

No Compliance, No Enforcement:

What a State Attorney General Can Do About Ambient Biometric Devices While the Commission Will Not

Travis Gilly* 🦋 August 2026 (v0.7 draft)

Abstract

On February 25, 2026, the Federal Trade Commission announced that it will not bring enforcement actions under the Children’s Online Privacy Protection Rule against operators who collect personal information for the sole purpose of determining a user’s age. The announcement has been read as a general retreat from children’s privacy enforcement in the age of biometric sensing. That reading is wrong, and the error matters. The policy statement is narrow by its own terms. It reaches general audience and mixed audience services, it requires that the collection serve age determination and nothing else, it conditions relief on prompt deletion, and it withholds relief from any operator not otherwise in compliance. An ambient biometric device satisfies none of these conditions. It collects because collection is the product, it retains because retention is the product, and it collects from bystanders who are not its users at all. The Commission did not license ambient biometric collection. It built a lane that ambient devices cannot enter, and then declined to walk down the other one. This paper argues that the resulting gap is an enforcement gap rather than a legal one, and that it is a gap State attorneys general are already authorized to close. Section 6504 conditions State enforcement on a single obstacle, the pendency of a Commission action against the same defendant for the same regulation. Where the Commission has announced it will not act, that obstacle is absent by the Commission’s own representation. Section 6502(d) preempts only inconsistent State law, and the Ninth Circuit, with the Commission’s own agreement as amicus, has held that State causes of action which proscribe the same conduct COPPA proscribes are not inconsistent. The paper closes by taking the Commission’s premise seriously: if the measuring instrument cannot separate a child of twelve from a child of fourteen, a rule that turns on that boundary cannot be administered, and the boundary should be moved to where measurement is not required, as the European, United Kingdom, and South African regimes already illustrate in different ways.

Keywords: COPPA; age verification; age assurance; ambient biometric sensing; smart glasses; bystander consent; enforcement discretion; State attorneys general; parens patriae; preemption; children’s privacy; biometric identifiers.

*Travis Gilly is Founder and Executive Director of the Real Safety AI Foundation. ORCID: 0009-0007-2954-6313. Correspondence: t.gilly@ai-literacy-labs.org. The author discloses the use of speech-to-text software (Wispr Flow) and Anthropic’s Claude as assistive technology for a diagnosed neurodevelopmental condition. All legal analysis, case synthesis, theoretical framing, doctrinal arguments, and conclusions are solely the author’s own.

Contents

I	Introduction	3
II	The Carve Out and Its Boundaries	5
	A What the Statement Says	5
	B Relevant Operators, and Who Is Not One	6
	C The Six Conditions	7
	D The Trap in Footnote Nine	8
	E The Consequence	9
III	Measurement, Discretion, and Incapacity	9
	A The Instrument Cannot Locate the Line.	9
	B Discretion and Incapacity Are Different Things	11
IV	What a State Attorney General Can Do Today	12
	A Section 6504 Names One Obstacle	12
	B Non-Enforcement Removes the Only Bar	13
	C State Law Runs in Parallel, and the Commission Agrees.	14
	D The Bystander, After Zellmer and Samsung.	16
	E What the Package Looks Like.	19
V	If the Line Cannot Be Measured, Move the Line.	19
VI	Conclusion	21

I. Introduction

A prior work established that ambient biometric sensing devices face a structural compliance impossibility under the amended COPPA Rule. The argument runs as follows and is restated here as a premise. The Commission’s 2025 amendments expanded the definition of personal information to include biometric identifiers, among them facial templates, voiceprints, and gait patterns.¹ COPPA makes it unlawful for an operator of a child directed service, or any operator with actual knowledge that it is collecting personal information from a child, to collect that information in a manner violating the Commission’s regulations.² An ambient device must process biometric data from every person in its sensing field in order to function at all; the sensing that drives the product is the same sensing that exposes the bystander.³ To determine whether any given person in that field is a child, the device must first capture that person’s biometric. The capture is the regulated act. The device must break the law in order to learn whether it is breaking the law.

That is where the earlier argument stopped. This paper begins at the next question, which the earlier work could not have reached because the event had not yet occurred. On February 25, 2026, the Commission issued an enforcement policy statement announcing that it will not bring actions under the COPPA Rule against certain operators collecting personal information solely to determine a user’s age.⁴ The Commission announced the statement the same day by

1. Children’s Online Privacy Protection Rule, Statement of Basis and Purpose, 90 Fed. Reg. 16,918 (Apr. 22, 2025). The Commission’s enforcement policy statement confirms this citation and dates the Rule’s substantive revisions to 2013 and 2025. *See infra* note 4, at 1 nn.4–5.

2. 15 U.S.C. §6502(a)(1) (“It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).”).

3. See Joseph O’Hagan et al., *Privacy-Enhancing Technology and Everyday Augmented Reality*, 6(4) Proc. ACM on Interactive, Mobile, Wearable & Ubiquitous Techs. 1, 1 (2022) (finding that the “requisite sensing” that drives augmented reality wearables “opens the door” to activities including “biometric identification” that “expose bystanders to significant privacy risks,” and that always-on operation defeats access-control safeguards).

4. Fed. Trade Comm’n, COPPA – Enforcement Policy Statement Promoting the Adoption of Age-Verification Technology (Feb. 25, 2026), https://www.ftc.gov/system/files/ftc_gov/pdf/coppa-age-verification-policy-statement.pdf [hereinafter Enforcement Statement].

press release.⁵ The statement issued roughly eight weeks before the April 22, 2026 compliance deadline for the amendments that created the impossibility in the first place.⁶

The reception was broad and, on the whole, imprecise. Practitioner commentary described the statement as a relaxed enforcement position,⁷ as limited safe harbor protection,⁸ and as reassurance that the verification process itself will not trigger enforcement.⁹ Read at that altitude, the statement looks like a regulator confronting an impossible rule and responding by declining to apply it. If that were what happened, the impossibility argument would be intact but inert: correct on the law, irrelevant in practice, and awaiting a Commission that had already announced it was not coming.

That is not what happened, and the difference is the whole of this paper. Part II reads the statement against its full text and shows why ambient sensing falls outside every one of its conditions. Part III takes up the measurement problem the Commission's own record concedes, and distinguishes enforcement discretion from enforcement incapacity. Part IV is the operative part: what a State attorney general can do today, without the Commission, without a new statute, and without a change in federal posture. Part V argues that if the Commission's premise about measurement is correct, the protected class should be redefined at a boundary an instrument can find. Part VI concludes.

5. Press Release, Fed. Trade Comm'n, FTC Issues COPPA Policy Statement to Incentivize the Use of Age Verification Technologies to Protect Children Online (Feb. 25, 2026), <https://www.ftc.gov/news-events/news/press-releases/2026/02/ftc-issues-coppa-policy-statement-incentivize-use-age-verification-technol>

6. Davis Polk & Wardwell LLP, FTC Prioritizes COPPA Enforcement as New Compliance Obligations Take Effect (Apr. 16, 2026), <https://www.davispolk.com/insights/client-update/ftc-prioritizes-coppa-enforcement-new-compliance-obligations-take-effect>.

7. Greenberg Traurig LLP, FTC Signals Relaxed COPPA Enforcement for Age-Verification Technologies (Mar. 4, 2026), <https://www.gtlaw.com/en/insights/2026/3/ftc-signals-relaxed-coppa-enforcement-for-age-verification>

8. Cooley LLP, FTC Issues COPPA Enforcement Discretion Policy to Incentivize Use of Age Verification Technologies (Mar. 2, 2026), <https://www.cooley.com/news/insight/2026/2026-03-02-ftc-issues-coppa-enforcement-discretion-policy-to-incentivize-use-of-age-verification-technol> (“The policy statement offers limited safe harbor protection from the risk of enforcement by the FTC . . .”).

9. Mayer Brown LLP, FTC Issues Policy Statement on Age Verification Technologies Under COPPA (Feb. 26, 2026), <https://www.mayerbrown.com/en/insights/publications/2026/02/ftc-issues-policy-statement-on-age-verification-technologies-under-coppa>.

II. The Carve Out and Its Boundaries

A. *What the Statement Says*

The statement follows a January 28, 2026 public workshop at which Commission leadership acknowledged a tension between the Rule’s prohibition on collecting a child’s personal information without prior verifiable parental consent and the operation of age assurance tools that must process information about a user to estimate that user’s age.¹⁰ The Commission’s chairman opened the workshop by framing the project as ensuring the Rule “does not unduly inhibit” the technology.¹¹ The press release put the premise in one line: age verification technologies “play a critical role” in protecting children and helping parents.¹² The tension is real, and it is the same tension the impossibility argument identifies, arriving from the opposite direction. Where the impossibility argument says the Rule cannot be complied with, the Commission says the Rule should not be allowed to deter a technology it regards as protective.¹³

The statement defines its subject in a footnote, and the footnote is doing more work than the operative text. For the statement’s purposes, age verification “refers to a variety of tools used to obtain information about a user’s age, including: (1) age estimation tools that estimate a user’s age or age range; (2) age-verification tools that verify a user’s age; and (3) age inference tools that infer a user’s likely age or age range based on various signals.”¹⁴ Estimation, verification, and inference are three different epistemic acts with three different error structures, and the

10. Hogan Lovells, FTC COPPA Workshop and Policy Statement Promote Flexibility for Use of Age Verification Technologies (Mar. 19, 2026), <https://www.hoganlovells.com/en/publications/ftc-coppa-workshop-and-policy-statement-promote-flexibility-for-use-of-age-verification-technologies>; Greenberg Traurig, *supra* note 7 (dating the workshop to January 28, 2026, and quoting the Bureau of Consumer Protection director’s description of age verification technologies as “some of the most child-protective technologies to emerge in decades”).

11. Davis Polk, *supra* note 6 (quoting Chairman Ferguson’s January 28, 2026 workshop remarks).

12. Press Release, *supra* note 5.

13. Enforcement Statement, *supra* note 4, at 2 (“Age verification can play a critical role in protecting children online and helping parents as they monitor their children’s online activities.”).

14. *Id.* at 1 n.7.

statement folds them into one defined term without distinguishing among them. Part III returns to what that concession costs.

The response the Commission chose was a statement of prosecutorial intention rather than a rule amendment.¹⁵ The statement is explicit that it “does not create any substantive rights or entitlements,” that the Commission “retains the right to investigate and bring actions for violations of the COPPA Rule in individual cases,” and that it remains effective only until the Commission publishes final rule amendments on the issue or withdraws it.¹⁶

B. Relevant Operators, and Who Is Not One

The relief extends to what the statement calls Relevant Operators: operators of general audience services, and operators of mixed audience services, meaning child directed services that do not target children as their primary audience.¹⁷ Services primarily directed to children are excluded outright, and for them the Commission’s position is unchanged: they “must treat all users as children and therefore must provide the COPPA Rule’s protections to all users.”¹⁸

The taxonomy assumes a user. The statement describes the covered mechanism as one that determines a user’s age before that user interacts with the site or service.¹⁹ A general audience service is general as to its users; a mixed audience service is mixed as to its users. Every category in the frame is defined by the relationship between an operator and the people who come to it. An ambient sensing device collects from people who never came to it, and the empirical work on wearable capture confirms that the people collected from expect to be asked first, an expectation the form factor cannot honor at scale.²⁰ The bystander in the frame of a pair of smart

15. Hogan Lovells, *supra* note 10 (the statement “does not amend the COPPA Rule” and instead “articulates how the FTC intends to exercise its prosecutorial discretion” while rule amendments are evaluated).

16. Enforcement Statement, *supra* note 4, at 3.

17. *Id.* at 2 & n.8.

18. *Id.* at 2 n.8.

19. Enforcement Statement, *supra* note 4, at 2 (describing operators that have “determined a user’s age by simply requesting that the user provide his or her age before interacting with the site or service” and the mechanisms now replacing that request).

20. Soumyadeb Chowdhury et al., *Lifeloggging User Study: Bystander Privacy*, Proc. British HCI Conf. (2016) (reporting that bystander subjects uniformly expected a wearable camera user to obtain their consent before

glasses is not a general audience user or a mixed audience user. The bystander is not a user in any sense the taxonomy recognizes, which means the statement's central classification does not describe the transaction at issue.

C. *The Six Conditions*

The second boundary is the one doing the work, and the full text supplies five companions the summary coverage mostly omitted. The Commission's forbearance applies only where the Relevant Operator satisfies all six of the following: it does not use or disclose information collected for age verification purposes for any other purpose; it discloses that information only to third parties it has taken reasonable steps to vet, under written assurances of confidentiality, purpose limitation, and prompt deletion; it does not retain the information longer than necessary and deletes it promptly; it gives clear notice to parents and children in its privacy policy; it employs reasonable security safeguards; and it takes reasonable steps to determine that any tool it uses "is likely to provide reasonably accurate results as to the user's age."²¹ On top of all six sits a seventh, global condition: no forbearance "unless the Relevant Operator is complying with the COPPA Rule's requirements in every other respect with regard to personal information collected from children."²² Practitioner reaction registered the deletion condition as the pressure point most likely to be tested.²³

The statement gives the sole purpose condition a defined term, Age Verification Purposes, meaning collection, use, or disclosure "for the purpose of determining a user's age."²⁴ Applied to an ambient biometric device, the sole purpose condition is not merely difficult. It is definitionally

recording); Soumyadeb Chowdhury et al., *Bystander Privacy in Lifelogging*, Proc. British HCI Conf. (2016) (documenting bystander privacy concerns as a distinct problem from wearer privacy).

21. Enforcement Statement, *supra* note 4, at 2–3 (enumerating the six conditions).

22. *Id.* at 3; *accord* Cooley, *supra* note 8; Davis Polk, *supra* note 6 (both flagging the every-other-respect condition as the practical limit of the relief).

23. Keller & Heckman LLP, FTC Issues COPPA Enforcement Policy Statement Promoting Age-Verification Technology (Apr. 3, 2026), <https://www.khlaw.com/insights/ftc-issues-coppa-enforcement-policy-statement-promoting-age-verification-technology> ("it remains to be seen if this language will satisfy critics").

24. Enforcement Statement, *supra* note 4, at 2.

unavailable. Facial and voice processing on such a device exists to deliver the product’s function, whether that function is recognition, indexing, contextual response, or the training of downstream models. Age determination, where it occurs at all, is incidental to a collection that would occur regardless. There is no counterfactual in which the device collects the bystander’s face for age purposes and no other purpose, because the device would have collected the face anyway. The retention and deletion conditions fail with it: a device that retains as a matter of design cannot promptly delete what it exists to keep. The privacy policy notice condition presumes a party who could read the policy, which a street bystander is not. And the global condition is unavailable to an operator whose ambient collection is itself the unremedied violation.

D. The Trap in Footnote Nine

One passage of the statement deserves more attention than any commentary has given it. Addressing general audience operators, the Commission writes that in the course of using age verification mechanisms, an operator “may obtain actual knowledge about the age of a user,” and gives the example: a mechanism that identifies a user as eleven years old “would provide the operator with actual knowledge that the user is a child.”²⁵

The passage is framed as a warning to the operators the statement relieves: age verification mechanisms are one way, though “not the only way,” that actual knowledge arrives.²⁶ Read against an ambient device, that footnote is not a caveat. It is the whole case. A wearable that runs age estimation across its sensing field does not merely fail the conditions for forbearance; every child its models flag generates the actual knowledge that triggers the operator’s full obligations under section 6502(a)(1),²⁷ as to a person from whom verifiable parental consent was never and can never be obtained in advance. The statement’s own mechanics convert the device’s age determination capability from a compliance tool into a

25. Enforcement Statement, *supra* note 4, at 2 n.9.

26. *Id.* at 2 n.9 (“Note that general audience sites and services can also obtain actual knowledge through means other than utilizing an age-verification mechanism.”).

27. 15 U.S.C. §6502(a)(1); *see supra* note 2.

scienter generator. The more accurately the device estimates, the more actual knowledge its operator accumulates, and the forbearance built for websites cannot reach any of it.

E. The Consequence

The consequence inverts the common reading. The statement does not weaken the impossibility argument. It leaves the argument exactly where it stood and adds a datum: the Commission has examined the collision between age determination and prior consent, has relieved one class of operators from one narrow slice of it under seven cumulative conditions, and has left ambient biometric sensing outside the relief. Nothing in the statement's four pages mentions ambient devices, wearables, or bystanders at all.²⁸ The Commission's own announcement confines the relief to operators collecting "for the sole purpose of determining a user's age."²⁹ The silence is not an authorization. It is an absence.

III. Measurement, Discretion, and Incapacity

A. The Instrument Cannot Locate the Line

COPPA draws its protected class at thirteen.³⁰ An operator's obligations turn on whether the person whose information is collected is under that age, and the actual knowledge trigger presumes the answer is knowable in the ordinary case.³¹

Age estimation from biometric signal does not deliver that answer. It delivers a distribution. A system reports a most likely age with an error term, and the published evaluations put that error term, at its best, above a year and often several, with the borderline between minority and adulthood identified as the region where the instruments perform worst.³² The

28. See generally Enforcement Statement, *supra* note 4.

29. Press Release, *supra* note 5.

30. 15 U.S.C. §6501(1) (defining "child" as an individual under the age of 13).

31. The Commission's actual knowledge example presupposes exactly that determinacy: a mechanism that "identified a user as 11 years old." Enforcement Statement, *supra* note 4, at 2 n.9.

32. Felix Anda et al., *Improving Borderline Adulthood Facial Age Estimation Through Ensemble Learning*, ARES '19: Proc. 14th Int'l Conf. on Availability, Reliability & Sec. (2019) (surveying mean absolute error across studies of 1.47 to 8 years and describing performance at the adulthood borderline as a persistent challenge); Felix Anda

direction of the error compounds it: the same evaluations report that deployed commercial services systematically overestimate age in the underage range, which classifies minors as adults, the failure mode the statute exists to prevent.³³ The pattern holds across generations of the technology and across kinds of judge. The federal government’s own vendor evaluation, run over a corpus exceeding six million images, put the most accurate algorithm’s mean error at 4.3 years, with two thirds of estimates landing within five years of truth.³⁴ A 2026 benchmark of thirty four systems found the best general model missing by 4.32 years on average and specialized architectures by 9.88, and at the eighteen year threshold measured false adult rates for minors between 39 and 100 percent across specialized models, and between 16 and 29 percent even for the strongest new systems.³⁵ Human judges do no better, overestimating adolescents’ ages by three and a half years on average,³⁶ and machine error is not evenly distributed, varying measurably with the race, age, and gender of the person judged.³⁷ A reported fourteen and a true twelve are ordinary rather than exceptional outputs.

The Commission’s own record concedes the point in three places. Its 2024 notice of proposed rulemaking acknowledged that self declaration is unreliable and endorsed the development of alternatives.³⁸ The statement itself describes reliable determination as an emerging marketplace capability, citing a Congressional Research Service survey rather than a

et al., *Evaluating Automated Facial Age Estimation Techniques for Digital Forensics*, 2018 IEEE Sec. & Privacy Workshops 129 (attributing inaccurate predictions for minors to the absence of adequately labeled training data).

33. Anda et al., *Improving Borderline Adulthood Facial Age Estimation*, *supra* note 32 (reporting that evaluated services “tend to overestimate age” for subjects near the adulthood borderline, “which would lead to underage victims being classified as adults,” and measuring baseline accuracy for the sixteen to seventeen group at roughly one in six before ensemble correction).

34. M. Ngan et al., *Face Recognition Vendor Test (FRVT): Performance of Automated Age Estimation Algorithms*, Nat’l Inst. of Standards & Tech. (2014) (reporting a mean absolute error of 4.3 years for the most accurate participating algorithm and 67 percent of estimates within five years of actual age).

35. Simiao Ren et al., *Out of the Box Age Estimation Through Facial Imagery: A Comprehensive Benchmark of Vision-Language Models vs. Out-of-the-Box Traditional Architectures* (2026) (arXiv preprint).

36. R. Norja et al., *How Old Was She? The Accuracy of Assessing the Age of Adolescents Based on Photos*, Nordic Psych. (2021) (mean overestimation of 3.51 years for targets aged twelve to eighteen).

37. Zahra Stardust et al., *Mandatory Age Verification for Pornography Access: Why It Can’t and Won’t “Save the Children”*, Big Data & Soc’y (2024) (documenting racial, age, and gender bias in a widely deployed convolutional age classifier).

38. Children’s Online Privacy Protection Rule, Notice of Proposed Rulemaking, 89 Fed. Reg. 2034, 2048 (Jan. 11, 2024), cited in Enforcement Statement, *supra* note 4, at 2 n.10.

validation study.³⁹ And the sixth condition requires only “reasonably accurate results,” a standard that concedes on its face that exact results are not on offer.⁴⁰ A mature instrument does not need to be incentivized into existence.

B. Discretion and Incapacity Are Different Things

Enforcement discretion is a choice among available actions: a regulator with the capacity to prove a violation elects not to pursue it. Enforcement incapacity is different: the proof path does not exist. The statute’s trigger condition is a fact about a person; the instruments the Commission is encouraging cannot establish that fact within the tolerance the statute requires; and where the trigger cannot be established, an enforcement action premised on it has no reliable proof path. On the record the Commission has assembled, its position sits closer to incapacity than to discretion, and its announced intention to reopen the Rule is consistent with an agency that has recognized as much.⁴¹

Two consequences follow. First, a policy statement that does not amend the Rule cannot alter what the Rule requires. The Sixth Circuit put the principle plainly in an adjacent setting: “a statutory safe harbor is not very safe if a federal agency may add a new requirement to it through a policy statement,”⁴² because such a statement “offers non-binding advice about the agency’s enforcement agenda, not a controlling interpretation of the statute,” and binds neither courts nor the agency itself.⁴³ The deference framework has since shifted, and it shifted against agency statements; the core holding, that an enforcement policy is not law, now needs no deference doctrine at all.⁴⁴ The obligations of an operator on April 23, 2026 are the obligations the Rule

39. Enforcement Statement, *supra* note 4, at 2 n.10 (citing Cong. Rsch. Serv., Identifying Minors Online (Sept. 23, 2025), <https://www.congress.gov/crs-product/R47884>).

40. Enforcement Statement, *supra* note 4, at 3.

41. Enforcement Statement, *supra* note 4, at 3 (announcing the Commission’s intent “to initiate a review of the COPPA Rule to address age-verification mechanisms”).

42. *Carter v. Welles-Bowen Realty, Inc.*, 736 F.3d 722, 726 (6th Cir. 2013) (Sutton, J.).

43. *Id.* at 728 (denying both *Chevron* deference and *Skidmore* weight to a policy statement that purported to add conditions to a statutory safe harbor).

44. See *Loper Bright Enters. v. Raimondo*, 603 U.S. 369 (2024) (overruling *Chevron*). The Enforcement Statement says the same of itself. Enforcement Statement, *supra* note 4, at 3 (“This Enforcement Statement does not create any substantive rights or entitlements . . .”).

imposes, not the obligations the Commission has said it will pursue. Second, and more usefully, the symmetrical point: a non-enforcement posture that creates no rights against the Commission creates none against anyone else.

IV. What a State Attorney General Can Do Today

A. Section 6504 Names One Obstacle

Congress split COPPA enforcement between the Commission and the States,⁴⁵ and gave State attorneys general their authority from the statute's first day; the enforcement design is original to the 1998 enactment, contemporaneous with the Commission's initial rulemaking.⁴⁶ Where a State attorney general has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by a practice violating a Commission regulation prescribed under section 6502(b), the State may bring a civil action as *parens patriae* on behalf of its residents in federal district court, to enjoin the practice, to enforce compliance with the regulation, to obtain damages, restitution, or other compensation on behalf of residents, or to obtain such other relief as the court considers appropriate.⁴⁷ The *parens patriae* form is the ordinary vehicle for a State's quasi-sovereign interest in the health and well-being of its residents, and it does not require the State to identify individually injured plaintiffs.⁴⁸

The procedural conditions are light. The State must give the Commission written notice and a copy of the complaint before filing, and where advance notice is not feasible, notice and the complaint may be provided at filing.⁴⁹ The Commission may intervene, be heard, and appeal.⁵⁰ Nothing in the chapter prevents a State attorney general from exercising the investigative powers

45. 15 U.S.C. §6505(a) (Commission enforcement); see *Jones v. Google LLC*, 73 F.4th 636, 640 (9th Cir. 2023) (describing the two-track structure).

46. See Children's Online Privacy Protection Rule, Notice of Proposed Rulemaking, 64 Fed. Reg. 22,750 (Apr. 27, 1999), cited in Enforcement Statement, *supra* note 4, at 1 n.1 (tying the Rule to the 1998 statute).

47. 15 U.S.C. §6504(a)(1).

48. See *Alfred L. Snapp & Son, Inc. v. Puerto Rico ex rel. Barez*, 458 U.S. 592, 607 (1982) (recognizing a State's quasi-sovereign interest in the health and well-being, both physical and economic, of its residents).

49. 15 U.S.C. §6504(a)(2)(A)–(B).

50. 15 U.S.C. §6504(b).

conferred by that State's own laws, including the powers to conduct investigations, administer oaths, and compel witnesses and evidence.⁵¹ Venue follows the general federal venue statute, and process reaches any district where the defendant is an inhabitant or may be found.⁵²

Against that grant, the statute names exactly one bar: while an action instituted by or on behalf of the Commission is pending, no State may institute an action against a defendant named in the Commission's complaint for violation of the same regulation.⁵³

B. Non-Enforcement Removes the Only Bar

The structural point is small and, so far as the author has found, unmade in the commentary. The single statutory obstacle to State enforcement is the pendency of a federal action. The February statement is a public representation that, as to a defined class of conduct, no such action is coming, and as to ambient biometric sensing, the Commission has filed nothing in the sixteen months since the amendments were published.⁵⁴ A State attorney general assessing the practical risk of being displaced mid-litigation has the answer supplied by the record. The statement does not deprive the Commission of authority, and it is revocable by its own terms; what it cannot be revoked into is a pending action that existed at the time the State filed.

The Ninth Circuit has described the statutory architecture in exactly these terms: the statute confers enforcement authority on the Commission and on State attorneys general, who notify the Commission and proceed as *parens patriae*.⁵⁵ And State attorneys general have run this road before. New Mexico's litigation against an app developer, its embedded ad networks, and Google produced the working template, and its lessons cut in both directions. The court dismissed the COPPA count against the ad network defendants for failure to plead actual knowledge that the apps were child directed, holding that transmission of data from an embedded

51. 15 U.S.C. §6504(c).

52. 15 U.S.C. §6504(e).

53. 15 U.S.C. §6504(d).

54. See 90 Fed. Reg. 16,918, *supra* note 1.

55. *Jones v. Google LLC*, 73 F.4th 636, 640 (9th Cir. 2023) (describing the enforcement structure of 15 U.S.C. §§6504(a), 6505(a)).

kit to the network's servers does not, without more, impart actual knowledge, because the Rule deliberately holds ad networks to an actual knowledge standard⁵⁶ while holding the developers of child directed apps strictly liable.⁵⁷ Companion decisions carried the surviving counts forward.⁵⁸ And having dismissed the federal count for want of actual knowledge, the court dismissed the parallel State counts too, reasoning that treating the same conduct more strictly under State law than COPPA treats it would be the inconsistency the preemption clause forbids.⁵⁹ The template's lesson is pleading discipline: the knowledge element carries the complaint, federal and State alike.

For an ambient wearable the knowledge pleading is a different animal than it was for an ad network's embedded kit. The operator manufactures the sensor, runs the models, and processes the stream on its own infrastructure; the device's function is to apprehend the people in front of it; and the presence of children in public space is not a fact the operator can disclaim awareness of in the way a network could disclaim knowledge of one app's audience among thousands. Where the operator's own systems perform age estimation, the Commission's footnote closes the loop: the estimate is the actual knowledge.⁶⁰

C. State Law Runs in Parallel, and the Commission Agrees

A State attorney general is not confined to the federal count. COPPA's preemption clause forbids State liability "inconsistent with the treatment" of the covered activities under section 6502.⁶¹

56. *Balderas v. Tiny Lab Prods.*, 457 F. Supp. 3d 1103, 1121–25 (D.N.M. 2020).

57. *Id.* at 1124–25 (contrasting developers of child directed apps, "who are strictly liable for the collection of personal information from children," with ad networks, liable "only where they have actual knowledge that the apps are child-directed").

58. *Balderas v. Tiny Lab Prods.*, 516 F. Supp. 3d 1293 (D.N.M. 2021); *Balderas v. Google LLC*, 489 F. Supp. 3d 1254 (D.N.M. 2020).

59. *Tiny Lab*, 457 F. Supp. 3d at 1127 ("[B]ecause Plaintiff's COPPA claim fails as to the SDK Defendants for lack of actual knowledge, and because COPPA preempts state law that treats like conduct differently, Plaintiff's state law claims equally must fail for lack of actual knowledge.").

60. Enforcement Statement, *supra* note 4, at 2 n.9; *see supra* Part II.D.

61. 15 U.S.C. §6502(d).

District courts had once read that clause to occupy the field, reasoning that COPPA's enforcement scheme was clear and detailed and left no room for State law to add liability.⁶²

The Ninth Circuit reversed, holding that “COPPA’s preemption clause does not bar state-law causes of action that are parallel to, or proscribe the same conduct forbidden by, COPPA.”⁶³ State laws that supplement federal law, or require the same thing, do not stand as an obstacle to Congress’s objectives and so are not inconsistent; the contrary construction would read the word inconsistent out of the provision.⁶⁴ The court placed its holding in the long line of cases preserving State damages remedies for conduct federal regulation already proscribes.⁶⁵ The Commission itself told the panel so: on rehearing, the court quoted the Commission’s amicus position that the contrary reading “would have the extreme effect of providing immunity from a wide swath of traditional state law claims that were never discussed in COPPA’s legislative history.”⁶⁶ The agency now declining to enforce is the same agency that argued, in court, that State law enforcement survives.

The practical effect: a State attorney general may plead the section 6504 count and, in the same complaint, parallel State counts. The biometric count where the State has a biometric statute,⁶⁷ the eavesdropping count where the device records audio in an all party consent jurisdiction,⁶⁸ and the unfair practices count under the State’s own consumer statute, the same

62. *Hubbard v. Google LLC*, 508 F. Supp. 3d 623, 629 (N.D. Cal. 2020) (concluding the scheme “does not leave room for state laws to impose additional liability”); *Hubbard v. Google LLC*, 546 F. Supp. 3d 986 (N.D. Cal. 2021), rev’d sub nom. *Jones v. Google LLC*, 73 F.4th 636 (9th Cir. 2023).

63. *Jones*, 73 F.4th at 644.

64. *Id.* at 642–43 (holding also that express and conflict preemption collapse into one inquiry where the clause turns on inconsistency).

65. *Id.* at 643–44 (citing *Bates v. Dow Agrosciences LLC*, 544 U.S. 431, 448 (2005); *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 495 (1996); and *Wigod v. Wells Fargo Bank*, 673 F.3d 547, 581 (7th Cir. 2012), for the propositions that parallel State duties and remedies survive, and that the absence of a federal private right of action is no reason to dismiss a State claim incorporating a federal element).

66. *Id.* at 644 (quoting the Commission’s invited amicus brief).

67. See, e.g., 740 Ill. Comp. Stat. 14/15(b) (barring a private entity from collecting, capturing, or otherwise obtaining “a person’s or a customer’s” biometric identifier or biometric information absent written notice, disclosure of purpose and term, and a written release).

68. See, e.g., Cal. Penal Code §632 (confidential communications); 720 Ill. Comp. Stat. 5/14-2 (eavesdropping).

register in which the Rule itself speaks.⁶⁹ Practitioners on the defense side read the statement the same way: State rules governing the collection and processing of minors’ data, often intertwined with COPPA, continue to apply notwithstanding the Commission’s posture.⁷⁰ And the New Mexico court sustained the State’s standing to press even a common law intrusion on seclusion count in its *parens patriae* capacity, on the quasi-sovereign interest in the health and welfare of the State’s children.⁷¹ The federal count survives the Commission’s forbearance because forbearance is not preemption. The State counts survive because parallel is not inconsistent, and the Balderas symmetry then works in the State’s favor rather than against it: where the federal count is well pleaded, the parallel State counts demanding the same thing are, by the same logic, consistent.⁷²

D. The Bystander, After Zellmer and Samsung

The theory has one contested seam, and the two controlling appellate decisions, one of them eleven days old, now define it precisely.

The first question is whether a bystander is protected at all. It is answered. In *Zellmer*, the district court had granted summary judgment on the ground that it would be “patently unreasonable” to require a platform to obtain consent from “total strangers” with whom it had no relationship.⁷³ The Ninth Circuit rejected that reasoning outright: section 15(b) of the Illinois statute forbids collecting “a person’s or a customer’s” biometrics, and by delineating between

69. 16 C.F.R. §312.1 (the Rule “prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet”), quoted in *Tiny Lab*, 457 F. Supp. 3d at 1113.

70. Ogletree Deakins, FTC Releases COPPA Policy Statement Promoting Age Verification Technology (Mar. 2, 2026), <https://ogletree.com/insights-resources/blog-posts/ftc-releases-coppa-policy-statement-promoting-age-verification-technology/> (observing that intertwined State rules on minors’ data “still apply” and that enforcement risks persist).

71. *Tiny Lab*, 457 F. Supp. 3d 1103 (holding the complaint adequately articulated a quasi-sovereign interest in the health and welfare of New Mexico children sufficient to carry the intrusion on seclusion claim against the network defendant in the State’s *parens patriae* capacity).

72. See *Tiny Lab*, 457 F. Supp. 3d at 1127; Jones, 73 F.4th at 644.

73. *Zellmer v. Facebook, Inc.*, No. 3:18-cv-01880-JD, 2022 WL 976981, at *3 (N.D. Cal. Mar. 31, 2022), quoted in *Zellmer v. Meta Platforms, Inc.*, 104 F.4th 1117, 1122 (9th Cir. 2024).

persons and customers the statute protects non-users regardless of any preexisting relationship.⁷⁴ The defendant prevailed anyway, on a narrower ground with a longer reach: the face signatures at issue were ephemeral numerical abstractions, deleted within a fraction of a second, incapable of being reverse engineered, and incapable of identifying anyone, and an artifact that cannot identify a person is not a biometric identifier at all.⁷⁵

The second question is whose conduct counts. Eleven days before this draft, the Seventh Circuit held that the operative verbs of sections 15(a) and 15(b), possess, collect, capture, and obtain, all require the defendant to have gained some degree of control over the biometric data, and affirmed dismissal where a device manufacturer supplied the phones and the gallery software that generated face templates but never itself accessed, used, or exercised control over data that lived only on the users' own devices.⁷⁶ The court took its definitions from the Illinois Supreme Court, which reads the section 15(b) verbs to “mean to gain control,”⁷⁷ and distinguished the pleading that had survived against another device maker on allegations of exclusive control over data held on the device.⁷⁸

Read together, the decisions replace the folk objection with a test of two elements. A bystander biometric claim survives where the artifact is capable of identifying a person and the defendant controls the data. Neither element resembles the gallery app or the ephemeral face signature when the device at issue is an ambient wearable whose voice and image processing runs through the operator's own servers and whose facial recognition capability has been confirmed on shipping hardware. In June 2026, the Electronic Frontier Foundation's Threat Lab confirmed through static analysis, following reporting by Wired, that facial recognition code had been

74. *Zellmer v. Meta Platforms, Inc.*, 104 F.4th 1117, 1122–23 (9th Cir. 2024).

75. *Id.* at 1123–25 (affirming on the distinct ground that no material dispute existed over whether face signatures can identify a person).

76. *G.T. v. Samsung Elecs. Am., Inc.*, No. 25-1120, slip op. at 2, 10–14 (7th Cir. Aug. 7, 2026).

77. *Cothron v. White Castle Sys., Inc.*, 216 N.E.3d 918, 923–24 (Ill. 2023) (defining “collect” and “capture” and concluding the active verbs of section 15(b) all mean to gain control), quoted in *G.T.*, slip op. at 11–12.

78. *Hazlitt v. Apple Inc.*, 543 F. Supp. 3d 643, 653 (S.D. Ill. 2021) (allegations that only the manufacturer could access or disable the on device biometric database sufficed at the pleading stage), distinguished in *G.T.*, slip op. at 12–13.

deployed to millions of the leading smart glasses line's devices: the feature converts every face in the glasses' sightlines into a faceprint of 2,048 numbers uniquely representing the positioning of facial features and compares it against stored faceprints, and a researcher who added a face to the database in debug mode watched the glasses subsequently detect that face; the operator stripped the unactivated code days after publication.⁷⁹ Members of the Senate had put the company on written notice in March that glasses of this kind could capture thousands of faces without knowledge or consent and link them to identities.⁸⁰ Capability to identify and operator control are, on the public record, what this product category has built; the human computer interaction literature identified biometric identification of bystanders as the signature risk of the form factor before the code shipped.⁸¹ Those are pleading burdens, and they are pleadable.

The relocation point then does the remaining work. The impossibility argument never depended on the bystander holding a private remedy. Under section 6504 the plaintiff is the State, appearing as *parens patriae* for its residents,⁸² and the injury pleaded is the injury to the State's residents as a class rather than to a named individual who must establish a statutory relationship with the defendant. The federal count leads; the State biometric counts follow where identification capability and operator control can be pleaded; and the wiretap and UDAP counts run beside them, untouched by either decision.

79. Elec. Frontier Found., *Move Fast, Surveil Things* (June 4, 2026, updated June 8, 2026), <https://www.eff.org/deeplinks/2026/06/move-fast-surveil-things> (confirming the code's presence by static analysis and describing the faceprint architecture, the debug mode demonstration, and the June 8 removal following Wired's reporting); the underlying Wired investigation of June 4, 2026 is at <https://www.wired.com/story/meta-smart-glasses-face-recognition-nametag-connections/>; Elec. Frontier Found., *VICTORY: Meta Strips Facial Recognition Code from Smart Glasses App After Public Outcry* (June 8, 2026), <https://www.eff.org/deeplinks/2026/06/victory-meta-strips-facial-recognition-code-smart-glasses-app-after-public-outcry>.

80. Letter from Sen. Edward J. Markey et al. to Mark Zuckerberg, Chairman & CEO, Meta (Mar. 17, 2026), https://www.markey.senate.gov/imo/media/doc/letter_to_meta_on_frt_in_smart_glasses1.pdf.

81. O'Hagan et al., *supra* note 3, at 1.

82. 15 U.S.C. §6504(a)(1); Snapp, 458 U.S. at 607.

E. What the Package Looks Like

Assembled, a State attorney general holds the following today, on existing law, with no federal cooperation required beyond a copy of the complaint, which may arrive as the case is filed.⁸³ Investigative authority under State law, expressly preserved by section 6504(c).⁸⁴ A civil action in federal district court under section 6504(a)(1) for injunctive relief, compliance, and monetary relief for residents.⁸⁵ Parallel State counts that survive preemption under the Ninth Circuit's construction, a construction the Commission urged.⁸⁶ A knowledge theory the Commission's own footnote supplies.⁸⁷ And a federal regulator that has announced, as to the adjacent conduct, that it does not intend to be in the case.

V. If the Line Cannot Be Measured, Move the Line

The last part takes the Commission's premise seriously rather than contesting it. Suppose age assurance is the direction of travel and the instruments improve. They will still return a distribution rather than a fact, and the distribution will still be widest exactly where the statute draws its line.⁸⁸ A rule that turns on a boundary the measuring instrument cannot resolve is not a rule that becomes administrable with better engineering. It has selected the wrong boundary.

The boundary is difficult to defend on its own terms once measurement is conceded. A person of fourteen receives no protection from a statute that protects a person of twelve, notwithstanding that no available instrument can reliably distinguish them and that the commercial practices at issue do not change character across the line. The line was a legislative convenience in 1998. Sustaining it in 2026 requires an argument that the two cases differ, and the Commission's own account of measurement supplies the reason they cannot be told apart.

83. 15 U.S.C. §6504(a)(2)(B) (notice at filing where advance notice is not feasible).

84. 15 U.S.C. §6504(c).

85. 15 U.S.C. §6504(a)(1).

86. Jones, 73 F.4th at 644.

87. Enforcement Statement, *supra* note 4, at 2 n.9.

88. See *supra* notes 32–33 and accompanying text.

If the protected class were defined at eighteen, the measurement problem would not disappear, but it would move to where the instrument performs better and where the consequences of error invert: an adult misclassified as a minor receives protection unneeded, rather than a minor misclassified as an adult losing protection owed.⁸⁹

Comparable regimes already sit above thirteen, by three different mechanisms. The European regime treats every person under eighteen as meriting specific protection,⁹⁰ sets sixteen as the default age below which processing on a consent basis requires parental authorization for information society services offered directly to a child, and permits Member States to legislate a lower age no lower than thirteen.⁹¹ The United Kingdom took the derogation to its floor, setting the consent age at thirteen by statute,⁹² The regulator's guidance states the consequence without hedging: only children aged thirteen and over may lawfully provide their own consent, and an adult with parental responsibility must consent below that age.⁹³ And then it did the interesting thing: its design code, issued under a statutory mandate, regulates how services are built rather than who may consent, and applies to everyone under eighteen.⁹⁴ And South Africa simply defines the protected class at majority: a child is "a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or

89. See Anda et al., *Improving Borderline Adulthood Facial Age Estimation*, *supra* note 32 (documenting overestimation as the dominant error direction at the borderline).

90. Regulation (EU) 2016/679, recital 38, 2016 O.J. (L 119) 1 (children merit specific protection with regard to their personal data).

91. Regulation (EU) 2016/679, art. 8(1), 2016 O.J. (L 119) 1, 37 ("[T]he processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.").

92. Data Protection Act 2018, c. 12, §9 (UK); *id.* sch. 6, para. 11 (modifying art. 8 for domestic application); Explanatory Notes to the Data Protection Act 2018, §9 ("Any reference to age 16 in Article 8 of the GDPR, should be read as age 13 for the purposes of its application in the UK.").

93. Info. Comm'r's Off., What Are the Rules About an ISS and Consent?, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr-old/what-are-the-rules-about-an-iss-and-consent/>.

94. Info. Comm'r's Off., Age Appropriate Design: A Code of Practice for Online Services (2020) (issued under Data Protection Act 2018, c. 12, §123, and applying to information society services likely to be accessed by children, with child defined as a person under eighteen). The United Kingdom thus runs a thirteen year consent line and an eighteen year design line simultaneously, an official admission that consent age and protection age are different questions.

decision in respect of any matter concerning him- or herself,”⁹⁵ and the processing of children’s personal information is prohibited unless a statutory exception, principally the consent of a competent person, applies.⁹⁶

Three regimes, three structures, all reaching past thirteen, and one of them reaching the age this Part proposes. The American line is not a considered judgment the rest of the field rejected. It is a 1998 artifact the rest of the field declined to copy.

VI. Conclusion

The Commission did not decide that ambient biometric devices may collect children’s biometrics without parental consent. It decided something much smaller, about a different class of operators, doing a different thing, under seven cumulative conditions an ambient device cannot meet,⁹⁷ in a document that by its own terms creates no rights and awaits its own replacement.⁹⁸ The gap that remains is not a hole in the law. It is a hole in who is enforcing it.

Congress anticipated that hole and legislated for it.⁹⁹ Section 6504 exists because Congress did not intend children’s privacy enforcement to depend on the appetite of a single federal agency in a single administration. The statute conditions State authority on one thing only,¹⁰⁰ and on this conduct that condition is absent by the Commission’s own hand. The instrument is on the table. It has not been picked up.

❖ ❖

95. Protection of Personal Information Act 4 of 2013 §1 (S. Afr.) (definition of “child”).

96. *Id.* §§34–35 (prohibition and exceptions).

97. See *supra* Part II.C.

98. Enforcement Statement, *supra* note 4, at 3.

99. 15 U.S.C. §6504(a)(1); see *supra* Part IV.A.

100. 15 U.S.C. §6504(d).

References

- 720 Ill. Comp. Stat. 5/14-2.
- 740 Ill. Comp. Stat. 14/15.
- Alfred L. Snapp & Son, Inc. v. Puerto Rico ex rel. Barez, 458 U.S. 592 (1982).
- Anda, F., et al. (2018). Evaluating automated facial age estimation techniques for digital forensics. *2018 IEEE Security & Privacy Workshops*, 129.
- Anda, F., et al. (2019). Improving borderline adulthood facial age estimation through ensemble learning. *ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security*.
- Balderas v. Google LLC, 489 F. Supp. 3d 1254 (D.N.M. 2020).
- Balderas v. Tiny Lab Prods., 457 F. Supp. 3d 1103 (D.N.M. 2020).
- Balderas v. Tiny Lab Prods., 516 F. Supp. 3d 1293 (D.N.M. 2021).
- Bates v. Dow Agrosiences LLC, 544 U.S. 431 (2005).
- Cal. Penal Code §632.
- Carter v. Welles-Bowen Realty, Inc., 736 F.3d 722 (6th Cir. 2013).
- Children’s Online Privacy Protection Act, 15 U.S.C. §§6501–6506.
- Children’s Online Privacy Protection Rule, 16 C.F.R. pt. 312.
- Children’s Online Privacy Protection Rule, Notice of Proposed Rulemaking, 64 Fed. Reg. 22,750 (Apr. 27, 1999).
- Children’s Online Privacy Protection Rule, Notice of Proposed Rulemaking, 89 Fed. Reg. 2034 (Jan. 11, 2024).
- Children’s Online Privacy Protection Rule, Statement of Basis and Purpose, 90 Fed. Reg. 16,918 (Apr. 22, 2025).
- Chowdhury, S., Ferdous, M. S., & Jose, J. M. (2016). Bystander privacy in lifelogging. *Proceedings of the British HCI Conference*.
- Chowdhury, S., Ferdous, M. S., & Jose, J. M. (2016). Lifelogging user study: Bystander privacy. *Proceedings of the British HCI Conference*.
- Congressional Research Service. (2025). *Identifying Minors Online* (R47884).
- Cooley LLP. (2026). FTC issues COPPA enforcement discretion policy to incentivize use of age verification technologies.
- Cothron v. White Castle Sys., Inc., 216 N.E.3d 918 (Ill. 2023).
- Data Protection Act 2018, c. 12 (UK).
- Davis Polk & Wardwell LLP. (2026). FTC prioritizes COPPA enforcement as new compliance obligations take effect.
- Electronic Frontier Foundation. (2026). Move fast, surveil things.
- Electronic Frontier Foundation. (2026). VICTORY: Meta strips facial recognition code from smart glasses app after public outcry.

- Explanatory Notes to the Data Protection Act 2018, c. 12 (UK).
- Federal Trade Commission. (2026). *COPPA: Enforcement Policy Statement Promoting the Adoption of Age-Verification Technology*.
- Federal Trade Commission. (2026). FTC issues COPPA policy statement to incentivize the use of age verification technologies to protect children online [Press release].
- G.T. v. Samsung Elecs. Am., Inc., No. 25-1120 (7th Cir. Aug. 7, 2026).
- Greenberg Traurig LLP. (2026). FTC signals relaxed COPPA enforcement for age-verification technologies.
- Hazlitt v. Apple Inc., 543 F. Supp. 3d 643 (S.D. Ill. 2021).
- Hogan Lovells. (2026). FTC COPPA workshop and policy statement promote flexibility for use of age verification technologies.
- Hubbard v. Google LLC, 508 F. Supp. 3d 623 (N.D. Cal. 2020).
- Hubbard v. Google LLC, 546 F. Supp. 3d 986 (N.D. Cal. 2021), rev'd sub nom. Jones v. Google LLC, 73 F.4th 636 (9th Cir. 2023).
- Information Commissioner's Office. (2020). *Age Appropriate Design: A Code of Practice for Online Services*.
- Information Commissioner's Office. (n.d.). What are the rules about an ISS and consent?
- Jones v. Google LLC, 73 F.4th 636 (9th Cir. 2023).
- Keller & Heckman LLP. (2026). FTC issues COPPA enforcement policy statement promoting age-verification technology.
- Loper Bright Enters. v. Raimondo, 603 U.S. 369 (2024).
- Markey, E. J., et al. (2026). Letter to Mark Zuckerberg, Chairman and CEO, Meta.
- Mayer Brown LLP. (2026). FTC issues policy statement on age verification technologies under COPPA.
- Medtronic, Inc. v. Lohr, 518 U.S. 470 (1996).
- Ngan, M., et al. (2014). Face Recognition Vendor Test (FRVT): Performance of automated age estimation algorithms. *National Institute of Standards and Technology*.
- Norja, R., et al. (2021). How old was she? The accuracy of assessing the age of adolescents based on photos. *Nordic Psychology*.
- O'Hagan, J., Saeghe, P., Gugenheimer, J., et al. (2022). Privacy-enhancing technology and everyday augmented reality. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 6(4), 1.
- Ogletree Deakins. (2026). FTC releases COPPA policy statement promoting age verification technology.
- Protection of Personal Information Act 4 of 2013 (S. Afr.).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
- Ren, S., et al. (2026). Out of the box age estimation through facial imagery: A comprehensive benchmark of vision-language models vs. out-of-the-box traditional architectures. *arXiv*.
- Stardust, Z., et al. (2024). Mandatory age verification for pornography access: Why it can't and won't "save the children". *Big Data & Society*.
- Wigod v. Wells Fargo Bank, N.A., 673 F.3d 547 (7th Cir. 2012).

Zellmer v. Facebook, Inc., No. 3:18-cv-01880-JD, 2022 WL 976981 (N.D. Cal. Mar. 31, 2022).

Zellmer v. Meta Platforms, Inc., 104 F.4th 1117 (9th Cir. 2024).