Age Verification / OS Age Signals / School Technology Research Packet

Prepared for: Jonathan Westmoreland
Purpose: Working research packet for a conversation with Rep. Emerson Levy and/or other Oregon lawmakers about proposed 2027 legislation involving operating-system age verification, app-store age verification, EdTech, student privacy, and school technology regulation.
Date compiled: June 17, 2026 · **Last updated:** June 18, 2026
Status: Internal research archive — source-checking pass substantially complete. Statutory and case-law claims are pinned to primary sources (see §1A Source & Status Log and §1A-Pins); confidence is graded throughout. A shorter legislator-facing memo has been drafted separately (`levy_briefing_memo.md`); this packet remains the source archive. A small number of fast-moving items (Texas SB 2420 posture, AB 1856 progress) still warrant a live-status check the morning of any formal use. The platform technical-architecture layer is now substantially addressed in a companion technical analysis (`os_age_signal_technical_analysis.md`); remaining technical follow-ups include Microsoft/Xbox, Meta/Snap/TikTok/Discord/Roblox, browser-level relay behavior, and same-day checks of the beta platform documentation before formal use.

---

1. Immediate Context

Jonathan attended a virtual call/town hall described as **"The Future of AI and Technology"** and later identified as the official Oregon Legislature event:

Virtual Town Hall — "What's Next: AI, Social Media, and EdTech"

Opening presenter: Before the elected officials spoke, **Ami Formica, Co-Founder of Well Wired** (wellwired.org), gave an opening presentation. This framing detail matters: the event opened from a healthy-tech / child-protection advocacy posture, which shapes how the subsequent legislative discussion was set up.

Reported speaker pattern from the event:

- Ami Formica — Co-Founder, Well Wired (opening presentation)
- Sen. Lisa Reynolds
- Rep. Emerson Levy
- Rep. April Dobson
- Rep. Kim Wallan

Well Wired — organizational profile (source-checked June 17, 2026):

- **What it is:** A Bend, Oregon-based parent community and advocacy group. Per its own About page, it is a "local parent community and advocacy group whose mission is to change the status quo of smartphone and social media use among elementary and middle school aged-kids, and to promote healthy screen use in schools."

- **Co-founders:** Ami Formica and Brooke Mues, both Bend parents with children in the Bend-La Pine School District.
- **Founded:** Early 2024 (reported as February 2024).
- **Mission/positioning:** Advocates for "healthy tech at home, in our schools, and in the community"; promotes dialogue about intentional tech use and "limited, educationally valuable use of tech in our schools." The group states it is not anti-tech.
- **Known activity:** "Healthy Tech Talks" at Bend-La Pine elementary schools; a "Healthy Tech Pledge" campaign (reported 500+ Central Oregon kids); working with Bend-La Pine Schools on classroom device policies (e.g., docking iPads when not in use); and advocacy to restrict social media use for adolescents until age 16.
- **Contact:** P.O. Box 1418, Bend, OR 97709; wellwired.org.
- **Source basis:** wellwired.org "About" page; Bend Bulletin (May 3, 2024); Central Oregon Daily (May 4, 2024); KTVZ (June 19, 2024); Source Weekly "Bend Don't Break" podcast (2024).

Why Well Wired matters for the conversation with Rep. Levy:

- Well Wired sits squarely in **Track A (school technology / EdTech)** and the broader child-safety/healthy-tech movement — not in the OS-level or app-store age-signal architecture that is the highest-priority privacy concern. Its presence as the opening presenter is a clue that the 2027 effort may be motivated more by *school screen-time and social-media harm* concerns than by a worked-out age-verification *architecture*.
- The group's stated goal of restricting social media until age 16 is conceptually adjacent to age-assurance proposals, so it is worth being precise about where Well Wired's school-focused asks end and where statewide age-signal infrastructure begins. The four-track distinction in Section 2 is the tool for keeping those separate.
- Well Wired is a Bend-La Pine-anchored group, which makes it a locally relevant stakeholder/potential point of contact (and a likely ally on EdTech data-minimization questions even where positions diverge on broad age verification).

During the call, it was announced that lawmakers expect to introduce legislation during the **2027 Oregon legislative session** involving **operating-system age verification** or a related age-assurance model. The conversation with lawmakers suggested that some sponsors may not yet have fully worked through the technical, privacy, data-storage, and implementation concerns.

Other items referenced on the call. Speakers also pointed to several existing Oregon measures as context for the 2027 effort: **HB 2251** (the 2025 school cell-phone bill), **SB 1546** (the 2026 AI-companion chatbot law), and the fact that the cell-phone bill died but the Governor achieved similar functionality through an executive order. These are all now source-checked in Section 1A. The short version: HB 2251 *was* the cell-phone bill that died; it was replaced by **Executive Order 25-09**. SB 1546 is a separate, already-enacted AI-chatbot law. Both trace back to **Sen. Lisa Reynolds**, who presented at this town hall — useful to know going into the Levy conversation, since the 2027 proposal is emerging from the same cluster of sponsors and the same legislate-then-fall-back-to-executive-action pattern.

The door was left open for Jonathan to contact **Rep. Emerson Levy** for a deeper conversation.

Initial Working Frame

The strongest posture for that conversation is not simply opposition. A more constructive frame is:

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

1A. Source & Status Log — Confidence-Graded (Pass 1–2, last updated June 17, 2026)

This section records claims that have been checked, **with graded confidence** so nothing overclaimed reaches a memo or testimony. Per reviewer guidance, "verified" is retired in favor of five labels:

- **Primary-source checked** — confirmed against the statute, court order, or agency document itself.
- **Secondary-source checked** — confirmed against reputable legal/news reporting, but not yet the primary text.
- **Needs primary pin-cite** — substance is reliable but a memo should cite the underlying section/page.
- **Needs status update** — fast-moving; re-confirm against the docket/legislative record before use.
- **Interpretive conclusion** — analysis or framing, not a neutral fact; labeled as such.

A consolidated **source table** appears at the end of this section (§1A-Sources). Anything not logged here should be treated as first-pass and unverified.

Oregon HB 3696 (2025) — DIED IN COMMITTEE [PRIMARY: OLIS / LegiScan]

- Sponsor: **Rep. E. Werner Reschke**. Introduced Feb 25, 2025; first reading; referred to the **House Committee on Commerce and Consumer Protection on Feb 27, 2025**. No work session, no committee vote, no further recorded action. The bill **died in committee** at sine die.
- Architecture: app-store / developer accountability model (age verification, age-group categories, parental consent before download/purchase, age ratings, parental time-limit tools, AG enforcement, $500/day statutory damages). It also defines "mobile operating system," so it brushes the OS layer but is fundamentally an app-store bill.
- **Implication for the Levy conversation:** Oregon's most recent app-store age-verification attempt came from a Republican sponsor and went nowhere. The 2027 effort discussed at the town hall (Reynolds/Levy/Dobson, with Wallan) is a separate, later initiative. Ask explicitly whether 2027 revives HB 3696's app-store model or pivots to the OS-signal model.

California AB 1043 — Digital Age Assurance Act — ENACTED [Primary-source checked: CA Legislative Information; secondary for vote/backers]

- Author: **Assemblymember Buffy Wicks** (who also authored the CA Age-Appropriate Design Code Act). Signed by **Gov. Newsom on Oct 13, 2025**. Passed both chambers unanimously (**76–0 Assembly, 38–0 Senate**), with support from Google and Meta. **Effective Jan 1, 2027.**
- Mechanism (stated precisely, now pinned to the codified text — **Civil Code Title 1.81.9, §§1798.500 et seq.**, added by Ch. 675, Stats. 2025): beginning Jan 1, 2027, an **"operating system provider"** (defined as a person/entity that **develops, licenses, or controls** the OS on a computer, mobile, or other general-purpose device) must provide an **accessible interface at account setup requiring the account holder to indicate the birth date, age, or both** of the device's user, "for the sole purpose of providing a signal regarding the user's age bracket." It must then provide a requesting developer a real-time API signal, **send only the minimum information necessary**, and not share it with third parties for non-required purposes. Minimum **age brackets: under 13; 13 to under 16; 16 to under 18; 18 or older.** The **"actual knowledge" clause** is the operative hook: a developer that receives a signal **"shall be deemed to have actual knowledge of the age range of the user … across all platforms of the application and points of access of the application even if the developer willfully disregards the signal."** Penalties (**§1798.503**): up to **$2,500 per affected child** per negligent violation, **$7,500** per intentional violation; **California AG** enforcement; good-faith safe harbor for erroneous signals. **Crucial distinction from Texas/Utah:** AB 1043 requires only that the account holder *"indicate"* age (self-report) — **no government ID or biometric verification** — which is why it reads as lighter-touch even though it builds the deeper infrastructure.
- **Careful framing on adults (per reviewer note — do not overstate).** The statute does not, on its face, say "every adult must verify their age." But because a system must distinguish minors from adults to know whether protections apply, **OS-level age-signal laws may, depending on implementation, pressure platforms to collect or infer age data broadly — including for adults.** State it that way, not as a literal universal-verification mandate.
- Newsom's signing statement itself flagged unresolved problems: multi-user family accounts and profiles used across devices.
- **This is the closest match to "OS-level age verification" and remains the highest-priority model to analyze.**

California AB 1856 — amends AB 1043 — IN PROGRESS, NOT YET LAW — ★ MAJOR WATCH ITEM [Secondary-source checked: EFF, Tom's Hardware, CA Legislative Information; needs primary pin-cite to enrolled text]

This is not a minor cleanup bill — treat it as one of the strongest privacy warnings in the file. It shows how an "OS age signals for apps" law can grow into "OS-to-browser-to-website age signaling."

- Also authored by **Buffy Wicks**; introduced **Feb 11, 2026**. **Passed the Assembly 68–1 on May 28, 2026**; referred to the Senate (Rules Committee). **Not yet enacted** as of mid-June 2026. AB 1043's Jan 1, 2027 effective date is unchanged.
- **The scope-creep is the headline.** Per the California text, AB 1856 would extend the age-signal pathway beyond OS providers and app stores to **covered application stores, developers, browser providers, and internet website operators** — defining browser providers and website operators into the age-signal chain and requiring browsers to relay the OS age signal to covered sites. The signal layer would migrate from the OS down to the open web.
- **Open-source carve-out.** It narrows "operating system provider" to exclude software distributed under licenses permitting copy, redistribution, and modification — sparing most Linux/BSD distros (hybrid cases like SteamOS remain unresolved).
- **EFF position (May 29, 2026): "one step forward, two steps back."** Directly usable for the Levy conversation: even though AB 1043 does not *explicitly* mandate age verification, its **liability structure pressures companies to verify ages anyway**, and an age signal normalized at the OS layer becomes infrastructure later laws can extend — which is exactly what AB 1856 demonstrates: how the framework could be pushed to browsers and websites.
- **Oregon warning to state plainly:** a 2027 Oregon bill drafted as a narrow "OS age signal for apps" measure can, in a single follow-up session, be amended into web-wide age gating. Ask for the *full* intended scope up front, and for anti-scope-creep language.
- Useful precedent: open-source carve-out language exists and can be modeled; **Colorado** reportedly passed a bill (awaiting signature) with broader open-source exemptions (OS, apps, code repositories, containers).

Texas SB 2420 — App Store Accountability Act — BLOCKED, THEN REVIVED ON APPEAL; NOW IN EFFECT [Primary-source checked: district orders + 5th Cir.; secondary for dates]

- Authored by **Sen. Angela Paxton**; signed by **Gov. Abbott in May 2025**; scheduled to take effect **Jan 1, 2026**.
- **CCIA sued Oct 16, 2025**; consolidated with a challenge from Students Engaged in Advancing Texas (SEAT). After a Dec 16, 2025 hearing, **Judge Robert Pitman (W.D. Tex.) granted a preliminary injunction on Dec 23, 2025**, enjoining the **entire law**.
- Reasoning (highly relevant): the court treated app stores as **gateways to protected speech**, applied **strict scrutiny** (content-based), found Texas failed narrow tailoring / least-restrictive-means, found the law over- and under-inclusive, and found key provisions (age-rating liability; "significant changes" notice) **unconstitutionally vague**. Could not be saved by severance. The court noted it would also fail intermediate scrutiny.
- **AG Paxton appealed (Dec 23, 2025)** and moved to stay the injunction pending appeal. **The status has since flipped:** on **May 6, 2026, Judge Pitman denied** the State's motion to stay the injunction; Texas appealed that to the Fifth Circuit; the **Fifth Circuit entered an administrative stay (May 28, 2026) and then formally stayed the injunction pending appeal (June 4, 2026)** — so **SB 2420 took effect June 4, 2026 and is currently being enforced** (new Apple/Google accounts in Texas require age assurance; existing accounts exempt). The **constitutional merits remain undecided**

at the Fifth Circuit. Case Nos.: CCIA v. Paxton, 1:25-cv-01660 (W.D. Tex.); 5th Cir. No. 25-51073. **[Needs-status-update item — confirm against the Fifth Circuit docket before citing in a memo.]**

- The district court expressly **distinguished Free Speech Coalition v. Paxton** (the narrower porn-site age-verification law SCOTUS upheld) to show SB 2420's overbreadth — but note that distinction came from the *enjoining* court, and the appellate posture is now less favorable to that view.

Free Speech Coalition, Inc. v. Paxton — SCOTUS, decided [PRIMARY: slip opinion]

- **606 U.S. 461 (2025), No. 23-1122, decided June 27, 2025, 6–3.** Majority: Thomas (with Roberts, Alito, Gorsuch, Kavanaugh, Barrett). Dissent: Kagan (with Sotomayor, Jackson).
- Held: Texas HB 1181 (age verification for commercial sites where >1/3 of content is "sexual material harmful to minors") triggers **intermediate scrutiny** and survives it, because it **only "incidentally burdens" adults' protected speech**. Rejected both strict scrutiny (FSC's position) and rational basis (the Fifth Circuit's).
- **Critical limiting principle (load-bearing for the constitutional section):** the holding is expressly confined to **sexual material that is obscene as to minors**. EFF, the ACLU, and the Harvard Law Review all emphasize the reasoning does **not** extend to general-audience content such as social media or app stores, where minors and adults have coextensive access rights. **This is the single strongest doctrinal point against OS-level / app-store age verification for general content** — and it is exactly the distinction the Texas SB 2420 court used to strike that law down.

FTC COPPA Enforcement Policy Statement — issued [PRIMARY: FTC]

- **Issued Feb 25, 2026**, following the FTC's **Jan 28, 2026 Age Verification Workshop**. The FTC says it will **not bring COPPA enforcement actions** against general-audience and mixed-audience operators that collect/use/disclose personal information **solely to determine a user's age** without first obtaining verifiable parental consent — *provided* they meet conditions: purpose limitation (age determination only), prompt deletion, vetted third parties, clear notice, reasonable security, and reasonable accuracy.
- It does **not** amend the COPPA Rule (a formal review is signaled) and does **not** change obligations for child-directed sites. The 2025 COPPA Rule amendments carry an **April 22, 2026 compliance deadline**.
- **Two-edged for the Levy conversation:** the federal regulator is now actively *encouraging* age verification (reframes the "is this necessary?" debate), but the FTC's own conditions — purpose limitation, prompt deletion, security, accuracy — closely **mirror the safeguards proposed in Section 15** and can be cited as the federal baseline any Oregon bill should meet or exceed.

Federal landscape note [AUTH-SECONDARY]

- **COPPA 2.0:** the Senate reportedly passed its version unanimously; the House Energy & Commerce Committee tabled its version after the Senate vote. Federal action could reshape or preempt state approaches — relevant to the "should Oregon wait/harmonize" question.

- **Alabama HB 161** (signed Feb 17, 2026; effective Jan 1, 2027) is a newer App Store Accountability Act not in the original packet — explicitly covers pre-installed apps, with a retroactive verification requirement. Worth adding to the model-bill set.
- **Federal AI preemption pressure:** A Trump administration executive order on AI (signed Dec 11, 2025) and a DOJ **AI Litigation Task Force** (announced by AG Bondi Jan 9, 2026) aim to challenge state AI regulation. Relevant to whether *any* Oregon 2027 measure survives federal challenge.

Oregon measures referenced on the town-hall call [PRIMARY: OLIS / Governor's Office + AUTH-SECONDARY]

These were name-checked on the call and are likely to recur in Jonathan's future work. All three connect to **Sen. Lisa Reynolds** (a pediatrician and town-hall presenter) and illustrate Oregon's pattern of pairing child-tech legislation with executive fallback.

- **HB 2251 (2025) — school cell-phone bill — DIED, replaced by executive order.** Chief sponsor **Rep. Lisa Reynolds (D)**; Rep. **Emerson Levy (D-Bend)** also worked on the cell-phone effort for over a year. The bill would have required all districts to bar student cell-phone use "bell to bell" (start to end of the instructional day, including lunch and passing periods), with exceptions (e.g., medical, IEP/504). It **failed to clear a key Senate committee vote** amid opposition from school board / administrator groups over a state mandate and enforcement cost. **HB 2251 is itself "the cell-phone bill that died"** — not a separate item.
- **Executive Order 25-09 (signed by Gov. Tina Kotek, July 2, 2025) — the executive fallback.** Directs all Oregon K-12 public school districts to adopt bell-to-bell personal-electronic-device policies; districts had to adopt policies by **Oct 31, 2025**, fully in effect by **Jan 1, 2026**. ODE issued an implementation FAQ and model policies; consequences may not include loss of instructional time (no suspension/expulsion). By early 2026 the Governor's office reported **100% of Oregon districts** had adopted policies. Well Wired (Ami Formica / Brooke Mues) publicly praised the order. **Relevance:** demonstrates the "legislate, and if it fails, do it by executive action" pattern that could recur with a 2027 age-assurance proposal — worth raising directly with Rep. Levy.
- **SB 1546 (2026) — AI Companion chatbot law — ENACTED (Chapter 85, 2026 Oregon Laws).** Chief sponsor **Sen. Lisa Reynolds**; carried in the House by Rep. April Dobson; modeled on California SB 243 and paired with Washington HB 2225. Passed the Senate Feb 19, 2026 (26-1) and the House March 5, 2026 (52-0). **Signed by Gov. Kotek March 31, 2026** (a ceremonial signing with Lines for Life was held later); **effective Jan 1, 2027.** Primary source: Oregon Laws 2026, ch. 85 (oregonlegislature.gov/bills_laws/lawsstatutes/2026orLaw0085.pdf). Regulates "AI companions" (systems simulating sustained human-like relationships): requires clear disclosure that the user is interacting with AI; suicide/self-harm detection protocols with referral to 988 and YouthLine; "take a break" reminders; bans engagement-maximizing reward loops and emotional-manipulation tactics; bars sexually explicit content for minors; and applies extra protections when an operator **"has reason to believe" a user is a minor**. Enforced by a **private right of action ($1,000 per violation statutory damages); no AG enforcement**; annual operator reporting to the

Oregon Health Authority. (Follows Oregon **HB 2748** (2025, effective Jan 1, 2026), which targets AI agents posing as humans, notably nurses.)

  - **Why it matters for the age-verification conversation:** SB 1546's **"reason to believe a minor" inference standard** is an age-*assurance* trigger that already exists in Oregon law without any OS/app-store age-signal infrastructure — a concrete counter-example to "we need OS-level age verification to protect minors from AI." Its **private-right-of-action enforcement model** also mirrors Oregon SB 1516 (ALPR) and is likely the enforcement template a 2027 bill would copy.

Pass 2 — App-store models updated: both Utah and Louisiana DELAYED to 2027 [PRIMARY: state legislatures + AUTH-SECONDARY]

The app-store-accountability model is **legally contested and unsettled — not dead, and not safely "in retreat."** *(This is analysis, not a neutral fact; the underlying status of each law is below.)* The accurate pattern to take to Rep. Levy: district courts have repeatedly blocked these laws on First Amendment grounds, **but appellate courts are increasingly staying those injunctions and letting the laws operate while appeals proceed.** Texas's law is the cautionary example — blocked, then revived on appeal and now in force.

- **Utah SB 142 — first ASAA in the nation, since amended.** Signed by Gov. Cox March 26, 2025; effective May 7, 2025 with obligations originally due May 6, 2026. CCIA sued Feb 5, 2026 (First Amendment). While the suit was pending, Utah enacted **HB 498 (signed March 18, 2026)**, which (1) **pushed the compliance date to May 6, 2027**, (2) **removed AG enforcement entirely — now a private right of action only** (greater of $1,000/violation or actual damages, plus fees; PRA effective Dec 31, 2026), (3) expanded coverage to pre-installed apps, and (4) tightened developer data-use to three purposes only (enforce age restrictions, legal compliance, safety features; no third-party sharing — mirroring the Feb 2026 FTC statement). Because AG enforcement was gone, the AG agreed not to enforce and **CCIA voluntarily dismissed its challenge on April 21, 2026.** Net: Utah's law survives on paper but is now hard to challenge (no obvious defendant) and hard to enforce (private action only).
- **Louisiana — the packet's citation IS HB 570; also delayed to 2027.** Confirmed: the packet's "Louisiana App Store Accountability Act" link (legis.la.gov Law.aspx?d=1428945) is **HB 570 (2025), Act No. 481**, by Rep. Kim Carver, signed by Gov. Landry June 30, 2025, originally effective July 1, 2026. **Correction to the earlier "no developer safe harbor" note:** on **May 15, 2026, Louisiana enacted HB 977**, which (1) **delayed the effective date to July 1, 2027**, (2) clarified that **developers may rely on app-store-provided parental-consent signals** (removing standalone developer obligations — so there now is reliance protection), and (3) removed the emergency-services carve-out. Enforcement is by the AG (civil penalties up to $10,000/violation) with a 45-day cure period for first violations.
- **Bottom line for the model-bill table ($10):** Texas = **in effect since June 4, 2026** (district-court injunction stayed by the Fifth Circuit; merits still on appeal); Utah = amended to private-action-only, challenge dismissed, effective May 2027; Louisiana = delayed to July 2027; Alabama = effective Jan 1, 2027; California AB 1043 (OS model) = effective Jan 1, 2027 and **not yet challenged**. *Interpretive conclusion:* the OS-signal model (AB 1043) is the only one that has not drawn a First Amendment challenge —

plausibly because it transmits an age signal rather than directly blocking access. That may make it **more litigation-resistant**, which is a reason to treat it as a serious privacy concern, **not** a reason to assume it will or won't ultimately survive. Its constitutional, compelled-collection, and anonymous-speech questions are untested.

Oregon SB 141 interim testing — CONFIRMED [PRIMARY: ODE + OLIS]

- **SB 141, the 2025 Education Accountability Act** (helmed by Gov. Kotek; signed late July / Aug 1, 2025; passed largely on party lines). Sections 24–25 require districts and charter schools to **administer interim tests in math and language arts three times per year in grades K-8**, choose from a **State Board-approved list of up to four** vendors (selected via competitive RFQ; list released January 2026), and **review the data at least three times per year, including at a public board meeting.**
- **Timing:** the requirement begins in the **2026-27 school year**; districts that must switch to an approved vendor keep their current test through 2026-27 and must have the approved test in place **no later than August 30, 2027** — this is the precise "2027 deadline."
- Federally required summative tests (grades 3-8 and 11) are unchanged; families can opt out of summative tests easily. SB 141 did **not** fund the assessments. Approved/expected tools include MAP Growth, iReady, Smarter Balanced (Cambium), and Star — consistent with the packet's §7.
- **Why it matters:** confirms the §7 tension is real. A 2027 "no student-facing screens in K-5" or device-opt-out proposal collides directly with a *state-mandated, vendor-administered, three-times-a-year digital assessment* regime that itself launches in 2026-27. Any age/EdTech bill must reconcile with SB 141.

Oregon's existing privacy baseline — what a 2027 bill would build on [PRIMARY: ORS + Oregon DOJ/ODE]

This is the "what does Oregon already have" baseline the packet was missing. It reframes the Levy conversation from "should we protect kids?" to "what specific gap is left after these four layers?"

- **Oregon Student Information Protection Act (OSIPA), ORS 336.184 (2015 c.528 §2; effective July 1, 2016).** Governs ed-tech "operators." Pinned prohibitions, all in **ORS 336.184(3)(a)**: bans **selling student data — (3)(a)(D)**; bans **targeted advertising to students — (3)(a)(A)–(B)**; bans **amassing a non-educational student profile — (3)(a)(C)**; limits **disclosure of covered information — (3)(a)(E)**. Reasonable-security duty at **(4)(a)** and **deletion-on-school-request at (4)(b)**; **general-audience exemption at (9)** (does not reach general-audience sites/apps); **violation is an unlawful trade practice — (10), via ORS 646.607**, enforced by the Oregon AG (investigative-demand authority at ORS 646A.589). "Operator," "covered information," and "targeted advertising" are defined in **(2)**. **Implication:** much of the Safe School Technology Package's data-minimization / no-targeted-ads asks (packet §5–6) is *already Oregon law*; the package's genuine additions are the screen-time tiers, the registry, and the opt-out — not the core data protections.
- **Oregon Consumer Privacy Act (OCPA), SB 619 (2023), codified at ORS 646A.570–646A.589 (effective July 1, 2024 for-profit; July 1, 2025 nonprofit).** Minor

protections strengthened by **HB 2008 (signed June 3, 2025; substantive prohibitions effective Jan 1, 2026)**, which amends **ORS 646A.578**: a controller that knows or willfully disregards a consumer is **under 16** may not **sell** their data, **process it for targeted advertising**, or **profile** them in furtherance of decisions with legal/similarly significant effects — **with no consent exception** (previously 13–15, consent-permitted, until 12/31/2025). Sale of **precise geolocation** (within a 1,750-ft radius) is also barred regardless of age; "sale" is defined at **ORS 646A.570(17)**. Applicability/thresholds at **ORS 646A.572(1)**; entity/data exemptions at **646A.572(2)**. **Correction to an earlier draft note:** Oregon does **NOT** exempt higher-education institutions (unusual among state privacy laws); the exemptions are entity/data-specific (e.g., HIPAA, GLBA, FERPA-regulated data, certain government bodies), not a blanket education carve-out. **No private right of action — ORS 646A.586**; exclusive Oregon AG enforcement; civil penalty up to $7,500/violation; the 30-day cure period sunset Jan 1, 2026. *(One tracker lists a Sept 26, 2025 general effective date for the 2025 amendments; the operative minor/geolocation prohibitions run from Jan 1, 2026 per the law-firm analyses — confirm against the enrolled HB 2008 if the exact date matters.)*

- **SB 1546 (AI companions, eff. Jan 1, 2027)** and **HB 2748 (AI-posing-as-human, eff. Jan 1, 2026)** — already logged above.
- **FERPA (federal)** plus Oregon State Board record rules (e.g., OAR 581-022-2260) govern education records. **Oregon Consumer Information Protection Act (OCIPA), ORS 646A.600–646A.628** governs data security and breach notification (relevant to the age-data breach-risk argument): "breach of security" is defined at **646A.602**; the **breach-notification duty is ORS 646A.604** — notice to affected consumers "without unreasonable delay, but not later than **45 days**" after discovery (**646A.604(3)(a)**), notice to the **Attorney General when a breach affects more than 250 Oregon consumers** (**646A.604(1)(b)**), and notice to nationwide consumer-reporting agencies when a breach affects **more than 1,000** consumers (**646A.604(6)**); the separate **affirmative duty to maintain reasonable safeguards is ORS 646A.622**. Violations of 646A.604 or 646A.622 are unlawful trade practices (enforced by the AG via ORS 646.607), with penalties up to **$1,000 per violation and up to $500,000 for a continuing violation**. Personal information includes biometric identifiers (added by SB 684 (2019), eff. Jan 1, 2020). **Why it matters:** any OS-level age-attribute layer or app-store age database is exactly the kind of sensitive personal-information store OCIPA already regulates — so the §15 "breach notification" safeguard is partly *already Oregon law*, and an age-signal infrastructure measurably enlarges Oregonians' breach-exposure surface.
- **Takeaway for the memo:** Oregon already regulates student data (OSIPA), minors' commercial data to age 16 (OCPA), AI companions (SB 1546), and education records (FERPA). A 2027 OS/app-store age-verification bill is **not** filling an empty field — so the burden is on sponsors to identify the *specific* harm these layers leave unaddressed, and to show that an age-signal infrastructure is the least-restrictive way to address it.

Still to verify in later passes

- **[Source-checked]** Google Play Age Signals API and Apple Declared Age Range API have been source-checked against the primary developer documentation in the technical companion (`os_age_signal_technical_analysis.md`). Remaining technical

work: Microsoft/Xbox, Meta/Snap/TikTok/Discord/Roblox, browser-level relay behavior, and live-doc checks before formal use.

- **[Needs primary pin-cite]** Whether **HB 2008** (the 2025 OCPA minor-protection amendment) carries other provisions relevant to an age-assurance bill.
- **[Needs status update]** California AB 1043 litigation, if any, as it nears its Jan 1, 2027 effective date; and AB 1856's Senate progress.
- **[Resolved]** SB 1546 signing date — **March 31, 2026; Chapter 85, 2026 Oregon Laws** (see source table).

1A-Sources. Consolidated Source Table (Pass 1–2)

Confidence labels as defined above. "Primary?" = whether the cited source is the statute/court order/agency record itself (Y) or reputable secondary reporting (N). Where a row says **Needs primary pin-cite**, pull the underlying section/order before quoting in a Levy memo or testimony.

#	Claim	Best source	Primary?	Confidence	Notes / action
1	**HB 3696 (OR 2025)** died — referred to House Commerce & Consumer Protection 2/27/2025, no further action; sponsor Rep. Reschke	OLIS measure history; LegiScan	Y/N	Primary-source checked	Confirm "died" via OLIS sine die status page for the pin-cite
2	**AB 1043 (CA)** — Civil Code Title 1.81.9, **§§1798.500 et seq.** (Ch. 675, Stats. 2025); OS interface at setup, 4 brackets (<13, 13–<16, 16–<18, 18+), developer	CA Civil Code §§1798.500–.503; leginfo.legislature.ca.gov	Y	Primary-source checked	Self-report only (no ID/biometric), unlike TX/UT; AG enforcement; good-faith safe harbor

#	Claim	Best source	Primary?	Confidence	Notes / action
	"actual knowledge" clause, penalties **§1798.503** ($2,500 negligent / $7,500 intentional per child); eff. 1/1/2027 (legacy devices by 7/1/2027)				
3	**AB 1856 (CA)** — amends the Digital Age Assurance Act (Civil Code Title 1.81.9 / §§1798.500 et seq.); passed Assembly 68–1 (5/28/2026), in Senate, **not yet law**. Per the Legislative Counsel's Digest: requires the OS age signal to be provided to a **covered application store, application developer, browser provider,**	CA Legislative Counsel's Digest (AB 1856); EFF (5/29/2026)	Y/N	Secondary-source checked (digest-level)	Exact new Civil Code section numbers will settle only when chaptered; status still moving

#	Claim	Best source	Primary?	Confidence	Notes / action
	OR internet website operator; deletes the "user" definition; recasts the "actual knowledge" clause to reach a **developer or internet website operator** "when the user accesses the application from a specified device" (and **deletes** the current "across all platforms … even if willfully disregards" language); open-source carve-out				
4	**Texas SB 2420** signed 5/27/2025; PI granted 12/23/2025 (Pitman, W.D. Tex.); stay denied 5/6/2026; 5th Cir. stayed injunction;	W.D. Tex. orders (1:25-cv-01660); 5th Cir. (No. 25-51073); TX AG release; trade press	Y/N	Needs status update	Fast-moving — re-confirm 5th Cir. docket before citing

#	Claim	Best source	Primary?	Confidence	Notes / action
	in effect 6/4/2026; merits pending				
5	**Utah SB 142** (Utah Code Title 13, Ch. 76, §§13-76-101 et seq.); **HB 498** (signed 3/18/2026) delayed key provisions to **5/6/2027**, **removed AG enforcement → private action only** (greater of actual damages or $1,000/violation + costs, §13-76-402 area), expanded to pre-installed apps, repealed Division rulemaking (§13-76-301); CCIA challenge dismissed 4/21/2026	Enrolled HB 498 (le.utah.gov); Utah Code Title 13 Ch. 76	Y	Primary-source checked	Developer data-use limited to 3 purposes (§13-76-401 area), aligning w/ Feb 2026 FTC statement
6	**Louisiana — HB 977 (2026), enacted as Act No. 185**, signed 5/15/2026 by	Enrolled HB 977 / Act 185 (legis.la.gov d=1471343, d=1475238)	Y	Primary-source checked	Packet's old "Louisiana ASAA" link (d=1428945 = Act 481/R.S. 51:1773) is now

#	Claim	Best source	Primary?	Confidence	Notes / action
	Rep. Beaullieu: **repeals Act 481 (2025)** before it took effect and **reenacts the ASAA as R.S. 51:1771–1775** (Title 51, Ch. 20-A, new Part II), effective **July 1, 2027**; lets developers rely on app-store signals; removed the emergency-services carve-out				repealed/superseded
7	**Alabama HB 161 (2026), Act 2026-59** (Reps. Sells/Mooney; Sen. Chambliss), signed by Gov. Ivey **Feb 17, 2026**; eff. **Jan 1, 2027** (existing accounts verified by **Oct 1, 2027**, §2(a)); 4 age categories (<13/13–<16/16–<18/18+, §1(2)); covers pre-installed apps	Engrossed HB 161 (alison.legislature.state.al.us) — full text read	Y	Primary-source checked — **conflicts resolved**	**$7,500 confirmed (PACMap's $10,000/$50,000 is wrong); NO express private right of action — AG exclusive (the bill caption's "parents authorized to bring civil action" is not in the operative text)**

#	Claim	Best source	Primary?	Confidence	Notes / action
	incl. browsers/search/messaging (§1(18)); **AG rulemaking** for verification; **AG has "exclusive jurisdiction," penalty up to $7,500/violation, punitive damages possible ($11)**				
8	**Free Speech Coalition v. Paxton**, No. 23-1122, 606 U.S. ___ (2025), slip op. (6/27/2025), 6–3; **intermediate scrutiny holding at slip op. 13**; "adults have no First Amendment right to avoid age verification" at **slip op. 18**; strict-scrutiny limiting principle (laws banning both	SCOTUS slip opinion, No. 23-1122	Y	Primary-source checked	Pin-pages confirmed; safe to quote the holding language with slip-op cites

#	Claim	Best source	Primary?	Confidence	Notes / action
	adults and minors) at **Pp. 21–28**; holding limited to obscene-as-to-minors content				
9	**SB 1546 (OR 2026)** AI-companion law; Senate 26-1, House 52-0; **signed ~3/31/2026; Chapter 85, 2026 Oregon Laws; effective 1/1/2027**; **§1** = definitions + obligations (AI disclosure, suicide/self-harm protocol w/ 988/YouthLine referral, minor protections, annual public report); **§2** = private right of action (ascertainable loss → damages + injunctive relief; $1,000/violation); no AG enforcement	Enrolled SB 1546 / Oregon Laws 2026 ch. 85 (OLIS)	Y	Primary-source checked	**Enrolled numbering: §1 obligations, §2 private action.** Some analyses (Baker Botts) cite an earlier printing (§2 def, §4 report, §6 PRA) — use the enrolled/Ch. 85 numbers

#	Claim	Best source	Primary?	Confidence	Notes / action
10	**HB 2251 (OR 2025)** school personal-electronic-device bill; left in Senate Education committee (died)	OLIS measure page	Y	Primary-source checked	Confirms HB 2251 *is* the cell-phone bill
11	**Executive Order 25-09** (Kotek, 7/2/2025) — districts adopt bell-to-bell policies by 10/31/2025, in effect 1/1/2026	Governor's Office announcement; EO text	Y	Primary-source checked	"Legislate-then-executive-fallback" is *interpretive* framing, not fact
12	**SB 141 (OR 2025), §§24–25** — interim math/ELA tests 3×/yr K-8; State Board list of up to 4 vendors (RFQ); review 3×/yr incl. public board meeting; transition by 8/30/2027; begins 2026-27	Enrolled SB 141 (OLIS); ODE Interim Tests FAQ	Y	Primary-source checked	ODE FAQ expressly cites "Sections 24 and 25"; §27 repealed ORS 337.065; unfunded
13	**OSIPA, ORS 336.184** — bans selling student data **(3)(a)(D)**,	ORS 336.184 (2015 c.528 §2)	Y	Primary-source checked	Subsections pinned; deletion-on-request confirmed at

#	Claim	Best source	Primary?	Confidence	Notes / action
	targeted ads to students **(3)(a)(A)–(B)**, non-educational profiling **(3)(a)(C)**; general-audience exemption **(9)**; UTPA enforcement **(10)/ORS 646.607**				ORS 336.184(4)(b)
14	**OCPA, ORS 646A.570–.589**; **HB 2008** amends **ORS 646A.578** — no sale/targeted-ad/profiling of under-16 data, no consent exception, eff. 1/1/2026; no PRA **(646A.586)**	ORS 646A.570–.589; HB 2008 (2025)	Y	Primary-source checked	Higher-ed is **not** exempt (corrected); confirm exact HB 2008 effective-date wording
15	**OCIPA, ORS 646A.600–.628** — breach def **646A.602**; 45-day notice **646A.604(3)(a)**; AG notice at 250+ **646A.604(1)(b)**; CRA notice at 1,000+ **646A.604(6)**	ORS 646A.600–.628	Y	Primary-source checked	Penalties to $500k continuing violation; biometrics covered since 2019 (SB 684)

#	Claim	Best source	Primary?	Confidence	Notes / action
	; safeguards duty **646A.622**				
16	**FTC COPPA Enforcement Policy Statement** (2/25/2026) — no COPPA enforcement vs. general/mixed-audience operators collecting PI *solely* for age determination, if six conditions met: (1) purpose limitation, (2) prompt deletion, (3) vetted third parties w/ written assurances, (4) notice to parents/children, (5) reasonable security, (6) reasonable accuracy	FTC PDF (coppa-age-verification-policy-statement.pdf); FTC press release	Y	Primary-source checked	Not a rule change; child-directed sites excluded; mirrors §15 safeguards — cite as the federal floor

Whenever a row above is used in the Levy memo, convert "Needs primary pin-cite" to an actual section/page citation first. Do not carry "Secondary-source checked" claims into testimony as settled.

1A-Pins. Statutory Pin-Cite Progress (Pass 3, June 17, 2026)

Deliberate, primary-source pin-cite work — no deadline pressure, building the foundation first. Done so far:

- **OSIPA — ORS 336.184**, pinned to subsection: selling student data **(3)(a)(D)**; targeted advertising **(3)(a)(A)–(B)**; non-educational profiling **(3)(a)(C)**; disclosure limits **(3)(a)(E)**; operator affirmative duties **(4)** — reasonable security **(4)(a)** and **deletion of a student's covered information within a reasonable time on the school/district's request (4)(b)**; general-audience exemption **(9)**; UTPA enforcement **(10)** via **ORS 646.607**; definitions **(2)**; enacted **2015 c.528 §2**, eff. **July 1, 2016**. *(Source: oregonlegislature.gov/bills_laws/ors/ors336.html; cross-checked on Justia/FindLaw/Public.Law — deletion duty confirmed at (4)(b).)*
- **OCPA — ORS 646A.570–.589**; **HB 2008** amends **ORS 646A.578** (under-16 sale/targeted-ad/profiling ban, no consent exception, eff. Jan 1, 2026); "sale" defined **646A.570(17)**; applicability **646A.572(1)**; exemptions **646A.572(2)** (higher ed **not** exempt — earlier draft corrected); no private right of action **646A.586**. *(Source: ORS 646A; Oregon DOJ FAQs; corroborated by DWT, Proskauer, CommLaw, Hunton analyses.)*
- **Free Speech Coalition, Inc. v. Paxton — No. 23-1122, 606 U.S. __ (2025), slip op. (U.S. June 27, 2025)**, decided 6–3 (Thomas, J., for the Court; Kagan, J., dissenting, joined by Sotomayor & Jackson). **Pinned holding pages:** the syllabus "Held" — *"H. B. 1181 triggers, and survives, review under intermediate scrutiny because it only incidentally burdens the protected speech of adults" (Pp. 5–36)*; the operative scrutiny holding is at **slip op. 13** ("Applying our precedents, we hold that intermediate scrutiny applies"); *"adults have no First Amendment right to avoid age verification"* at **slip op. 18**; and the **limiting principle** — strict scrutiny in this area has applied only to laws that **"banned both minors and adults"** from the speech (distinguishing *Sable*, *Playboy*, *Reno*, *Ashcroft*) — at **Pp. 21–28**. Intermediate-scrutiny standard drawn from *Turner Broadcasting*. *(Source: SCOTUS slip opinion, supremecourt.gov/opinions/24pdf/23-1122_3e04.pdf; pin-pages cross-checked against Constitution Annotated, which cites slip op. 5, 13, 18, 23.)*
- **SB 1546 — Chapter 85, 2026 Oregon Laws** (enrolled text, OLIS 2026R1). Internal structure pinned: **Section 1** carries the definitions and the operative obligations — defines "artificial intelligence companion" (a system using AI/generative AI/emotion-recognition algorithms designed to simulate a sustained human-like platonic/intimate/romantic relationship by (a) retaining info to personalize and drive ongoing engagement, (b) asking unprompted questions on emotional topics, and (c) sustaining ongoing personal dialog); requires AI-disclosure when a reasonable person would think they were talking to a human; mandates a suicide/self-harm detection-and-prevention protocol with referral to a crisis lifeline (988 / YouthLine); applies extra duties when the operator "has reason to believe" a user is a minor; and requires an **annual public report**. **Section 2** is the **private right of action** — an individual who suffers "an ascertainable loss of money or property or other injury in fact as a result of an operator's violation of section 1" may sue for damages and injunctive relief; statutory damages **$1,000/violation**; **no AG enforcement**. **Numbering caution:** the enrolled/Chapter 85 text uses §1 (obligations) and §2 (private action); some published analyses (e.g., Baker Botts) cite an earlier printed version numbering definitions at §2, reporting at §4, and the private action at §6 — cite the enrolled Chapter 85 numbers, not the earlier draft's. *(Source: Enrolled SB 1546 / Oregon Laws 2026 ch. 85, OLIS; Miller Nash, Troutman, Baker Botts analyses.)*

- **OCIPA — ORS 646A.600–.628**: breach definition **646A.602**; notification duty **646A.604** (45-day deadline **(3)(a)**; AG notice >250 **(1)(b)**; nationwide-CRA notice >1,000 **(6)**; law-enforcement delay **(3)/(7)**; federal-overlap exemptions **(9)**); reasonable-safeguards duty **646A.622**; SSN protections **646A.620**; enforcement via UTPA (ORS 646.607), penalties to **$1,000/violation, $500,000 continuing**. History: SB 583 (2007) → SB 601 (2015) → SB 1551 (2018) → SB 684 (2019, biometrics added, eff. 1/1/2020). *(Source: ORS 646A.600–.628 via oregon.public.law & Justia; Oregon DOJ; Perkins Coie OR breach chart.)*
- **SB 141 — 2025 Education Accountability Act, §§24–25** (ODE FAQ expressly attributes the interim-test mandate to "Sections 24 and 25"): districts/charters must (1) select an interim test from the **State Board-adopted list of up to four** (competitive RFQ; list released Jan 2026), (2) administer **math + ELA interim tests three times per year in grades K-8**, and (3) review the data **at least three times per year, including at a public meeting** of the superintendent and school board. Begins **2026-27**; transition to an approved vendor required **no later than August 30, 2027**. **§27** repealed **ORS 337.065** (publisher fees). Federally-required summatives (grades 3-8, 11) unchanged; not funded by the bill. *(Source: Enrolled SB 141, OLIS 2025R1; ODE "Interim Tests" FAQ; ODE SB 141 implementation report, Dec 2025.)*
- **AB 1043 (CA Digital Age Assurance Act) — Civil Code Title 1.81.9, §§1798.500 et seq.** (Ch. 675, Stats. 2025; eff. 1/1/2027, legacy devices by 7/1/2027): OS-provider account-setup interface to "indicate" birth date/age (self-report — no ID/biometric); 4 minimum brackets (under 13 / 13–<16 / 16–<18 / 18+); developer **"actual knowledge … across all platforms … even if the developer willfully disregards the signal"**; data-minimization + no-third-party-share; penalties **§1798.503** ($2,500 negligent / $7,500 intentional per affected child); CA AG enforcement; good-faith safe harbor; carve-outs for broadband/telecom/physical products. *(Source: CA Civil Code §§1798.500–.503 via leginfo.legislature.ca.gov; corroborated by Hunton, Kelley Drye, TrueVault, EFF.)*
- **FTC COPPA Enforcement Policy Statement (Feb 25, 2026)** — pinned to the FTC's own document. The FTC will not bring a COPPA Rule enforcement action against a **"Relevant Operator"** (general-audience or mixed-audience site/service — **not** child-directed) that collects/uses/discloses personal information for the **sole purpose of determining a user's age ("Age Verification Purposes")** without first obtaining verifiable parental consent, **provided** the operator: (1) **uses/discloses the info only to determine age** (purpose limitation); (2) **does not retain it longer than necessary and deletes it promptly**; (3) **discloses it only to third parties** reasonably determined capable of maintaining confidentiality/security/integrity, **with written assurances**; (4) **gives clear notice to parents and children**; (5) **employs reasonable security**; and (6) **takes reasonable steps to ensure the method is reasonably accurate** — and complies with the COPPA Rule in every other respect. Not a rule amendment (no substantive rights; FTC retains case-by-case enforcement); a formal COPPA Rule review on age verification is signaled; 2025 COPPA Rule amendments compliance deadline **April 22, 2026**. **Key point for BPA:** these six federal conditions essentially *are* the §15 safeguards — cite the FTC statement as the federal floor any Oregon bill should meet or exceed, and note the FTC itself frames purpose-limitation + prompt-deletion as mitigating the "honey pot" breach risk. *(Source:*

ftc.gov/system/files/ftc_gov/pdf/coppa-age-verification-policy-statement.pdf; FTC press release 2/25/2026.)

Out-of-state app-store laws (the four bills) — pinned:

- **Utah HB 498 (2026 G.S.; signed by Gov. Cox 3/18/2026)** — amends the Utah App Store Accountability Act at **Utah Code Title 13, Chapter 76** (amends §§13-76-101, -201, -202, -401, -402, -404; **repeals §13-76-301** Division rulemaking). **Delays key operational provisions to May 6, 2027**; **removes Utah AG enforcement, leaving only a private right of action** (a harmed minor or parent/guardian may recover the greater of actual damages or **$1,000/violation plus costs**); **expands coverage to pre-installed applications**; narrows the "significant change" trigger; **limits developer use of age-category data to three purposes** (enforce age restrictions / legal compliance / safety features) with no third-party sharing — which the bill's analysts note aligns with the Feb 2026 FTC statement; requires "commercially available methods … reasonably designed to ensure accuracy" with parental attestation for minors. CCIA's challenge to the original SB 142 was **voluntarily dismissed 4/21/2026** once AG enforcement was removed (mootness). *(Source: Enrolled HB 498, le.utah.gov; FKKS, Wiley, Loeb, Alston analyses.)*
- **Louisiana HB 977 (2026 R.S.; Rep. Beaullieu; enacted as Act No. 185; signed 5/15/2026)** — **repeals Act No. 481 of 2025 before it took effect** ("Act No. 481 … shall not become effective") and **reenacts the ASAA as R.S. 51:1771–1775** (Title 51, Chapter 20-A "Protection of Children's Internet Data Online," new **Part II "Protection of Children on Applications"**), **effective July 1, 2027**. House 94-0 (4/22/2026); Senate 36-0 (5/11/2026). Refinements: **developers may rely on app-store-provided age signals** (drops the prior "and other sources" duty); clarifies developers may rely on app-store info for parent-account affiliation and verifiable parental consent; **removes the emergency-services (911/crisis-line) carve-out** — a change widely read as defensive against the content-based-exemption First Amendment argument. Note: the packet's old "Louisiana ASAA" citation (legis.la.gov d=1428945 = R.S. 51:1773 as enacted by Act 481) is now **superseded**. *(Source: Enrolled HB 977 / Act 185, legis.la.gov d=1471343 & d=1475238; Alston analysis; NetChoice opposition testimony.)*
- **Alabama HB 161 (2026 R.S.; Reps. Sells/Mooney, Sen. Chambliss; Act 2026-59; signed by Gov. Ivey Feb 17, 2026)** — fourth state ASAA; **effective Jan 1, 2027**; four age categories (§1(2): <13 / 13–<16 / 16–<18 / 18+); **uniquely retroactive** (existing accounts as of 10/2/2026 must be categorized/verified by **10/1/2027**, §2(a)); covers **pre-installed apps** (§1(18) — expressly includes browsers, search engines, messaging apps; excludes core OS functions/drivers/phone+settings); requires app-store providers to **encrypt** age-verification data (§6(2)) and limits developer use of age-category data to three purposes (§9(a)(3)); provides for **Alabama AG rulemaking** on verification methods. **Conflicts now RESOLVED against the engrossed text (full text read): §11 sets a civil penalty of up to $7,500/violation** (not the $10,000/$50,000 some trackers report — PACMap is wrong) and gives the **Attorney General "exclusive jurisdiction to bring an action,"** enforced as a deceptive trade practice under **Title 8, Chapter 19 (§8-19-1 et seq.)**, with possible punitive damages — i.e., **no express private right of action**; the bill's official caption ("parents authorized to bring civil action") does **not** match the operative text and appears vestigial. Signing date **Feb 17, 2026** (Loeb +

LegiScan "Enacted 2/17"); the "March 9" in one analysis is an article-date artifact. *(Source: Engrossed HB 161 §§1–11, alison.legislature.state.al.us; Hunton & Troutman both confirm "no express private right of action.")*

- **California AB 1856 (2026; Wicks)** — amends the Digital Age Assurance Act (Civil Code Title 1.81.9); **passed the Assembly 68-1 on 5/28/2026**, now in the Senate, **not yet enacted**. Per the **Legislative Counsel's Digest**, it would require the OS age signal to be provided not just to app stores but to a **covered application store, application developer, browser provider, OR internet website operator** — the OS-to-browser-to-website expansion that is the file's strongest scope-creep warning. It would also **delete the current "user" definition** ("a child that is the primary user of a device") and **recast the "actual knowledge" clause**: a developer **or internet website operator** that receives a signal is deemed to have actual knowledge "when the user accesses the application from a specified device," and the bill **deletes** AB 1043's broader "across all platforms … and points of access … even if the developer willfully disregards the signal" language. (So the net effect is *narrower* cross-platform knowledge but *broader* recipients — worth stating precisely rather than only as "expansion.") Adds the **open-source carve-out** (excludes OS distributed under copy/redistribution/modification licenses). **Status: secondary/digest-level only** — exact new Civil Code section numbers won't be fixed until the bill is chaptered. *(Source: CA Legislative Counsel's Digest for AB 1856 via CalMatters Digital Democracy; EFF (5/29/2026).)*

Pin-cite batch complete (Pass 3–5). Every item from the prior "next batch" and short-list is now logged above and pinned to the statute, code section, court order, or agency document. **Short-list items resolved this pass:** the **Alabama Act 2026-59 conflicts** (penalty = $7,500/violation per §11; AG exclusive jurisdiction, no express private right of action; signing 2/17/2026 — PACMap's $10,000/$50,000 and the "parents may sue" caption are not in the operative text); **AB 1856** browser/website expansion (per the Legislative Counsel's Digest — recipients now include browser providers and internet website operators; the cross-platform actual-knowledge language is deleted; still pre-enactment so section numbers will settle at chaptering); **SB 1546 / Ch. 85** internal numbering (§1 obligations, §2 private action — earlier-draft citations like Baker Botts' §2/§4/§6 are stale); **OSIPA deletion-on-request** at **ORS 336.184(4)(b)**; and **FSC v. Paxton** pin-pages (scrutiny holding at slip op. 13; limiting principle at Pp. 21–28).

The only genuinely-open *statutory/legal* primary item is the **AB 1856 enrolled text** — and that can't be pinned to final section numbers until the bill is chaptered (it's still in the California Senate). Every other statute, court order, and agency document a Levy memo would rely on is now citable to primary source. **On the *technical* side,** Google Play Age Signals and Apple Declared Age Range have now been source-checked against the primary developer documentation in the technical companion (`os_age_signal_technical_analysis.md`); remaining technical work is Microsoft/Xbox, Meta/Snap/TikTok/Discord/Roblox, browser-level relay behavior, and live-doc checks before formal use.

---

2. Core Distinction: Do Not Collapse These Policy Models

The central issue is that the term **"age verification"** is being used to describe several different architectures. These should be separated before any Oregon bill is drafted.

Track	What it covers	Why it matters
A. School technology / EdTech package	Screen limits, device opt-outs, school technology registry, school device rules, EdTech procurement, AI restrictions, caregiver notice, student data privacy	This is the package shared from Distraction-Free Schools. It is about schools, school-issued devices, and EdTech procurement.
B. App-store age verification / app-store accountability	App stores verify age, assign age categories, obtain parental consent for minors, share age/consent signals with developers	This is the Oregon HB 3696 / Texas / Utah / Louisiana / federal App Store Accountability model.
C. Operating-system age signals	OS providers collect or prompt for age/birthdate at device/account setup and transmit age-bracket signals to apps through APIs	This is closest to California AB 1043 / Digital Age Assurance Act and is the highest-priority concern if Oregon is discussing "OS-level age verification."
D. Privacy-preserving proof-of-age credential	User proves they are over a threshold, such as 18+, without disclosing exact birthdate, identity, or other unnecessary information	This is closer to the EU age-verification/wallet approach and may be a useful alternative model.

Key Question for Rep. Levy

> When you say Oregon is considering "operating-system age verification," do you mean a California AB 1043-style law requiring operating systems to collect age or birthdate and send age-bracket signals to apps, an Oregon HB 3696-style app-store parental-consent bill, a school technology bill, or something new?

---

3. Sources Provided by Jonathan

These are the links and materials Jonathan provided directly in this research thread.

3.1 Distraction-Free Schools / Safe School Technology Package

- Main site: https://www.distractionfreeschools.com

Jonathan was shown or given text from a document titled:

SAFE SCHOOL TECHNOLOGY PACKAGE

The package included three model bills:

1. **Safe School Technology Act**
2. **An Act to Create a School Technology Registry**
3. **An Act to Ensure an Electronic Device Opt-Out**

3.2 Oregon Department of Education Interim Tests

- ODE Interim Tests page: https://www.oregon.gov/ode/accountability/pages/interim-tests.aspx

Relevance: Oregon's SB 141 / Education Accountability Act implementation appears to require K–8 interim testing in math and English language arts three times per year using approved vendors/tests. This may conflict with or create exceptions to any proposal limiting student-facing screen time in K–5 or K–8.

3.3 Lake Oswego School District Granicus Video

- Lake Oswego clip: https://loswegok12.granicus.com/player/clip/973?view_id=3&redirect=true

Relevance: This appears to be a Lake Oswego School District board meeting video with agenda items relevant to school technology and educational data, including a technology update and educational data discussion. It should be reviewed or transcribed later if it becomes an Oregon implementation case study.

---

4. Links Embedded in the Safe School Technology Package

These were included in the pasted Safe School Technology document and should be source-checked before public use.

Student Data / Privacy / Surveillance Claims

- Internet Safety Labs, 2022 K–12 EdTech Safety Benchmark, National Findings Part 1: https://internetsafetylabs.org/wp-content/uploads/2022/12/2022-k12-edtech-safety-benchmark-national-findings-part-1.pdf
- Human Rights Watch, online learning products enabled surveillance of children: https://www.hrw.org/news/2022/07/12/online-learning-products-enabled-surveillance-children
- Internet Safety Labs, School Mobile Apps Student Data Sharing Behavior: https://internetsafetylabs.org/resources/reports/spotlight-report-1-school-mobile-apps-student-data-sharing-behavior/
- Internet Safety Labs, 2022 K–12 EdTech Safety Benchmark Findings Report 2: https://internetsafetylabs.org/wp-content/uploads/2023/06/2022-K12-Edtech-Safety-Benchmark-Findings-Report-2.pdf

- New York Times, student privacy / Illuminate hack: https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html

Screen Time / Health / Learning Claims

- Education Week Market Brief, student screen time / EdTech use: https://marketbrief.edweek.org/meeting-district-needs/how-much-time-are-students-spending-using-ed-tech/2022/03
- CBS News, digital devices and children's eyesight / nearsightedness: https://www.cbsnews.com/news/digital-devices-screen-time-damaging-childrens-eyes-vision/
- Fondation Reboot, NAEP data update memo: https://www.fondation-reboot.org/wp-content/uploads/_docs/2019_NAEP_Data_Update_Memo.pdf
- PostPress, importance of paper in learning and literacy: https://postpressmag.com/articles/2023/the-importance-of-paper-in-learning-and-literacy/
- Hechinger Report, education research bias / developer studies: https://hechingerreport.org/the-dark-side-of-education-research-widespread-bias/

AI in K–12 Education Claims

- Stanford SCALE, 2026 report, evidence base on AI in K–12: https://scale.stanford.edu/sites/default/files/The%20Evidence%20Base%20on%20AI%20in%20K-12%20Report.pdf
- Brookings, AI in students' education / prosper, prepare, protect: https://www.brookings.edu/articles/a-new-direction-for-students-in-an-ai-world-prosper-prepare-protect/

---

5. Safe School Technology Package — Extracted Summary

The pasted package should be treated as a **school technology / EdTech safety package**, not the same thing as operating-system age verification. It may be politically connected to the same broader child-safety agenda, but it is technically and legally different.

5.1 Findings Claimed in the Package

The package states that online and digital products marketed to schools often provide unsafe, ineffective, or inappropriate experiences and collect/share student data without appropriate consent.

It identifies concerns including:

- Technology companies marketing commercial products as educational with little accountability.
- Children being given devices without proof of developmental appropriateness.
- Collection and monetization of student data for non-educational purposes.
- Advertising, gamification, AI, chat features, and addictive design in classrooms.
- Caregivers being excluded from decisions about children's digital exposure.
- Insufficient privacy and safety protections.
- Increased screen time, with alleged links to psychological and physical health risks.
- EdTech ineffectiveness or weak learning-outcome evidence.
- Uncertain evidence base for AI use in K–12 education.

5.2 Bill 1: Safe School Technology Act

Purpose: Ensure schools remain focused on effective, developmentally appropriate instruction grounded in evidence-based practices and respectful of student well-being and privacy.

Key Definitions

The bill defines or uses terms including:

- Addictive design feature
- Caregiver
- Compliance
- Digital device
- One-to-one device model
- Safety
- School-issued device
- School technology
- School technology provider
- Screen-free
- Social media
- Student-facing screens
- Student personal information
- Targeted advertising

Device Introduction Model

The package proposes a tiered school technology framework:

Grades Pre-K–5

- No student-facing screen time.
- All instruction hands-on and print-based.
- Narrow exception for required online assessment preparation beginning in third grade: three 20-minute device sessions during the week before assessment, using a cart or computer lab.

- Homework must not require internet or screen devices.
- Age-appropriate media literacy instruction.
- Teacher use of classroom screens/smartboards remains allowed for group instruction.

Grades 6–8

- Shared devices through carts or designated computer rooms.
- Device use must be teacher-led, actively supervised, and for defined academic purposes.
- Settings must restrict non-instructional content.
- Online textbooks allowed only if no other option exists.
- Print-based and analog methods prioritized.
- Homework must not require internet or screens.
- Digital devices remain on school property.
- Media literacy instruction required.

Grades 9–12

- Shared devices through carts or computer rooms.
- Device use must be teacher-led, actively supervised, and for defined academic purposes.
- Settings must restrict non-instructional content.
- One-to-one devices allowed with caregiver opt-in.
- Take-home devices allowed with caregiver opt-in.
- Print/analog methods prioritized.
- Online textbooks allowed only when no other option exists.
- Media literacy instruction required.

Digital Device Safety Standards

Before providing a school-issued device, districts would need to:

- Enable screen-time settings so caregivers can track/support healthy use.
- Disable cameras to reduce cyberbullying/sensitive image sharing.
- Block social media apps.
- Configure default privacy/safety settings to highest levels.
- Delete previous user personal information before reuse.

Transparency Requirements

Before each school year, districts must provide caregivers:

- Information about digital devices their child will use.
- List of software programs their child will be expected to use.
- Recent data regarding harms of excessive screen time and online harms.

School Technology Standards

The Attorney General, in collaboration with the state education authority, would set and annually review standards for:

- Safety
- Effectiveness
- Legal compliance

Student-facing school technology would be prohibited from having:

- Geolocation
- Generative or conversational AI
- Targeted advertisements
- Engagement maximization systems
- Access to adult strangers
- Addictive design features
- Features that interfere with learning or reduce focus

Effectiveness Requirements

School technology must be independently verified by an objective third party to provide instructional benefits equal to or greater than non-digital methods.

Compliance / Privacy Requirements

Providers would have to guarantee items including:

- COPPA Safe Harbor Certification
- Clear product information readable at a seventh-grade level
- Caregiver notice of information collected, maintained, used, and shared
- Access and correction rights
- Deletion within seven days on request by school, district, or caregiver
- Electronic copy of student personal information
- Successor/third-party compliance with district contract
- Recourse for breach or contract violation
- No privacy policy changes without caregiver and district consent
- No data transfer to successor entity without caregiver and district consent

Data Minimization

Providers may not:

- Collect data not essential to the product's educational function.
- Collect sensitive health information.
- Sell, share, or rent data to third parties.
- Create student profiles for non-educational uses, including targeted advertising, disciplinary actions, or discrimination.

Social Media Rules

Districts would need policies that:

- Prevent students from being forced to create social media accounts.
- Prohibit staff/volunteers from using social media for student-facing communication.
- Prohibit student access to social media and gaming apps during school day and school activities.
- Prohibit social media/gaming apps on school-issued devices.
- Block access to social media/gaming apps on school internet connections.

YouTube teacher-use exception:

- Teacher may show a YouTube video on classroom screen for educational purposes.
- Videos must be pre-vetted.
- Autoplay must be off.
- Ad blocker must be enabled.
- Students may not be asked to research using YouTube.

Media Literacy Standards

K–12 curriculum would include age-appropriate instruction about:

- Social media risks
- AI risks
- Emerging digital/online technologies
- Manipulative and addictive design
- Safe and appropriate internet use
- Critical thinking
- Risk-benefit analysis
- Mental/physical health consequences

Curriculum must not require social media or school-issued devices and must be developed or purchased from independent sources without financial ties to tech companies that benefit from student technology use.

5.3 Bill 2: School Technology Registry

The proposed registry bill would require school technology products used by districts to register with the Attorney General's office.

Providers must:

- File self-attestation that product meets safety, efficacy, and privacy obligations.
- Commit to notifying AG and district of changes that cause noncompliance.
- Acknowledge AG or state education authority audit rights.

Violations may include:

- Knowingly false self-attestation.
- Significant product change without proper reporting.

Proposed registry fees:

- Large provider: $500 annually per product
- Medium provider: $250 annually per product
- Small provider: $100 annually per product

Transparency provisions:

- AG website posts guidelines and continuously updated approved registry.
- Each registry listing links to product attestation.
- State education authority links to registry.
- Each district posts continuously updated list of school technology used at each school and grade level.

5.4 Bill 3: Electronic Device Opt-Out

This bill would create a caregiver/student right to refuse electronic device use as part of a course of instruction.

Key provisions:

- Caregiver or emancipated student may refuse electronic device use.
- Districts must create policies for exercising the right.
- Districts must provide alternative education and assessment methods.
- Students may not be penalized or discriminated against for opting out.
- Teachers may not be dismissed, suspended, disciplined, reassigned, or transferred for teaching without electronic devices.

---

6. Initial Analysis of the Safe School Technology Package

Strengths

The package contains several privacy-protective concepts:

- Data minimization
- Ban on targeted advertising
- Ban on geolocation in student-facing school technology
- Ban or restriction on generative/conversational AI
- Caregiver notice
- Deletion rights
- School technology transparency registry
- Device opt-out rights
- Restrictions on addictive design
- No forced social media accounts
- Annual review of school technology standards

Implementation Concerns

These ideas raise practical and legal questions:

1. **Registry self-attestation may be weak without audit power, staff capacity, meaningful penalties, and public complaint mechanisms.**
2. **Caregiver consent and opt-out systems create their own student data trail.** Schools would need to store which families opted in or out, what tools each student may use, and exceptions/accommodations.
3. **Seven-day deletion may conflict with education records, audit logs, security investigations, special education records, legal holds, or mandatory assessment data.**
4. **Blanket bans on cameras, AI, screens, or student-facing devices may need detailed exceptions for accessibility, assistive technology, language access, media production classes, computer science, online assessments, remote participation, and disability accommodations.**
5. **Claims about screen time, learning outcomes, myopia, AI harms, and student-data sharing vary widely in evidence quality and must be graded before use with legislators. See the evidence-confidence table in §6.1.**
6. **This package does not solve OS-level age-verification privacy problems.** It is about school procurement and student-facing EdTech, not broad device/account-level age signaling across the public internet.

6.1 Evidence-Confidence Table for Package Claims (Pass 1, June 17, 2026)

The package mixes well-documented facts with contested or advocacy-grade claims. Grading each one prevents a weak claim from undermining a strong argument in front of Rep. Levy or her staff. Grades reflect **source type and claim type**; a grade of "credible" or "strong" does **not** mean every cited document has been read line-by-line — items marked *needs verification* still require a read before public use.

Grade key: Strong = primary, peer-reviewed, or rigorous institutional review · **Credible** = reputable advocacy/reporting, not definitive · **Correlation only** = real data but no established causation · **Anecdotal** = single-case/testimonial · **Replace** = source is interest-conflicted or weak; find a better one · **Verify** = do not use without reading the underlying source first.

Claim cluster	Specific claim	Cited source(s)	Source type	Grade	How to use / caution
Student data / surveillance	EdTech apps and school apps share student data with third	Internet Safety Labs 2022 K-12 Benchmark; ISL school-	Nonprofit technical audit	**Strong** (for the data-sharing facts)	ISL ran actual app audits; solid for "many school apps

Claim cluster	Specific claim	Cited source(s)	Source type	Grade	How to use / caution
	parties, often without adequate consent	app report			share data." Cite the specific finding, not a sweeping claim.
	Online learning products enabled surveillance of children during the pandemic	Human Rights Watch (2022)	Credible NGO technical investigation	**Strong**	HRW did a real technical analysis of 164 products; defensible. Pin-cite the specific products/behaviors.
	A major student-data breach occurred (Illuminate Education)	NYT (2022)	Primary news, verifiable event	**Strong**	A real, documented breach. Safe to cite as a concrete example.
Screen time / health	Excessive screen time is linked to psychological /physical health risks	(package assertion; general)	Mixed / unsourced in packet	**Correlation only**	Associations exist but causation and dose-response are contested. Say "associated with," never "causes."
	Digital devices damage children's eyesight / drive nearsightedness	CBS News	News summary of contested science	**Correlation only / Replace**	The myopia rise is most robustly tied to **reduced time outdoors and near-work generally**, not screens specifically. Don't

Claim cluster	Specific claim	Cited source(s)	Source type	Grade	How to use / caution
					attribute myopia to screens as settled science; if used at all, cite primary ophthalmology literature, not CBS.
	National test-score (NAEP) declines reflect screen/EdTech use	Fondation/ Reboot Foundation 2019 NAEP memo	Advocacy memo	**Correlation only**	A 2019 advocacy memo cannot establish that screens caused NAEP trends (which also track the pandemic and much else). Correlation at best.
	Paper supports learning/literacy better than screens	PostPress	**Print-industry trade publication**	**Replace**	Source has a commercial interest in paper. The print-reading-comprehension literature is real but mixed; cite a meta-analysis (e.g., Delgado et al.) instead, and state the nuance.
	EdTech learning-outcome	Hechinger Report	Credible education journalism	**Credible**	Good support for "discount vendor-

Claim cluster	Specific claim	Cited source(s)	Source type	Grade	How to use / caution
	studies are often biased toward the developer				funded efficacy claims." Use it to argue for independent evidence, not as a health claim.
AI in K-12	The evidence base for AI in K-12 is thin / uncertain	**Stanford SCALE, "The Evidence Base on AI in K-12: A 2026 Review"**	Rigorous institutional review	**Strong**	The packet's best source. Reviewed 800+ (now 1,100+) papers; only ~20 high-quality causal studies; gains often don't persist once the tool is removed. Lead with this for the AI-evidence point.
	AI tools raise distinct risks for students (chatbots, addictive design)	Brookings	Credible think-tank analysis	**Credible**	Analytical, not empirical. Use for framing, pair with SB 1546 (the enacted AI-companion law) for the concrete hook.
District "success stories"	Specific districts/charters improved academically	*Not present in the extracted packet text*	—	**Verify / Anecdotal**	The reviewer flagged this as the weakest area. **No such**

Claim cluster	Specific claim	Cited source(s)	Source type	Grade	How to use / caution
	after reducing screens				**claim currently appears in the packet**; if pulled in from the Distraction-Free Schools source material, single-district before/after stories are anecdotal/correlation and must be backed by primary assessment data before use. Do not present as causal.

Two rules for using these with legislators:

1. **Lead with the Strong tier, never the weak tier.** Open the EdTech argument with ISL/HRW (documented data-sharing), the Illuminate breach (a real event), and the Stanford SCALE review (rigorous, recent). These are hard to attack. Keep myopia, NAEP-causation, and "paper beats screens" out of testimony unless re-sourced — a single contested claim lets an opponent discredit the rest.
2. **Match the verb to the evidence.** "Associated with" / "correlated with" for the health and test-score claims; "documented" / "found" only for the audited data-sharing facts and the breach. Reserve causal language for nothing here except where a primary causal study is cited.

7. Oregon ODE Interim Testing Link — Why It Matters

Source:

- https://www.oregon.gov/ode/accountability/pages/interim-tests.aspx

Initial read:

- The ODE interim testing page is highly relevant to the school technology / EdTech track.
- Oregon's SB 141 / Education Accountability Act appears to require districts and public charter schools to administer interim tests in math and English language arts three times per year in grades K–8.
- Approved vendors/tests appear to include iReady, MAP, Smarter Balanced via Cambium, and Star.
- Districts transitioning to a new approved test must have it in place by a specified 2027 deadline.

Why It Matters

Any school-technology bill that says Pre-K–5 should have no student-facing screens, or that allows only narrow online-assessment preparation, must account for Oregon's existing digital assessment infrastructure.

Questions Raised

1. Would interim testing platforms be covered by the proposed school technology registry?
2. Would iReady, MAP, Smarter Balanced/Cambium, and Star need to attest to privacy, safety, advertising, geolocation, AI, and data-minimization standards?
3. If a caregiver opts out of electronic device use, how would that interact with SB 141's K–8 interim testing mandate?
4. Who receives, stores, and analyzes interim test data: vendor, district, ODE, or all three?
5. Can approved vendors use student data for product improvement, analytics, benchmarking, AI training, or non-instructional purposes?
6. Would screen-time restrictions allow testing but prohibit related practice tools, dashboards, adaptive lessons, or online curricula?
7. If ODE-approved vendors fail privacy/safety standards, what happens to districts legally required to use approved interim tests?

---

8. Lake Oswego Granicus Clip — Why It Matters

Source:

- https://loswegok12.granicus.com/player/clip/973?view_id=3&redirect=true

Initial read:

- This appears to be a Lake Oswego School District School Board meeting video.
- The agenda/video index reportedly includes items such as a technology update and educational data discussion.
- No separate documents may be available through the Granicus page, so the video may be the primary public record.

Research Use

This may become an Oregon local implementation case study for:

- Classroom technology balance
- Device use policies
- Educational data systems
- Parent/community concerns
- District implementation burdens
- Whether districts are reducing tech use voluntarily or seeking state mandates

Follow-Up Needed

- Watch or transcribe the relevant sections, especially technology update and educational data discussion.
- Identify any specific vendors, dashboards, assessment tools, privacy concerns, device policies, or public comments.

---

9. Model-Bill Comparison — First Pass

This is the core legal/policy architecture comparison for age-verification and age-signal models.

Model Set

Model	Why include it
Oregon HB 3696, 2025	Closest Oregon precedent. It involved app stores, developers, age verification, parental consent, app age ratings, and parental tools.
California AB 1043 / Digital Age Assurance Act	Key operating-system age-signal model. It most directly matches the concern raised by "OS-level age verification."
Texas SB 2420	Major state app-store accountability model and active legal/implementation battleground.
Utah App Store Accountability Act	Early influential app-store accountability model.
Louisiana App Store Accountability Act	Another state app-store/developer model with timing relevant to 2027 implementation.
Federal App Store Accountability Act	Federal proposal that may influence, preempt, or shape state approaches.
EU privacy-preserving proof-of-age approach	Contrasting model designed around proving an age threshold while minimizing personal information shared.

Important Research Links for Model-Bill Comparison

- Oregon HB 3696 overview: https://olis.oregonlegislature.gov/liz/2025R1/Measures/Overview/HB3696
- California AB 1043 bill text: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1043

- Texas SB 2420 final bill text:
  https://capitol.texas.gov/tlodocs/89R/billtext/html/SB02420F.HTM
- Utah SB 142 PDF:
  https://le.utah.gov/Session/2025/bills/introduced/SB0142.pdf
- Louisiana law page:
  https://legis.la.gov/legis/Law.aspx?d=1428945
- Federal App Store Accountability Act press release, Rep. John James:
  https://james.house.gov/news/documentsingle.aspx?DocumentID=247
- EU age verification policy page:
  https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification
- Google Play Age Signals API overview:
  https://developer.android.com/google/play/age-signals/overview
- Google Play Age Signals API usage page:
  https://developer.android.com/google/play/age-signals/use-age-signals-api
- Google Play policy/support page on age signals:
  https://support.google.com/googleplay/android-developer/answer/16569691?hl=en
- Apple Declared Age Range documentation:
  https://developer.apple.com/documentation/declaredagerange
- Apple developer news on Declared Age Range API:
  https://developer.apple.com/news/?id=f5zj08ey
- Google blog on online age verification / risk-based approach:
  https://blog.google/innovation-and-ai/technology/families/google-approach-online-age-verification/
- FTC COPPA policy statement on age verification technologies:
  https://www.ftc.gov/news-events/news/press-releases/2026/02/ftc-issues-coppa-policy-statement-incentivize-use-age-verification-technologies-protect-children
- EFF discussion of California AB 1856/open-source age-gating concerns:
  https://www.eff.org/deeplinks/2026/05/one-step-forward-two-steps-back-cas-ab-1856-exempts-open-source-expands-age-gating
- Tom’s Hardware coverage of California open-source/Linux age-verification concerns:
  https://www.tomshardware.com/software/linux/california-moves-to-exempt-linux-from-its-upcoming-age-verification-law-after-backlash-over-forcing-operating-systems-to-collect-users-ages-amendment-proposed-by-the-same-lawmaker-who-wrote-the-original-law
- The Verge coverage of age verification bills and Linux/open source:
  https://www.theverge.com/tech/930573/age-verification-bills-linux-open-source

10. Model-Bill Comparison Table (status-folded, source-checked)

Status column added, last updated June 17, 2026 (see §1A and the source table). The pattern to convey accurately: app-store gatekeeper laws keep getting **blocked by district courts on First Amendment grounds, then revived by appellate courts** that stay those injunctions pending appeal — Texas's law was enjoined in December 2025 and is now back in effect (June 2026). The merits are unresolved. The OS age-*signal* model (AB 1043) has **not** been challenged; it may prove more litigation-resistant because it transmits a signal rather than blocking access, but that is an *interpretive* point, and its constitutional and privacy questions are untested. Treat the OS model as the higher-priority concern because of its infrastructure reach, not because anyone can predict the litigation.

Model	Basic architecture	Who verifies age?	What gets shared?	Main privacy concern	Status (as of June 2026)	Oregon relevance
Oregon HB 3696, 2025	App-store / developer model for minors' use of software applications.	App stores and developers would verify user age and categorize users.	Age category, parental consent status, app age ratings, parental controls.	Requires age checks before app use/downloads and creates parent/developer/app-store data flows.	**DIED IN COMMITTEE.** Rep. Reschke (R); referred to House Commerce & Consumer Protection 2/27/2025; no further action.	Closest Oregon precedent. Ask whether the 2027 proposal revives or abandons this app-store model.
California AB 1043 / Digital Age Assurance Act	Operating-system age-signal model.	OS provider prompts account holder for birth date, age, or both at setup.	Age-bracket signal through real-time API, generally under 13, 13–15, 16–17, or 18+.	Makes the OS a mandatory age-signal layer; creates actual-knowledge implications for developers; complicated for shared devices,	**ENACTED.** Signed 10/13/2025 (unanimous); effective Jan 1, 2027. Clean-up bill AB 1856 pending (passed Assembly 68-1, 5/28/2026	Most direct match for "OS age verification." The high-priority model and the most likely template for a 2027 Oregon bill.

Model	Basic architecture	Who verifies age?	What gets shared?	Main privacy concern	Status (as of June 2026)	Oregon relevance
				open source, and privacy-preserving systems.	). **Not yet challenged** — may be more litigation-resistant because it transmits an age signal rather than directly blocking access, but that remains untested.	
Texas SB 2420 / App Store Accountability Act	App-store gatekeeper model for mobile app stores.	App store verifies age category using a commercially reasonable method.	App stores provide developers access to age category and parental consent status.	Every app-store account may need age categorization; developers receive age/consent signals.	**BLOCKED, THEN REVIVED — NOW IN EFFECT.** PI granted 12/23/2025 (Pitman, W.D. Tex.); stay denied 5/6/2026; 5th Cir. stayed the injunction; **law took effect 6/4/2026**; merits still on appeal. *[Needs status update before citing.]*	Shows the volatility: a law can be struck down at the trial level and revived on appeal within months.

Model	Basic architecture	Who verifies age?	What gets shared?	Main privacy concern	Status (as of June 2026)	Oregon relevance
Utah SB 142 / App Store Accountability Act	App-store gatekeeper model; first in the nation.	App store providers verify user ages and obtain parental consent for minor accounts.	Age and consent data shared with developers.	Centralizes child age and parental-consent data in app-store ecosystem.	**AMENDED & NARROWED.** HB 498 (3/18/2026) pushed compliance to May 2027 and removed AG enforcement (private action only); CCIA challenge voluntarily dismissed 4/21/2026.	Shows states retreating to private-enforcement-only to dodge First Amendment challenges.
Louisiana HB 570 (Act 481) / App Store Accountability Act	App-store / developer shared-responsibility model.	Covered app store; developers may rely on app-store age signals.	Developers may verify age category through covered app-store data-sharing methods and may request age-verification data or parental consent.	Risk of duplicated age data collection and broad developer reliance on age signals.	**ENACTED, THEN DELAYED.** Signed 6/30/2025; HB 977 (5/15/2026) delayed it to July 1, 2027 and added developer reliance protection. (This is the packet's "Louisiana App Store Accountability Act.")	Shows the model spreading but stalling on the same constitutional headwinds.
Alabama HB 161 / App Store Accounta	App-store gatekeeper model; explicitly	App store verifies age; retroactive	Age category, parental consent,	Same speech/privacy risks as other	**ENACTED.** Signed 2/17/2026; effective	Newest ASAA — the model is still

Model	Basic architecture	Who verifies age?	What gets shared?	Main privacy concern	Status (as of June 2026)	Oregon relevance
bility Act *(new — add to set)*	covers pre-installed apps.	verification for existing accounts.	parent-account affiliation for minors.	ASAAs; retroactive scope is broader.	Jan 1, 2027; not yet challenged.	being adopted even as courts push back elsewhere.
Federal App Store Accountability Act	National app-store gatekeeper model.	App stores verify age and link minor accounts to parental accounts.	Age category, parental consent, app ratings, parental approval for downloads/purchases.	National age-categorization scheme could reduce state inconsistency but still raises privacy/speech risks.	**PROPOSED.** Introduced by Rep. James / Sen. Lee, May 2025; not enacted. Senate COPPA 2.0 passed; House E&C tabled its version.	Oregon may wait for, harmonize with, or draft around federal action — but federal movement is currently stalled.
EU proof-of-age approach	Credential/proof-of-age model rather than app-store gatekeeping.	Wallet or verification solution proves user meets a threshold.	Ideally only proof of being over threshold, such as 18+, without exact age or identity.	Still has security and implementation risk, but potentially less data sharing than OS/app-store age signals.	EU age-verification blueprint and prototype app in development (2025–26).	The privacy-preserving counter-model: prove a threshold without building a persistent age-attribute layer.

11. Architectural Takeaways

11.1 App-Store Laws

App-store laws ask Apple/Google-style stores to verify or categorize users and share age/consent signals with app developers.

Potential advantages:

- Centralizes compliance at the app-store layer.
- Avoids requiring every developer to independently verify age.
- Parents may already manage children's accounts through app-store ecosystems.

Potential risks:

- Adults may need to be categorized too.
- App stores become age/consent brokers.
- Developers receive sensitive age or parental-consent signals.
- Minors may need parental consent to access broad categories of lawful speech.
- Web apps, sideloading, alternate stores, and shared accounts may undermine effectiveness.

Current legal status (last updated June 2026) — contested and unsettled, not settled either way. *(Analysis; statuses sourced in §1A.)* This is no longer a theoretical "litigation risk," but it is also not a clean win for either side. The pattern: **district courts repeatedly enjoin these laws on First Amendment grounds, and appellate courts increasingly stay those injunctions and let the laws operate pending appeal.** Texas SB 2420 was enjoined in December 2025, the district court refused to lift the injunction in May 2026, and then the **Fifth Circuit stayed the injunction and the law took effect June 4, 2026.** On the social-media side, NetChoice won district-court injunctions in Arkansas (*Griffin*), Ohio (*Yost*), and Louisiana (*Murrill*, Act 456) — but the 11th Circuit stayed Florida's injunction and the 5th Circuit let Mississippi's law take effect (SCOTUS declined to block it, with Justice Kavanaugh writing it was "likely unconstitutional"). The honest throughline for Rep. Levy: **trial courts are skeptical of age-gating general lawful content, but the appellate law is in flux and several of these laws are operating right now.** See §12A.

11.2 Operating-System Age-Signal Laws

OS age-signal laws make the operating system or account setup flow collect or prompt for age/birthdate and provide age-bracket signals to apps.

Potential advantages:

- More universal than app-store layer.
- Can cover apps downloaded outside a single store, depending on drafting.
- Developers receive a standardized signal.

Potential risks:

- More invasive because the OS/account layer becomes an age broker.
- Shared devices create accuracy problems.
- School-managed devices create student privacy problems.
- Open-source and privacy-preserving operating systems may not be designed to collect or transmit user age.
- Age signal may become a persistent attribute usable for tracking/fingerprinting.

- Developers receiving age signals may obtain "actual knowledge" triggering additional legal duties.

Current legal status (last updated June 2026). The flagship OS model — **California AB 1043** — is **enacted** (signed Oct. 13, 2025; effective Jan. 1, 2027) and, unlike the app-store laws, **has not yet been challenged.** *(Interpretive conclusion follows.)* The OS-signal model may be **more litigation-resistant** than direct app-store or social-media age-gating, because it transmits an age signal rather than directly blocking access to speech. But it **has not been meaningfully tested**, and its constitutional, privacy, compelled-collection, and anonymous-speech implications remain unsettled. That combination — likely durable *and* untested — is exactly why it deserves the most scrutiny: a law that survives the First Amendment can still build a persistent device-level age-attribute layer, and the open-source/Linux problem is real enough that states are already drafting carve-outs (California's AB 1856, pending; Colorado's broader exemption).

11.3 Privacy-Preserving Proof-of-Age Models

These models aim to prove that a user meets a threshold, such as "over 18," without disclosing exact birthdate, identity, or more information than necessary.

Potential advantages:

- Better data minimization.
- Could reduce the need for every website/app to collect identity documents.
- May support threshold-only proof.

Potential risks:

- Depends heavily on implementation.
- Credential providers may become sensitive intermediaries.
- Government digital identity concerns may arise.
- Sites may still over-collect if the law does not prohibit it.
- Exclusion risks for people without accepted documents or credentials.

---

12. Preliminary Risk Matrix

Risk	App-store model	OS age-signal model	EU/proof-of-age model
Adult privacy burden	High: adults may need age categorization to prove they are not minors.	High: depending on implementation, the OS/account setup flow may prompt or infer age for users broadly, including adults, since the system must distinguish minors	Medium: depends on whether proof is threshold-only and anonymous.

Risk	App-store model	OS age-signal model	EU/proof-of-age model
		from adults.	
Data centralization	High: app store becomes age/consent broker.	Very high: OS/account layer becomes age-signal broker.	Lower in theory, but depends on credential provider design.
Developer tracking/fingerprinting	Medium/high: developers receive age category and consent status.	High: recurring age signal can become another persistent attribute.	Lower if only one-time threshold proof is sent.
Shared device problem	Significant: app-store account may not match actual user.	Severe: device/account holder may not match real user.	Medium: user-specific credentials can help, but not always.
School-device problem	Significant if school app stores or managed devices are covered.	Severe if OS account setup is controlled by district/vendor.	Depends on whether schools are excluded or separately regulated.
Open-source / small developer impact	Mostly developer compliance burden.	Potentially severe for Linux/open-source OSs and small OS distributions.	Depends on whether open standards and multiple providers are allowed.
Constitutional / First Amendment risk	**High at the trial level, but unsettled on appeal.** Texas's law was enjoined (Dec. 2025) yet took effect June 2026 after the 5th Cir. stayed the injunction; AR/OH/LA social-media analogues enjoined; FL/MS revived on appeal. Merits unresolved. See §12A.	**Untested.** AB 1043 transmits only an age bracket and has not been challenged; if it survives, the exposure shifts to privacy/compelled-collection/anonymous-speech grounds rather than free-speech access.	Medium/high depending on scope and whether lawful speech is gated.
Circumvention risk	Moderate: alternate stores, web apps, VPNs, parent accounts.	Moderate: false birthdates, shared accounts, alternate OSs, sideloading.	Moderate: borrowed credentials, VPNs, noncompliant sites.
Data breach risk	High if exact age/birthdate, parent-child link, or	Very high if OS/account providers hold age	Medium if well-designed; high if credential providers

Risk	App-store model	OS age-signal model	EU/proof-of-age model
	consent history is stored.	attributes for all users.	retain logs.
Repurposing risk	High unless law bans advertising, analytics, profiling, and law enforcement access.	Very high because OS-level signals can become infrastructure.	Medium if strict purpose limits and unlinkability are required.

12A. Constitutional Framework — What the Case Law Actually Says

(Source-checked June 17, 2026 — see §1A. This replaces the earlier "Civil Liberties / Constitutional Deep Dive" placeholder with grounded doctrine. It is the analytical spine for the Levy conversation and any memo.)

The constitutional question is not "can the state protect minors online?" — courts broadly accept that the state has at least an important, often compelling, interest in youth safety and mental health. The question is **how**, and the case law draws a sharp line between two things that the town-hall framing tends to blur together.

The dividing line: sexual content vs. general lawful content

- **Age verification for sexual material that is obscene as to minors → survivable.** In **Free Speech Coalition, Inc. v. Paxton, 606 U.S. 461 (2025)** (decided June 27, 2025, 6–3), the Supreme Court upheld Texas's requirement that sites where more than one-third of content is "sexual material harmful to minors" verify visitors' ages. The Court applied **intermediate scrutiny**, holding the requirement **only "incidentally" burdens adults' access to protected speech.** Crucially, the majority's reasoning is **expressly limited to the obscene-as-to-minors category** — EFF, the ACLU, and the Harvard Law Review all stress it does not bless age verification for general-audience content.
- **Age verification / parental consent as a gateway to general lawful content → repeatedly struck down.** When states have tried to gate *social media* or *app stores* — i.e., access to a vast range of lawful, non-obscene speech — courts have generally treated the laws as **content-based** restrictions triggering **strict scrutiny**, and most have fallen:
  - **Texas SB 2420 (app stores)** — preliminarily enjoined in full (Judge Pitman, W.D. Tex., Dec. 23, 2025) as content-based and failing least-restrictive-means; the enjoining court **expressly distinguished FSC v. Paxton** because SB 2420 reached far beyond sexual content. **But the appellate posture cut the other way:** the district court declined to lift the injunction (May 6, 2026), and the **Fifth Circuit then stayed it, letting SB 2420 take effect June 4, 2026** while the merits proceed. So even the strongest trial-court win for the speech side is now operating against it on appeal.
  - **Social-media age laws** — NetChoice has won injunctions in Arkansas (*Griffin*), Ohio (*Yost*), Louisiana (*Murrill*, Act 456), Georgia (*Carr*, on appeal), Virginia, and others, courts repeatedly invoking **Brown v. Entertainment Merchants Ass'n**

(2011): the state has **no "free-floating power to restrict the ideas to which children may be exposed."**

The doctrine is unsettled at the edges — be honest about this

The picture is **not** uniformly favorable to the privacy/speech side, and a careful memo should say so: - Appellate courts are now **splitting on the scrutiny level**. The **11th Circuit stayed** Florida's injunction (Nov. 2025); the **5th Circuit let Mississippi's HB 1126 take effect**; and the **Supreme Court declined to block Mississippi**, though Justice Kavanaugh wrote the law was "likely unconstitutional." Some judges are pressing whether user-to-user "social speech" really triggers strict scrutiny, and whether facial challenges sweep too broadly after **Moody v. NetChoice (2024)**. - So the safe statement is: *app-store and social-media age-gating of general content currently faces serious First Amendment headwinds and a majority of district courts have blocked these laws, but the appellate law is actively in flux.*

Why the OS age-signal model (AB 1043) is the constitutionally slipperier case

This is the part most relevant to Oregon's likely 2027 vehicle. **AB 1043 has not been challenged**, plausibly because it was **engineered to avoid the content-gating trigger**: the OS transmits an age *bracket* to developers and leaves any access decision to them. That design *may* be **more litigation-resistant** than the app-store laws — but it has not been meaningfully tested, and whether it ultimately survives, and on what theory, is unsettled. The strategic point does not depend on predicting the outcome: - A law that survives the First Amendment can still build a **persistent, device-level age-attribute layer** affecting users broadly — the infrastructure risk the rest of this packet is about. - The constitutional analysis shifts from *free speech* to **privacy, data-protection, and compelled-collection** grounds, where the protections are statutory (and thinner) rather than constitutional. - If Oregon couples an AB 1043-style signal with *downstream mandates* (e.g., requiring platforms to block or restrict minors), it risks re-importing the content-based problem and inheriting the app-store laws' litigation fate.

What this means for the conversation with Rep. Levy

1. **Separate the categories explicitly.** Support (or at least don't contest) narrowly-drawn verification for obscene-to-minors material; scrutinize hard any age-gate on general apps, social media, or the OS layer.
2. **The litigation record is an asset — used carefully.** Oregon would be legislating into an area where trial courts have repeatedly found app-store and social-media age-gating unconstitutional, even though several of those laws are now operating on appeal. "Why will Oregon's bill survive the First Amendment scrutiny that blocked Texas's, Arkansas's, and Louisiana's at the trial level — and is the goal to litigate to the same uncertain place?" is a fair, sourced question, not obstruction.
3. **Push the privacy frame for the OS model.** Because AB 1043-style laws may *pass* constitutional muster, the First Amendment will not save Oregonians from the data-infrastructure risk. That is where the §15 safeguards (data minimization, purpose limitation, deletion, no law-enforcement access, no repurposing) do the real work.

Primary/authoritative sources for this section: FSC v. Paxton slip opinion (No. 23-1122); CCIA v. Paxton (W.D. Tex.) order on SB 2420; NetChoice v. Griffin (W.D. Ark.) and NetChoice v. Murrill

(M.D. La.) rulings; Brown v. EMA, 564 U.S. 786 (2011); Moody v. NetChoice, 603 U.S. 707 (2024); appellate-posture reporting from Biometric Update and AEI. Pin-cite verification of each holding remains a [NEEDS PRIMARY] task before quoting in testimony.

---

13. Important Technical Development: Age-Signal Infrastructure Is Already Being Built

Google and Apple are already building mechanisms in response to state age-verification/app-store accountability laws.

Google Play Age Signals API

Research links:

- https://developer.android.com/google/play/age-signals/overview
- https://developer.android.com/google/play/age-signals/use-age-signals-api
- https://support.google.com/googleplay/android-developer/answer/16569691?hl=en

Initial note:

- Google's Play Age Signals API is designed to help developers meet obligations in jurisdictions such as Texas, Utah, and Louisiana.
- The API returns coarse age ranges, such as 0–12, 13–15, 16–17, and 18+, depending on jurisdiction.
- Google states that age-signal information may not be used for advertising, marketing, profiling, or analytics.

Apple Declared Age Range API

Research links:

- https://developer.apple.com/documentation/declaredagerange
- https://developer.apple.com/news/?id=f5zj08ey

Initial note:

- Apple's Declared Age Range API allows apps to request that a user share an age range.
- In Family Sharing contexts, parents can choose whether a child's age range is shared.
- Apple says the child's actual birthdate is not shared.

Why This Matters for Oregon

Oregon lawmakers may believe they are simply drafting a child-safety bill. In practice, Oregon may be deciding whether to participate in or accelerate a broader platform-wide age-signal infrastructure.

---

14. Oregon-Specific Questions for Rep. Levy

These are the first-pass questions to prepare before the conversation.

Context to carry in (last updated June 2026, see §1A): Oregon's last app-store attempt (HB 3696) died in committee; the app-store model is constitutionally contested but operating in several states (Texas's law took effect June 2026 on appeal); the leading OS template is California's AB 1043 (untested); and Oregon already regulates student data (OSIPA), under-16 commercial data (OCPA), and AI companions (SB 1546, Ch. 85). Several of these questions are sharper now that we know that.

1. **Which model is being considered?** A revived app-store model (HB 3696 died in committee in 2025 — is it coming back, given that Texas's version was enjoined and then took effect on appeal, while Utah's and Louisiana's were delayed to 2027?), the California OS age-signal model (AB 1043, enacted but untested), a school-technology package, or something new? This single answer determines almost everything else.

2. **What specific harm is the bill trying to solve — that existing Oregon law doesn't already reach?** Adult content, social-media addiction, AI chatbots, EdTech data, app downloads, in-app purchases, or school screen time? This matters because Oregon *already* bans selling student data and targeting ads to students (OSIPA), bans selling/profiling under-16 data (OCPA, as of Jan. 1, 2026), regulates AI companions with a "reason to believe a minor" standard (SB 1546), and has a statewide bell-to-bell school phone policy (EO 25-09). The fair question is what gap survives all four layers, and why an age-signal infrastructure is the least-restrictive way to fill it.

3. **How broadly will age be collected or inferred?** Depending on implementation, will the app store, OS account, device, or service need to determine the age of most or all users — including adults — to know whether minor protections apply? (Ask this as a design question, not an assumption.)

4. **What data will be collected?** Exact birthdate, exact age, age bracket, ID document, biometric estimate, credit-card data, parent attestation, self-declaration, or inferred age?

5. **Who stores the underlying age proof?** Apple, Google, Microsoft, school districts, developers, third-party verification vendors, Oregon DOJ, ODE, or another state agency?

6. **What signal is shared?** Age bracket only, parental consent status, supervision status, regulatory applicability, parent-child relationship, or other metadata?

7. **Who receives the signal?** Every app, only covered apps, only high-risk services, school apps, websites, AI tools, social media platforms, or app stores?

8. **Can age signals be used for advertising, analytics, profiling, personalization, content ranking, school discipline, fraud detection, law enforcement, or immigration enforcement?**

9. **What happens with shared family devices?** How does the system know whether a parent, teenager, younger child, sibling, guest, or caregiver is using the device?
10. **What happens with school-issued or district-managed devices?** Does the district become the age/account authority? Who controls age data? How does this interact with FERPA/COPPA/state student privacy law?
11. **What happens with foster care, custody disputes, guardianship conflicts, emancipated minors, homeless youth, and minors seeking sensitive safety/health information?**
12. **Will there be exceptions for open-source operating systems, small developers, public libraries, accessibility tools, assistive technology, and education-specific systems?**
13. **Will Oregon require a privacy impact assessment before bill introduction?**
14. **Will Oregon require an independent technical feasibility assessment before bill introduction?**
15. **Will Oregon hold stakeholder sessions with privacy advocates, student rights groups, disability rights advocates, educators, school IT staff, open-source developers, cybersecurity experts, youth, parents, and civil liberties organizations?**

---

15. Possible Oregon Safeguards / Red Lines

If Oregon proceeds with legislation, potential safeguards to propose include:

Data Minimization

- No exact birthdate sharing with developers.
- No government ID retention.
- No biometric age estimation mandate.
- Threshold-only or coarse-age signal where possible.
- No persistent unique age token that can be used for tracking.

Purpose Limitation

- Age signals may be used only for statutory child-safety compliance.
- Explicit ban on use for advertising, targeted marketing, analytics, profiling, personalization, algorithmic ranking, insurance, credit, employment, school discipline, or unrelated enforcement.

Retention / Deletion

- Underlying age proof must be deleted promptly after verification unless strictly necessary.
- Retention schedules must be public.

- Logs must be minimized and not linkable across services.

Security

- Mandatory security controls for any age-verification provider.
- Breach notification.
- Independent audits.
- Encryption in transit and at rest.
- No centralized state database of age verification.

Access / Law Enforcement

- No law-enforcement access to age-verification records without a warrant or court order.
- No immigration-enforcement use.
- No school discipline use.
- No civil subpoena fishing expeditions without user notice and opportunity to challenge.

Scope Limits

- Apply only to clearly defined high-risk services if any age assurance is required.
- Avoid universal OS-level age collection.
- Avoid requiring every adult to prove age to access lawful speech.
- Exempt public libraries, accessibility tools, and low-risk educational services where appropriate.

Open Source / Small Developer Protections

- Exempt open-source operating systems that do not collect user identity/age.
- Provide safe harbors for small developers that rely on privacy-preserving platform signals.
- Do not require developers to build independent age-verification systems unless strictly necessary.

Transparency / Accountability

- Public privacy impact assessment before enactment.
- Technical feasibility report before enactment.
- Annual public transparency reports.
- Public list of approved age-verification methods.
- Complaint mechanism.
- Sunset clause and mandatory legislative review.

School-Specific Safeguards

- Separate student EdTech rules from general public age-verification rules.
- Clarify interaction with ODE interim testing requirements.
- Require vendor data-use limitations for assessment platforms.
- Protect students with disabilities and assistive-technology needs.
- Ensure opt-out does not harm grades, graduation, services, or accommodations.

16. Key Distinction for Conversation

A concise explanation for lawmakers:

> App-store laws ask Apple and Google to check age or parental consent before minors download or use apps. Operating-system laws go further by making the device or OS account layer collect age or birthdate and transmit age-bracket signals to apps. That shift matters because the OS is closer to the root of a person's digital life. If Oregon chooses the OS layer, it risks creating an age-surveillance infrastructure that affects adults, minors, schools, families, developers, and open-source systems.

The counterintuitive part to convey (see §12A): the app-store model is the one courts have repeatedly blocked at the trial level — Texas, Arkansas, Ohio, Louisiana — yet several of those laws are now operating after appellate stays (Texas's took effect June 2026). The OS-signal model (AB 1043) hasn't been challenged at all and may be harder to challenge, because it passes an age bracket rather than blocking speech. So the OS layer is not obviously the safer choice for Oregonians' privacy: if it holds up, the First Amendment won't be there to stop the age-attribute infrastructure it builds. The protection has to come from the statute itself — data minimization, purpose limits, deletion, and no repurposing (§15).

---

17. Suggested First Conversation Agenda With Rep. Levy

1. Thank Rep. Levy for being willing to discuss the issue, and acknowledge her own long work on the cell-phone effort (HB 2251 / EO 25-09).
2. Acknowledge shared goals: child safety, student privacy, age-appropriate design, and responsible technology. Note Well Wired's role opening the town hall — the school/healthy-tech concern is real and shared.
3. Ask which model Oregon is considering (§14 Q1) — and surface that HB 3696 died, the app-store model is constitutionally contested but operating in several states, and AB 1043 is the leading (but untested) OS template.
4. Separate school EdTech regulation from OS/app-store age verification — and note that OSIPA already bans selling student data and ad-targeting students, so the EdTech "ask" may be narrower than it appears, while SB 141's three-times-a-year K-8 interim testing (in effect 2026-27) constrains any "no screens" framing.
5. Explain the constitutional picture (§12A, §16): trial courts keep finding app-store/social-media age-gating unconstitutional, but appellate courts are letting several laws operate pending appeal; the OS model is likely more litigation-resistant but untested, which is exactly why its privacy risk needs statutory guardrails rather than reliance on the courts.
6. Ask whether a privacy impact assessment and independent technical feasibility review can happen before bill drafting.
7. Offer to help convene or provide a privacy/civil-liberties perspective — within BPA's lane.
8. Share a short written checklist of questions (§14) and safeguards (§15).

---

18. Draft Framing Language for Future Memo

This language may be useful later in a memo, email, or testimony draft.

> Oregon can protect children online without creating a statewide age-surveillance layer. Before adopting app-store or operating-system age verification, lawmakers should define the specific harm they are addressing, identify the least invasive layer of intervention, and require strict data minimization, purpose limits, deletion rules, security safeguards, open-source protections, accessibility protections, and independent privacy review.

Alternative shorter version:

> Child safety and privacy should not be treated as competing values. Oregon should protect minors without requiring every Oregonian to prove their age to use ordinary digital tools or access lawful online speech.

---

19. Research Status — Completed and Open Tasks

Completed / archived (source-checked — see §1A, §1A-Pins, §6.1, §12A)

Exact text and pin-cites pulled and graded for: **AB 1043** (Civil Code §§1798.500 et seq.), **Texas SB 2420** (orders + 5th Cir. posture), **Utah HB 498** (Utah Code Title 13 Ch. 76), **Louisiana HB 977 / Act 185** (R.S. 51:1771–1775), **Alabama HB 161 / Act 2026-59**, **AB 1856** (digest-level; enrolled text pending chaptering), **SB 1546 / Ch. 85**, **OSIPA** (ORS 336.184), **OCPA** (ORS 646A.570–.589 + HB 2008), **OCIPA** (ORS 646A.600–.628), **SB 141 §§24–25**, the **FTC COPPA policy statement**, and **FSC v. Paxton** (pin-pages). Oregon's existing-privacy baseline (§1A), the constitutional framework (§12A), and the Safe School evidence-quality grading (§6.1) are drafted.

Still open — statutory / legal

- **AB 1856 final enrolled text** once chaptered (section numbers for the browser/website-operator definitions).
- **Live litigation status checks the morning of any memo/testimony use** — Texas SB 2420 Fifth Circuit posture (currently in effect on a stay), AB 1043 as it nears its 1/1/2027 effective date, and the NetChoice appellate split (11th Cir. FL/GA; 5th Cir. MS).
- Federal **App Store Accountability Act** (James/Lee) and **COPPA 2.0** status if either moves.

Technical Architecture Deep Dive — substantially addressed in the companion document `os_age_signal_technical_analysis.md` (June 18, 2026)

A full technical pass now exists as a separate deliverable: a one-page non-technical explainer, an architecture map, a data inventory, request-control and persistence/linkability analyses, an edge-case table, a Google/Apple platform review (source-checked against the developer docs), a security/abuse threat model, Oregon-specific implementation questions, and a sponsor checklist. The outline below is retained as the scope definition; the worked analysis is in the companion

file. Remaining open items: Microsoft/Xbox, Meta/Snap/TikTok/Discord/Roblox, and browser-level relays still need primary-doc confirmation.

The legal foundation is now strong; the weakest remaining area is *how the systems actually work*. The strongest privacy concerns all turn on technical implementation — persistence, linkability, access control, replay, revocation, audit logs, developer misuse, and whether an age signal can become a fingerprinting attribute. **Treat the operating-system layer as the primary architecture** (it is what Rep. Levy reportedly named, and AB 1043 is the leading model); Google/Apple are *implementation examples* beneath it, not the whole picture.

A. Operating-System Age-Signal Architecture (primary). Map the full OS-level age-signal flow: - *Collection → derivation → translation → request → delivery → legal effect:* age/birthdate collected at device or account setup; an age bracket stored or derived by the OS/account/platform layer; translation into a coarse signal; a request by an app, app store, browser, or website; delivery via API; and the downstream legal effect (notably whether the recipient is deemed to have **"actual knowledge"** of the user's age range, as AB 1043 provides). - *Where the age data lives:* on-device only; cloud account; app-store account; family/supervised account; school-managed account; third-party verifier; or a state/vendor database. - *What is actually shared:* exact birthdate; exact age; coarse bracket; over/under a threshold; parental-consent status; parent–child relationship; supervised-account status; device/account identifier; or an error/refusal/unknown-age state. - *Which entities may request the signal:* all apps; only covered apps; app stores; developers; browsers; websites; school apps; AI companions; social platforms; low-risk services. - *Edge cases:* shared family devices; multiple profiles on one device; a parent account used by a child (or a child account on many devices); custody/guardianship/foster-care/emancipated-minor situations; public-library computers; school-issued/district-managed devices; assistive technology; open-source and privacy-focused operating systems; users without stable identity documents or platform accounts. - *Privacy/security risks:* a persistent age attribute; tracking/fingerprinting; parent–child-relationship exposure; breach risk; law-enforcement or civil-subpoena access; immigration-enforcement use; school-discipline use; vendor analytics/product-improvement use; repurposing for advertising, profiling, or content ranking. - *Required safeguards to evaluate:* no exact-birthdate sharing; no biometric or government-ID mandate; no centralized state age database; strict purpose limitation; prompt deletion of underlying proof; no advertising/analytics/profiling/personalization use; warrant or court-order requirement for government access; transparency reports; independent security audits; open-source carve-out; school-managed-device protections; and a sunset / legislative-review clause.

B. Platform implementation examples (source-checked against developer docs, June 2026 — confirm against the live docs before formal use, since both are beta and changing): - **Google Play Age Signals API** (Android, beta) — a client-side runtime API returning a **status** (VERIFIED, SUPERVISED, SUPERVISED_APPROVAL_PENDING/DENIED, DECLARED, UNKNOWN) plus an **age range** via `ageLower`/`ageUpper`, default brackets **0–12, 13–15, 16–17, 18+** (customizable in Play Console). It returns data **only where Play is legally required** to, issues a Play-generated `installID`, and is governed by a **data-use policy (eff. Jan 1, 2026) barring use of age data for advertising, profiling, or analytics, and barring long-term storage (real-time query only)**; the info is usable only by the requesting app. Notably, it **went live for Texas users who created accounts after May 28, 2026** — corroborating the SB 2420-in-effect status. *(Source: developer.android.com/google/play/age-*

signals; Google Play Console Help.) - **Apple Declared Age Range API** (iOS, live Jan 1, 2026) — lets an app **request an age range without receiving the exact birthdate**. The developer sets the **age thresholds** it cares about (e.g., 13/16/18) and the API answers which bracket / over-threshold, plus an eligibility flag and **parental-controls status** for children in **Family Sharing**; paired with **Significant Change** and **PermissionKit** consent APIs and a sandbox (Settings → Developer → Sandbox Apple Account → Age Assurance). Apple's signal reports the **method** used for age assurance. *(Source: Apple developer documentation; FKKS, Median.co technical write-ups.)* - **To map:** Microsoft, Meta, and Snap equivalents; browser-level relays (the AB 1856 direction); and how each behaves on **shared, family/supervised, and school-managed devices**.

Oregon EdTech Deep Dive

Completed: ODE interim-testing requirements analyzed and SB 141 §§24–25 pinned (§1A); Oregon's existing student-data and consumer-privacy statutes confirmed (OSIPA, OCPA, OCIPA — §1A), answering the earlier "does Oregon already have overlapping statutes?" question (it does). *Still open:* - Vendor privacy/data terms for the State Board-approved interim-test vendors (**iReady, MAP Growth, Cambium/Smarter Balanced, Star**) — what student data each collects, stores, and shares, measured against OSIPA. - Watch/transcribe the **Lake Oswego Granicus clip** if it will be used as an Oregon case study. - Oregon school-district device, student-data, and screen-time policies.

Civil Liberties / Constitutional Deep Dive

Substantially addressed in §12A (Constitutional Framework). FSC v. Paxton pin-pages now pulled (§1A-Pins). Remaining follow-ups:

- Pull pin-cites from the **Texas SB 2420 (CCIA v. Paxton)**, **Arkansas (Griffin)**, and **Louisiana (Murrill)** opinions before any are quoted in testimony.
- Develop the **anonymous-speech** analysis (not yet built in §12A).
- Develop **parental-rights** arguments on both sides (NetChoice's "parents, not government" frame vs. the sponsors' parental-empowerment frame).
- Track the live appellate split (11th Cir. FL/GA; 5th Cir. MS) for any ruling that shifts the scrutiny standard.

Privacy / Security Deep Dive

Overlaps with Technical Architecture A above; keep them cross-referenced.

- Age-verification breach history (note the §1A OCIPA hook and the Discord/ID-upload breach precedents).
- Risks of storing parent–child relationship data and supervised-account status.
- Risks of age tokens / `installID`-style identifiers becoming tracking or fingerprinting signals.
- Privacy-preserving credential best practices (threshold proofs; the EU proof-of-age counter-model in §9–10).
- Centralized vs. decentralized verification models.

---

20. Working Takeaway

Oregon should not let **child safety**, **school technology**, **app-store accountability**, and **operating-system age verification** collapse into one vague proposal.

What the verification pass established (June 2026):

- The **app-store gatekeeper model is constitutionally contested but operating.** Oregon's HB 3696 died in committee; Texas's SB 2420 was enjoined in Dec. 2025 but **took effect June 4, 2026** after the Fifth Circuit stayed the injunction; Utah narrowed its law and the challenge was dismissed; Louisiana delayed to 2027. Trial courts are skeptical of these laws, but appellate courts are increasingly letting them run pending appeal, and the merits are unresolved. Oregon would be legislating into genuine constitutional uncertainty — not a settled win for either side.
- The **OS age-signal model (AB 1043) is the leading template — and the bigger long-term concern.** It is enacted, effective Jan. 1, 2027, and not yet challenged. It may be more litigation-resistant than the app-store laws because it transmits a signal rather than blocking access, but it is untested. The concern is not that it will fail in court — it's that if it *succeeds*, it normalizes a persistent device-level age-attribute layer, and **AB 1856 already shows that layer being extended from the OS to browsers and websites.** The First Amendment is unlikely to constrain this; only the statute's own guardrails will (§12A, §15).
- **Oregon is not a blank slate.** OSIPA (student data), OCPA (under-16 data, strengthened Jan. 1, 2026), SB 1546 (AI companions), and EO 25-09 (school phones) already occupy much of this space. The burden is on sponsors to show what gap remains.
- **SB 141 is a live constraint.** Its state-mandated, three-times-a-year K-8 interim testing (in effect 2026-27, vendor transition by Aug. 30, 2027) collides directly with any "remove screens from young classrooms" framing.

Each model still has a different data architecture, privacy risk, constitutional risk, school-implementation burden, cybersecurity risk, and impact on adults, minors, families, schools, developers, and open-source systems.

Before Oregon drafts a 2027 bill, lawmakers should identify the exact layer they want to regulate, show what gap it fills beyond existing Oregon law, and prove that the chosen layer is necessary, proportionate, technically workable, and privacy-preserving. The strongest posture for BPA is not opposition — it is insisting on that proof, and on the §15 safeguards for whichever layer survives.

---

21. Full URL List

User-provided links

- https://www.distractionfreeschools.com
- https://www.oregon.gov/ode/accountability/pages/interim-tests.aspx
- https://loswegok12.granicus.com/player/clip/973?view_id=3&redirect=true

Safe School Technology package embedded links

- https://internetsafetylabs.org/wp-content/uploads/2022/12/2022-k12-edtech-safety-benchmark-national-findings-part-1.pdf
- https://www.hrw.org/news/2022/07/12/online-learning-products-enabled-surveillance-children
- https://internetsafetylabs.org/resources/reports/spotlight-report-1-school-mobile-apps-student-data-sharing-behavior/
- https://internetsafetylabs.org/wp-content/uploads/2023/06/2022-K12-Edtech-Safety-Benchmark-Findings-Report-2.pdf
- https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html
- https://marketbrief.edweek.org/meeting-district-needs/how-much-time-are-students-spending-using-ed-tech/2022/03
- https://www.cbsnews.com/news/digital-devices-screen-time-damaging-childrens-eyes-vision/
- https://www.fondation-reboot.org/wp-content/uploads/_docs/2019_NAEP_Data_Update_Memo.pdf
- https://postpressmag.com/articles/2023/the-importance-of-paper-in-learning-and-literacy/
- https://hechingerreport.org/the-dark-side-of-education-research-widespread-bias/
- https://scale.stanford.edu/sites/default/files/The%20Evidence%20Base%20on%20AI%20in%20K-12%20Report.pdf
- https://www.brookings.edu/articles/a-new-direction-for-students-in-an-ai-world-prosper-prepare-protect/

Model-bill and age-verification research links

- https://olis.oregonlegislature.gov/liz/2025R1/Measures/Overview/HB3696
- https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1043
- https://capitol.texas.gov/tlodocs/89R/billtext/html/SB02420F.HTM
- https://le.utah.gov/Session/2025/bills/introduced/SB0142.pdf
- https://legis.la.gov/legis/Law.aspx?d=1428945
- https://james.house.gov/news/documentsingle.aspx?DocumentID=247
- https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification
- https://developer.android.com/google/play/age-signals/overview
- https://developer.android.com/google/play/age-signals/use-age-signals-api
- https://support.google.com/googleplay/android-developer/answer/16569691?hl=en
- https://developer.apple.com/documentation/declaredagerange
- https://developer.apple.com/news/?id=f5zj08ey
- https://blog.google/innovation-and-ai/technology/families/google-approach-online-age-verification/
- https://www.ftc.gov/news-events/news/press-releases/2026/02/ftc-issues-coppa-policy-statement-incentivize-use-age-verification-technologies-protect-children

- https://www.eff.org/deeplinks/2026/05/one-step-forward-two-steps-back-cas-ab-1856-exempts-open-source-expands-age-gating
- https://www.tomshardware.com/software/linux/california-moves-to-exempt-linux-from-its-upcoming-age-verification-law-after-backlash-over-forcing-operating-systems-to-collect-users-ages-amendment-proposed-by-the-same-lawmaker-who-wrote-the-original-law
- https://www.theverge.com/tech/930573/age-verification-bills-linux-open-source

---

22. Notes for Another LLM Model

This packet intentionally separates:

1. **School technology / EdTech regulation**
2. **App-store age verification**
3. **Operating-system age signals**
4. **Privacy-preserving proof-of-age credentials**

Please continue this work by:

- **reviewing the existing Levy memo (`levy_briefing_memo.md`), technical analysis (`os_age_signal_technical_analysis.md`), and plain-language explainer (`os_age_signals_explained.md`) for consistency, accessibility, technical accuracy, and missing citations** — all three derived documents already exist, so the task is review/refinement, not first drafting;
- extending the platform technical review (§19) to **Microsoft/Xbox, Meta/Snap/TikTok/Discord/Roblox, and browser-level relay behavior** — Google Play Age Signals and Apple Declared Age Range are already source-checked against the developer docs in the technical companion;
- pulling the **AB 1856 enrolled text** for final section numbers once it is chaptered;
- running a **same-day litigation-status check** (especially Texas SB 2420's Fifth Circuit posture, plus AB 1856 progress and any AB 1043 litigation) before any formal use;
- developing the **anonymous-speech** and **parental-rights** analyses flagged in §12A.

Statutory citations, litigation status, effective dates, Oregon legal context, and model amendments/safeguards have already been source-checked and pinned (see §1A, §1A-Pins, §6.1, §12A).