Derivation**	OS / account layer	Where the birthdate lives after the bracket is derived.
3	**Translation**	OS / platform	Extra fields — method, supervision, parent link — widen the surface.
4	**Request**	Recipient app + its code	**Who is allowed to ask** — third-party code inherits the app's access.
5	**Delivery**	OS / platform	Whether a **persistent identifier** rides along (it does, on Android).
6	**Legal effect**	Statute + recipient	"Actual knowledge" can be met by collecting *more* data, not less.

! THE MOST CONSEQUENTIAL QUESTION

"Only the requesting app" is not "first-party only."

The platforms scope the signal to the *app* — not to a first-party identity inside it. Everything in the app's process inherits that access.

AGE SIGNAL ENTERS →

THE COVERED APP — ONE BOUNDARY

✓ **First-party code**
Uses the bracket to apply child-safety protections. Legitimate.

✕ **Ad / analytics SDK**
Sits in the same process — **inherits the same access** to the signal.

THE FAILURE MODE

A "child-safety" signal becomes a **tracking attribute** the moment it sits next to ad-tech inside an app.

Platform terms ban this — but by **policy and audit**, not technical impossibility. The bar has to be in the **statute.**

C PERSISTENCE & LINKABILITY

The bracket isn't an identifier — until it's combined with one.

BRACKET ALONE

4 values, low entropy

<13 · 13–15 · 16–17 · 18+. Not enough to identify anyone on its own.

+

A PERSISTENT ID

Device ID | Account ID

Android installId

Android returns a persistent install ID developers are told to **store.**

→

RESULT

A durable attribute in a per-user profile

THE NEW CHOKEPOINT

Each platform's signal stops at **one operating system.** So compliance middleware has emerged that **aggregates Apple, Google, console, and web signals into a single cross-platform session** — a centralization and linkability point no single platform's privacy promise covers. A bill should treat any aggregation layer as a covered entity.

C THE TWO LIVE IMPLEMENTATIONS · BOTH IN BETA

The platforms hand over a signal — nothing more.

They don't decide what it means in Oregon law, and they don't gate any feature. Everything protective is built by the statute.

Google Play

Android · checkAgeSignals

Returns	A status + an age range (ageLower / ageUpper).
Identifier	**Persistent installId — developers told to store it.**
Use limits	No ads / profiling / analytics; no long-term storage.
Anti-spoof	Pairs with the Play Integrity API.

Live for new Texas accounts since **May 28, 2026**

Apple

iOS / iPadOS / macOS · requestAgeRange

Returns	An age band + the assurance method — never the birthdate.
Identifier	None of its own — but guidance says persist consent server-side.
Consent	Parent-controlled: always / per-request / never.
Revocation	Withdrawal can block app launch (PermissionKit).

Live for new Texas accounts since **Jan 1, 2026**

WHERE THE SIGNAL MISFIRES

It assumes one account = one known-age user, on one device.

Every case below either **over-restricts a legitimate adult** or **mislabels a minor as an adult.**

Child on a parent's phone

The device may tell apps the user is an adult.

Parent on a child's tablet

Apps may wrongly restrict a legitimate adult.

School-managed device

The district becomes the age authority — new student-data exposure.

Foster / emancipated minor

Doesn't fit a normal parent-consent model.

Library / public computer

No stable account — the signal is meaningless or simply wrong.

Open-source OS & assistive tech

May not collect age at all; age-gating can block accessibility.

THE COUNTERINTUITIVE PART

The model courts keep *blocking* is the app-store one. The OS age-signal model has *never been challenged* — and may be harder to challenge, because it passes a signal instead of blocking speech.

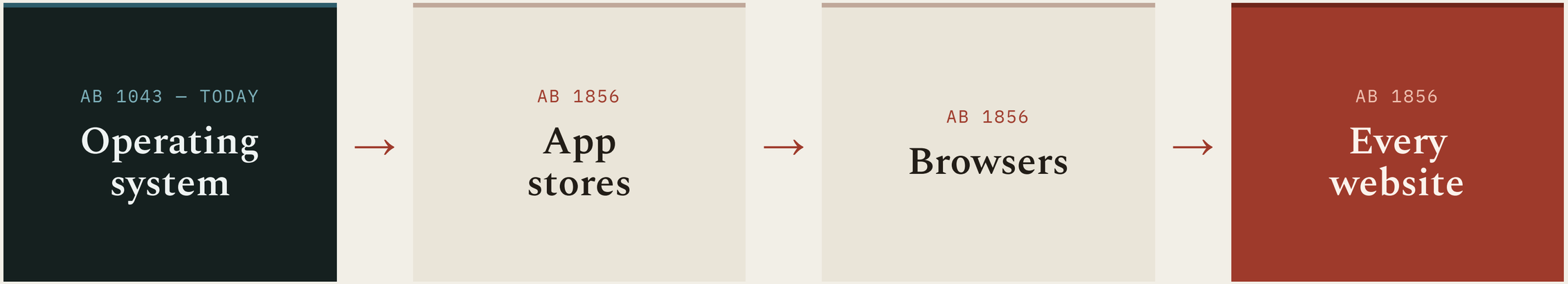
That durability isn't reassuring. It's the reason to worry — if it survives the First Amendment, only the statute's own guardrails will protect Oregonians.

Sources · 11.2 · 12A · 16

THE SCOPE-CREEP WARNING · CALIFORNIA AB 1856

A narrow signal becomes web-wide age gating.

In one follow-up session, AB 1856 extends the very same age signal from the OS to the open web.



EFF: "One step forward, two steps back." An age signal normalized at the OS layer becomes infrastructure that later laws extend — to the whole web.

Section 1A · AB 1856 — passed CA Assembly 68–1, May 2026 (not yet law)

WHAT THE CASE LAW ACTUALLY SAYS

The line courts draw — and the framing blurs.

SURVIVABLE ✓

Verifying age for sexual material obscene to minors

Free Speech Coalition v. Paxton (2025, 6–3) upheld it under **intermediate scrutiny** — only an "incidental" burden on adults.

Reasoning **expressly limited** to obscene-to-minors content. It does **not** extend to general audiences.

STRUCK DOWN ×

Gating general lawful content — social media, app stores

Treated as **content-based**, triggering **strict scrutiny**. Most have fallen at the trial level.

The state has *no "free-floating power to restrict the ideas to which children may be exposed."* — Brown v. EMA

WHERE THE LAWS STAND · JUNE 2026

Blocked, then revived. The merits are unresolved.

Oregon would be legislating into genuine constitutional uncertainty — not a settled win for either side.

LAW / MODEL	STATUS	WHERE IT STANDS
Oregon HB 3696	Died	App-store model; died in committee, 2025.
Texas SB 2420	In effect	Enjoined Dec 2025 → revived on appeal, in force June 2026.
Utah · Louisiana	Delayed	Narrowed to private enforcement; pushed to 2027.
California AB 1043 OS model	Not challenged	Enacted, effective Jan 2027. Untested — and the bigger long-term concern.

Sources · 1A · 10 · 12A — confirm against live dockets before formal use

OREGON IS NOT A BLANK SLATE

Four layers of law already occupy this space.

So the real question isn't "should we protect kids?" — it's **what specific gap survives all of these?**

OSIPA

Already bans **selling student data** and targeting ads to students.

ORS 336.184

OCPA

No sale, profiling, or ad-targeting of **under-16** data — since Jan 2026.

ORS 646A.578

SB 1546

Regulates **AI companions** with a "reason to believe a minor" standard.

Ch. 85, 2026

EO 25-09

Statewide **bell-to-bell** school phone policy — 100% of districts.

Kotek, 2025

⚠ LIVE CONSTRAINT

SB 141 mandates K–8 digital interim testing three times a year (2026–27) — colliding head-on with any "remove screens from young classrooms" proposal.

PRELIMINARY RISK MATRIX

The OS model carries the most risk on nearly every axis.

RISK	App-store	OS signal	Proof-of-age
Adult privacy burden	High	High	Medium
Data centralization	High	Very high	Lower
Tracking / fingerprinting	Medium	High	Lower
Data-breach exposure	High	Very high	Medium
Repurposing risk	High	Very high	Medium

WHAT'S ACTUALLY AT STAKE IN A BREACH

A coarse bracket can be re-issued. A face cannot.

AB 1043 is self-report for a reason. Every step toward **birthdates, biometrics, or ID scans** rebuilds a honeypot of data that can never be made un-leaked.

EXACT BIRTHDATE

Permanent. Unchangeable.

Paired with a name, it's the master key to **credit, account recovery, and identity verification.** Hospitals confirm it before discussing your medical records. You can reset a password — never your date of birth.

BIOMETRIC / FACE SCAN

Irreversible.

A leaked faceprint can't be re-issued like a credential. It enables **face-matching against you across cameras** for life — and feeds spoofing and deepfakes.

GOVERNMENT ID SCAN

A whole dossier, in one image.

Name, photo, address, document number — everything needed for **identity theft, stalking, and doxxing** — sold and merged on broker and criminal markets.

⚠ BEYOND THE HACKER

The same store invites **subpoenas, immigration enforcement, and data-broker enrichment.** A breach is only the loudest failure — repurposing is the quiet one. This is why Section 15 bars all three from traveling or being retained downstream.

IF OREGON PROCEEDS — THE RED LINES

Safeguards that must come built in.

These mirror the FTC's own federal conditions — cite them as the floor any Oregon bill should meet or exceed.

Data minimization

No exact birthdate to developers. No biometric or ID mandate. Coarse signal only — no persistent age token.

Purpose limitation

Child-safety compliance only. No advertising, profiling, personalization, or content ranking.

Deletion & security

Delete the underlying proof promptly. No centralized state age database. Encryption + independent audits.

No repurposing access

No law-enforcement access without a warrant. No immigration-enforcement or school-discipline use.

Scope & open source

High-risk services only. No universal OS-level collection. Carve out open-source systems and libraries.

Transparency & sunset

Privacy-impact + feasibility review before enactment. Annual reports. Mandatory sunset and legislative review.

BRING THESE TO YOUR LAWMAKER

Six questions that separate safety from surveillance.

1. Which of the four models is this — and what **specific harm** does it solve that existing Oregon law doesn't?
2. How broadly is age collected — will **adults** have to prove their age too?
3. Who **stores the underlying age proof** — and for how long?
4. Can the signal be **repurposed** — ads, profiling, law enforcement, school discipline?
5. What happens on **shared family and school-managed devices?**
6. Will a **privacy-impact and feasibility review** happen *before* drafting?

THE TAKEAWAY

Oregon can protect children online *without* creating a statewide age-surveillance layer.

Child safety and privacy are not competing values. No Oregonian should have to prove their age to use ordinary digital tools or read lawful speech.

THE STRONGEST POSTURE

It isn't opposition. It's insisting on proof.

01

Separate the four models — never one vague bill.

02

Name the gap that survives existing law.

03

Require the Section 15 safeguards up front.

04

Ask the six questions — before drafting begins.