

P → C → D // UNRESOLVABLE

The Compliance Impossibility

Why ambient biometric devices cannot comply with amended COPPA.

The device must break the law to find out whether it is breaking the law.

A scan is the collection. The collection is the regulated act. There is no age gate between a camera and a child's face, so the device must perform the regulated act to learn whether it needed permission to perform it. **No amount of engineering resolves a circular dependency.**

This is not a product bug. It is a category-wide structural impossibility inherent to ambient biometric sensing.

SOURCES FTC, Children's Online Privacy Protection Rule; Final Amendments, 90 Fed. Reg. 16,918 (Apr. 22, 2025); Gilly, The Compliance Impossibility (2026), sec. I.

Biometric identifiers are now children's "personal information."

COPPA's logic is sequential: **determine age first, then obtain consent before collecting.** That works for a web form with an age gate. It collapses when age determination itself *is* the regulated collection.

§ 312.2, NOW REGULATED

Facial templates

Faceprints

Voiceprints

Gait patterns

Iris / retina

Fingerprints

Apr 22, 2026

compliance deadline

Age determination is not a step before collection. It *is* the collection.

01 · CAPTURE

The camera captures facial geometry from everyone in range.

=

02 · ESTIMATE AGE

Estimating age **requires** processing that same geometry.

=

03 · COLLECTION

Processing biometric identifiers **is** the regulated act.

There is no age-determination operation that does not constitute biometric collection. D and C are the same act.

C collect biometric data from a subject

D determine whether the subject is a child

P obtain verifiable parental consent

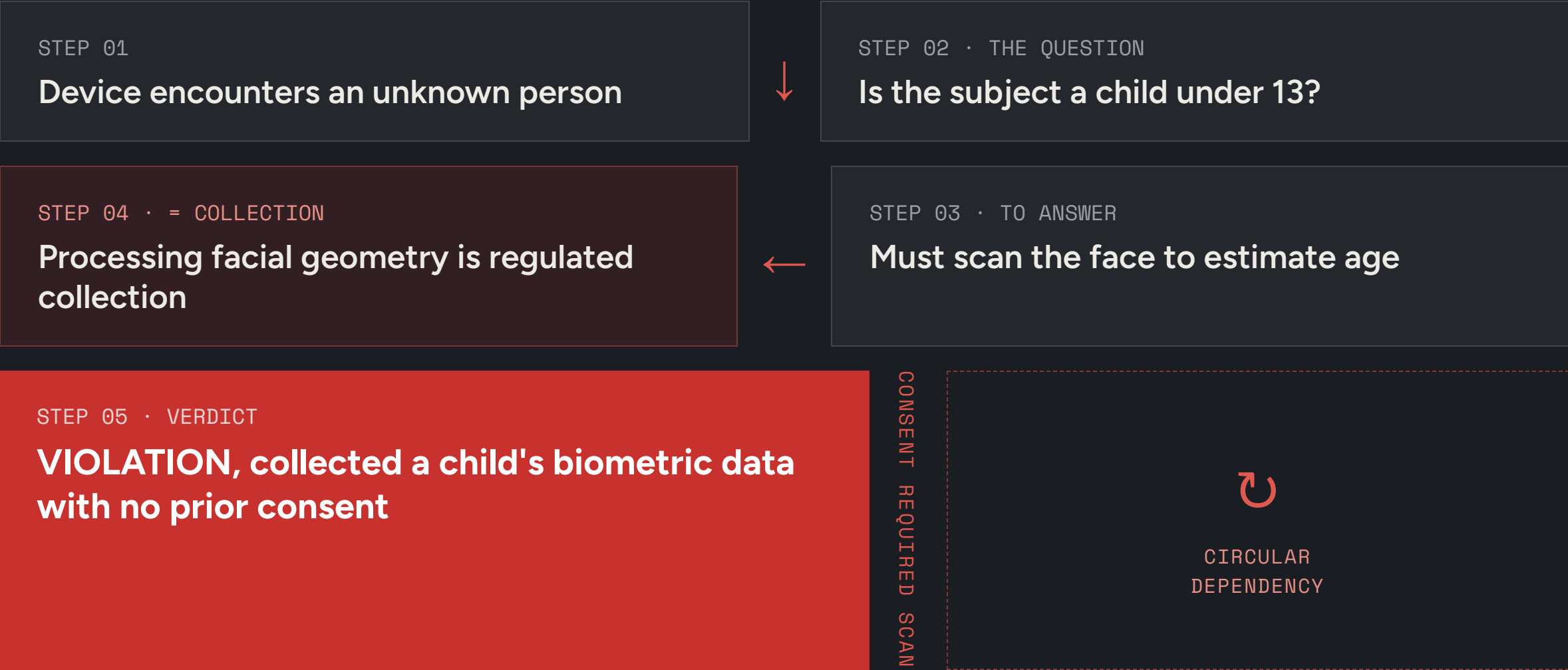
P → **C** → **D** required

but $D \subset C$ — and "need P" depends on D

∴ P must precede the operation that determines whether P was required.

D is a subset of C. They are the same act.

Consent must precede collection. Determining a child's status requires collection. So consent must precede the very act whose result determines whether consent was needed. **No reordering of operations resolves it.**

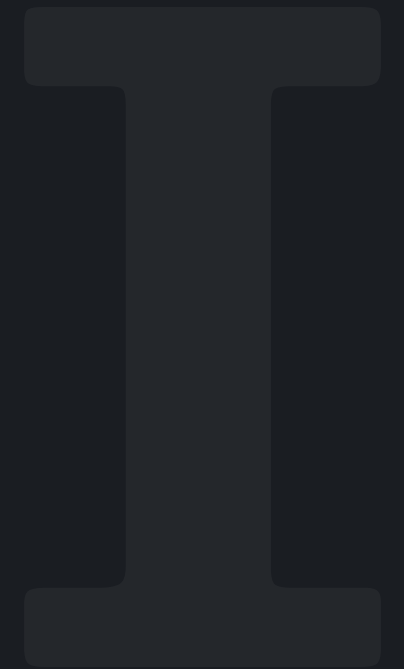


The device must perform the regulated act to determine whether the regulated act requires permission.

SOURCES 15 U.S.C. §§6501-6506 (COPPA); 90 Fed. Reg. 16,918 (2025).

No Way Out

Six engineering escapes are proposed. Each was raised in the rulemaking, and each fails.



The FTC was asked precisely these questions during the 2024–25 rulemaking, and declined to add any biometric exception. The volatile-memory defense was considered and rejected before the Rule was finalized.

Six proposed fixes. All collapse to the same circle.

On-device processing

COPPA regulates collection, not transmission. Edge AI just relocates the violation.

Immediate deletion

Discarding in 200 ms doesn't un-collect. The obligation attaches at capture.

Age estimation first

Estimating age is processing facial geometry, and least reliable at ages 10–12.

Bystander opt-out

Checking a do-not-scan list requires the identifying scan. The loop returns.

Geofencing

Children are everywhere. Disable sensing near them and you disable it everywhere.

De minimis / incidental

Commenters asked for this exception. The Commission expressly declined.

PRACTICAL DIFFICULTY

Hard, but achievable

Age verification is imperfect, but better technology or more investment could improve the result. The task is not contradictory.

VS

STRUCTURAL IMPOSSIBILITY

A logical contradiction

Consent-before-collection is incompatible with collection-before-determination. **No future technology resolves a contradiction.**

An Entire Product Class

Not one product, not one company, ten categories, dozens of shipping devices, the same structural defect.

Meta, Amazon, Apple, Google, Samsung, and numerous startups. Anything that processes biometrics from people in its environment, rather than from one consenting user, inherits the paradox.



The same defect, end to end across consumer technology.

Smart glasses / AR Meta Ray-Ban · Samsung · Google · Apple faceprints	AI pins / pendants Plaud NotePin · Humane · Project LUCI voiceprints	Home cameras Echo Show Visual ID · Nest face templates	Cashierless retail Amazon Just Walk Out · BIPA suit gait + face
Voice assistants Alexa · Google Assistant · Siri voiceprints	MR / AR headsets Meta Quest · Apple Vision Pro passthrough	Companion robots CES 2026 home robots face recog	Vehicle monitoring OEM occupant-monitoring systems driver ID
Connected toys Voice- & face-recognizing toys voice + face		Public-venue biometrics CLEAR · stadium & transit kiosks face ID	

SOURCES Counterpoint Research (2025); CNET (2026); MacRumors (2026); Hanif, AllAboutAI (2025); Harary, Darrow AI (2024), Amazon Just Walk Out BIPA suit. In no category has the cross-product structural impossibility previously been identified.

AI cameras streamed live footage of children on a playground, to the open internet.

December 2025: at least 60 of Flock Safety's Condor PTZ cameras left exposed with no authentication, no encryption, no access controls, deployed in parking lots, intersections, and playgrounds, auto-tracking individuals with AI.

60+

cameras exposed to the open internet, unauthenticated

30 days

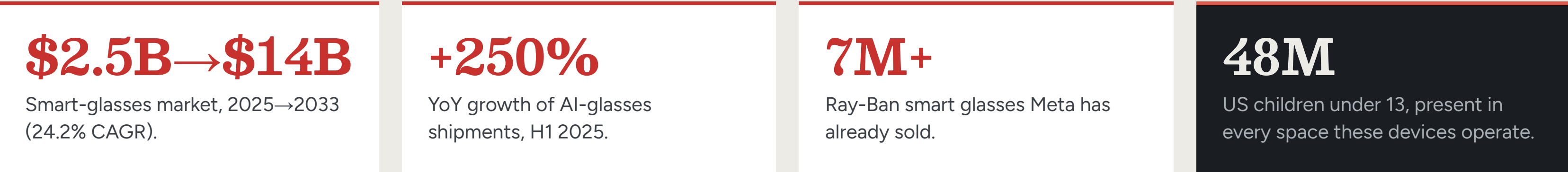
of stored video + full admin control, free to download

Four fields each saw a piece. None connected them.

SILO A Ambient devices capture bystander data	SILO B Children need heightened protection	SILO C COPPA now covers biometrics	SILO D Age estimation is unreliable
--	---	---------------------------------------	--

Σ *Together they imply a category-wide impossibility, visible only from a vantage point that takes in the whole landscape.*

Hundreds of billions resting on a legal assumption that does not hold.



An internal memo proposed launching facial recognition during a "dynamic political environment", while privacy advocates were distracted.

That is not a compliance plan. It is timing, distraction, and **fait accompli**, and it tells you the legal vulnerability is understood inside the company.

The less a manufacturer knows about its users, the stronger its legal position.

BUILD AGE ESTIMATION

Generates the actual knowledge that triggers liability

The instant the system flags a face as ~11, the operator knows it is processing a child's data.

REFUSE AGE ESTIMATION

Stronger defense, zero protection for children

Deliberate ignorance processes children's biometrics with no safeguards whatsoever.

The most responsible engineering approach is the legally self-defeating one.

\$275M Epic Games / Fortnite

Largest COPPA penalty ever, actual knowledge via surveys, toy deals, support tickets.

\$170M Google / YouTube

Sold itself to advertisers as a top kids' destination while denying under-13 users.

The deployment environment is itself the evidence.

The FTC read willful avoidance, not innocent ignorance, a combined **\$445M**. A device built to scan faces in parks, stores, and living rooms **will** encounter children. That is a census fact, not a marketing choice.

Four legal exits, none of them open.

First Amendment	A commercial server indexing a crowd ≠ a human glancing across a park. Commercial collection gets far lower protection.
Hardware / software split	FTC assesses the integrated product (as in Epic). Splitting the entity does not split the logical paradox.
Loper Bright / no Chevron	Courts may read "collection" independently, added risk for both sides, but no resolution under the Rule as written.
Safe Harbor	A program must be at least as protective as the Rule. It cannot authorize what the Rule prohibits.

"An entire technological era is about to discover it was never legal in the first place."

Three choices remain: redesign the product, lobby to weaken children's privacy, or proceed in knowing violation. The first is the only one consistent with the framework. The other two reveal what a company is actually optimizing for.

The device must break the law to find out whether it is breaking the law.

SOURCES Gilly, T. (2026). The Compliance Impossibility: Why Ambient Biometric Devices Cannot Comply with Amended COPPA. Working paper (v3), Real Safety AI Foundation.

— REFERENCES & AUTHORITIES

Gilly, T. (2026). *The Compliance Impossibility: Why Ambient Biometric Devices Cannot Comply with Amended COPPA*. Working paper (v3), Real Safety AI Foundation.

Children’s Online Privacy Protection Act of 1998, 15 U.S.C. §§6501-6506. CNET. (2026, January 7). Why Plaud’s newest tiny AI gadget is my CES 2026 secret weapon. https://www.cnet.com/tech/services-and-software/plauds-newest-wearable-ai-notetaker-is-my-ces-2026-se	Escobar-Planas, M., Gómez, E., & Martínez-Hinarejos, C.-D. (2022). Guidelines to develop trustworthy conversational agents for children. arXiv:2209.02403. https://arxiv.org/abs/2209.02403
Corbett, M., David-John, B., Shang, J., Hu, Y. C., & Ji, B. (2024). Securing bystander privacy in mixed reality while protecting the user experience. <i>IEEE Security & Privacy</i> , 22(1), 33–42. https://doi.org/10.1109/MSEC.2023.3331649	European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation), Arts. 4(14), 8, 9.
Counterpoint Research. (2025, August 11). Global smart glasses shipments soared 110% YoY in H1 2025, with Meta capturing over 70% share. https://counterpointresearch.com/en/insights/post-insight-research-br	Federal Trade Commission. (2023, May). Policy statement of the Federal Trade Commission on biometric information and Section 5 of the Federal Trade Commission Act. https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-biometric-information-section-5-fed
Libin, N., & Dharia, A. (2025, May 5). FTC amends COPPA Rule to address changes in technology and online practices. Davis Wright Tremaine LLP. https://www.dwt.com/blogs/privacy--security-law-blog/2025/05/coppa-rule-ftc-amended-childrens-privacy	Federal Trade Commission. (2025, April 22). Children’s Online Privacy Protection Rule; Final Amendments, 90 Fed. Reg. 16,918. https://www.federalregister.gov/documents/2025/04/22/2025-05904/childrens-online-privacy-protection-rule

— REFERENCES & AUTHORITIES (CONTINUED)

Federal Trade Commission & Department of Justice. (2022, December 19). Fortnite video game maker Epic Games to pay more than half a billion dollars over FTC allegations of privacy violations and unwanted charges [Press release]. <https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game->

Federal Trade Commission & Department of Justice. (2023, May 31). FTC and DOJ charge Amazon with violating children’s privacy law by keeping kids’ Alexa voice recordings forever and undermining parents’ deletion requests [Press release]. <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-re>

Federal Trade Commission & New York Attorney General. (2019, September 4). Google and YouTube will pay record \$170 million for alleged violations of children’s privacy law [Press release]. <https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-a>

Dupree, L. P., & Saeedi, Z. (2025, July 25). The FTC’s updated COPPA Rule: Redefining children’s digital privacy protection. Finnegan, Henderson, Farabow, Garrett & Dunner, LLP. <https://www.finnegan.com/en/insights/articles/the-ftcs-updated-coppa-rule-redefining-childrens-digital-privacy-phtml>

Gilly, T. (2026a). The device that can’t legally exist in a room with children [Substack post]. Real Safety AI Foundation. <https://open.substack.com/pub/travisgilly/p/the-device-that-cant-legally-exist>

Gilly, T. (2026b, February 16). The glasses that can’t legally look at your kids: Meta’s Name Tag and amended COPPA [Medium article]. Real Safety AI Foundation. <https://medium.com/@tgil212121/the-glasses-that-cant-l>

Grand View Research. (2026). Smart glasses market size, share & trends analysis report (2026–2033). <https://www.grandviewresearch.com/industry-analysis/smart-glasses-market-report>

Hanif, K. (2025, August 22). Meta’s new AI glasses could have a ‘super-sensing’ mode with facial recognition. AllAboutAI. <https://www.allaboutai.com/ai-news/metas-new-ai-glasses-could-have-a-super-se>

Hicks, M. L. (2026, January 14). CES 2026 laid out a Black Mirror future of wearable AI that’s always listening, watching, ready to help, and ‘knows everything about you.’ I’m not enthusiastic. Android Central. <https://www.androidcentral.com/wearables/ces-2026-laid-out-black-mirror-future-of-wearable-ai-th>

— REFERENCES & AUTHORITIES (CONTINUED)

Hill, K., Huang, K., & Isaac, M. (2026, February 13). Meta plans to add facial recognition technology to its smart glasses. The New York Times. <https://www.nytimes.com/2026/02/13/technology/meta-facial-recognition-smart-glasses.html>

Germano, C. (2026, January 26). Reminder: Amended COPPA Rule compliance date is approaching. BBB National Programs / Children’s Advertising Review Unit. [https://bbbprograms.org/media/insights/blog/coppa-amendedInternationalDataCorporation\(IDC\).](https://bbbprograms.org/media/insights/blog/coppa-amendedInternationalDataCorporation(IDC).) (2026,March25).XRmarketexpands44.4%in2025assmartglassestakecenterstage.<https://www.idc.com/promo/arvr/>

Bryan Cave Leighton Paisner LLP. (2026, January 16). U.S. biometric laws & pending legislation tracker – January 2026. JD Supra. <https://www.jdsupra.com/legalnews/u-s-biometric-laws-pending-legislation-87039>

Koebler, J. (2025, December 22). Flock exposed its AI-powered cameras to the internet. We tracked ourselves. 404 Media. <https://www.404media.co>

Loper Bright Enterprises v. Raimondo, 144 S. Ct. 2244 (2024) (overruling Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984)).

MacRumors. (2026, February 13). Meta plans ‘Name Tag’ facial recognition for Ray-Ban smart glasses. <https://www.macrumors.com/2026/02/13/meta-facial-recognition-smart-glasses/>

Shen, L., Thomson, A. C., & von Klein, M. P. (2025, April 28). FTC announces significant amendments to COPPA. Mayer Brown. <https://www.mayerbrown.com/en/insights/publications/2025/04/ftc-announces-s>

Niemeyer, K. (2024, October 13). The Harvard students who added AI facial recognition to Meta glasses share some of their other big ideas. Business Insider. <https://www.businessinsider.com/harvard-students-facial-rec>

Nguyen, A., & Ardayfio, C. (2025, January 29). I-XRAY: The AI glasses that reveal anyone’s personal details [Event with Prof. Jonathan Zittrain]. Harvard Library Innovation Lab. <https://lil.law.harvard.edu/events/i-xray-lunch/>

Perez, A. J., Zeadally, S., Matos Garcia, L. Y., Mouloud, J. A., & Griffith, S. (2018). FacePET: Enhancing bystanders’ facial privacy with smart wearables/Internet of Things. Electronics, 7(12), 379. <https://doi.org/10.3390/electronics7120379>

Quandary Peak Research. (2024, June). Expanding protections: Tracking new biometric privacy laws across the U.S. <https://quandarypeak.com/2024/06/expanding-protections-tracking-new-biometric-privac>

Harary, M. (2024, November 27). Amazon’s “Just Walk Out” tech faces BIPA lawsuit. Darrow AI. <https://www.darrow.ai/resources/amazon-bipa-lawsuit>

— REFERENCES & AUTHORITIES (CONTINUED)

Shahmansoori, A., & Roedig, U. (2022).
Dynamic recognition of speakers for
consent management by contrastive
embedding replay. arXiv:2205.08459.
<https://arxiv.org/abs/2205.08459>

State of Illinois. (2008). Biometric Information
Privacy Act, 740 ILCS 14. State and federal
age-knowledge statutes. See, e.g., Fla. Stat.
Ann. §501.1736 (treating willful disregard of
age as actual knowledge); Conn. Gen. Stat.
§42-515 et seq. (combining actual and
constructive knowledge standards);
Children and Teens’ Online Privacy
Protection Act (COPPA 2.0), S. 1628, 118th
Cong. (proposing constructive knowledge
standard for large platforms).

Takhshid, Z. (2024). Wearable AI, bystander
notice, and the question of privacy frictions.
Boston University Law Review, 104
(forthcoming).
<https://ssrn.com/abstract=4693396>

Davis, D.-M. (2025, May 23). Apple could
launch AI-powered smart glasses in 2026.
TechCrunch.
<https://techcrunch.com/2025/05/23/apple-could-launch-ai-powered-smart-glasses-in-2026/>

U.K. Information Commissioner’s Office. (2020). Age Appropriate Design Code (Children’s Code). <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information-compliance/code-of-practice-age-appropriate-design>
VIOLATIONCollectedchild’sbiometricdatawithoutpriorparentalconsentNoCOPPAobligation(butscanstilloccurred)Required:ParentalconsentBEFOREscanButconsentrequiresknowing