

The Compliance Impossibility:

Why Ambient Biometric Devices Cannot Comply with Amended COPPA

Travis Gilly

ORCID: 0009-0007-2954-6313

Real Safety AI Foundation

Illinois, United States

Working paper, February 2026 (v3)

ABSTRACT

The Federal Trade Commission's 2025 amendments to the Children's Online Privacy Protection Act (COPPA) Rule expanded the definition of personal information to include biometric identifiers such as facial templates, voiceprints, and gait patterns. Under COPPA, operators must obtain verifiable parental consent before collecting personal information from children under 13. This paper identifies a structural compliance impossibility affecting an entire class of consumer technology products: ambient biometric sensing devices. These devices, which include smart glasses with facial recognition, AI powered wearable recorders, smart home cameras with person identification, cashierless retail systems, and mixed reality headsets, must process biometric data from every person in their sensing environment to function. When children are present in that environment, the device must collect a child's biometric data to determine whether the subject is a child, but that collection itself constitutes collection of children's personal information requiring prior parental consent under amended COPPA. The device must break the law to determine whether it is breaking the law. This paper demonstrates that this paradox is not a product specific engineering problem but a category wide structural impossibility inherent to ambient biometric sensing. We survey ten product categories encompassing dozens of shipping and announced devices from companies including Meta, Amazon, Apple, Google, Samsung, and numerous startups, demonstrating that the impossibility applies universally. We further show that existing legal scholarship and regulatory guidance has not identified this cross product structural problem, treating bystander biometric collection as a product specific compliance challenge rather than a systemic regulatory paradox. With the COPPA compliance deadline of April 22, 2026, approaching, hundreds of billions of dollars in planned product launches face a legal obstacle that cannot be engineered around.

Keywords: COPPA, biometric identifiers, ambient sensing, facial recognition, children's privacy, regulatory compliance, smart glasses, wearable AI, structural impossibility, consent paradox

I. INTRODUCTION

Consider a pair of smart glasses equipped with facial recognition. The wearer walks through a park. The glasses scan every face in their field of view, processing facial geometry to determine whether each person is a recognized contact. Some of those faces belong to children.

Under the amended COPPA Rule, facial geometry is biometric data. Biometric data is personal information.

Collecting personal information from a child requires verifiable parental consent before the collection, not after.

But the system has no way to determine whether a face belongs to a child without first scanning that face. The scan is the collection. The collection is the regulated act. The device must perform the regulated act to determine whether it needs permission to perform the regulated act.

This is not an engineering problem with an engineering solution. It is a logical impossibility. No amount of computational sophistication, edge processing, privacy preserving design, or consent management can resolve a circular dependency between the precondition for compliance (knowing whether the subject is a child) and the act that triggers the compliance obligation (collecting biometric data from that subject).

This paper demonstrates that this impossibility is not unique to smart glasses or to any single product. It is structural to an entire class of consumer technology: ambient biometric sensing devices. Any device that processes biometric identifiers from people in its environment to function, rather than from a single consenting user, faces the same paradox whenever children may be present in that environment. Since children exist in virtually every public and domestic space where these devices operate, the impossibility is effectively universal for the product class.

We survey ten product categories encompassing devices from major technology companies and numerous startups, all of which share this structural characteristic. We examine the amended COPPA Rule's specific provisions that create the impossibility. We review the existing legal and academic literature to demonstrate that, while individual privacy concerns have been raised about specific products, no prior published analysis has identified the cross product structural impossibility as a category wide regulatory paradox. Finally, we discuss implications for the approaching April 22, 2026, compliance deadline and for the broader trajectory of ambient computing.

II. THE AMENDED COPPA RULE AND BIOMETRIC IDENTIFIERS

The Children's Online Privacy Protection Act of 1998 established a framework requiring operators of websites and online services directed at children under 13 to obtain verifiable parental consent before collecting personal information from those children. The FTC adopted implementing regulations (the COPPA Rule) in 2000 and last updated them in 2013.

On April 22, 2025, the FTC published comprehensive amendments to the COPPA Rule. The amendments became effective June 23, 2025, with a compliance deadline of April 22, 2026, for most provisions. Among the most significant changes was the expansion of the definition of personal information under § 312.2 to include biometric identifiers.

The amended Rule defines regulated biometric identifiers as those that can be used for the automated or semi-automated recognition of an individual, such as fingerprints; handprints; retina patterns; iris patterns; genetic data, including a DNA sequence; voiceprints; gait patterns; facial templates; or faceprints. The FTC deliberately chose not to include the broader category of data derived from voice data, gait data, or facial data that had been proposed in the January 2024 Notice of Proposed Rulemaking, but made clear that templates derived from such data and used for recognition purposes fall within the definition.

The COPPA framework's core mechanism is sequential: first, determine whether children under 13 are present; second, if so, obtain verifiable parental consent before collecting their personal information. This sequence functions adequately for traditional online services, where age can be assessed through neutral age gates, date of birth prompts, or account registration flows before any biometric data is collected. The user interacts with a digital interface, identifies their age through that interface, and the operator routes them accordingly.

The amended Rule preserves this sequential logic. Mixed audience operators are permitted to collect minimal data for age screening in a neutral manner before applying full COPPA protections. But the contemplated models are

classical web and application flows, not continuous sensing of every person in a device’s physical environment.

A threshold question is whether manufacturers of ambient biometric devices qualify as operators under COPPA, which applies to operators of websites or online services. The amended Rule defines online service broadly to include any service available over the internet or that connects to the internet, including services that connect to the internet to collect information. Virtually every device catalogued in this paper transmits biometric data to cloud infrastructure for AI processing, stores processed data on remote servers, or requires internet connectivity for core functionality. Meta’s smart glasses rely on Meta’s AI assistant; Amazon’s Echo Show connects to Amazon’s cloud for Visual ID processing; cashierless retail systems transmit tracking data to centralized servers; AI wearable recorders send audio to cloud transcription services. Even devices capable of on-device processing typically require internet connectivity for model updates, feature activation, and data synchronization. A manufacturer that deliberately architects a fully offline device specifically to escape operator status would be engaged in the same regulatory evasion strategy the FTC has already penalized: structuring operations to avoid triggering obligations the manufacturer knows would otherwise apply.

This is where the structural problem emerges. For ambient biometric sensing devices, there is no pre-collection interaction with the data subject. There is no age gate between the device’s camera and a child’s face. There is no registration flow between the device’s microphone and a child’s voice. The device processes biometric data from everyone in its sensing radius as a condition of functioning, and some of those people are children. The sequential logic of COPPA (determine age, then decide whether to collect) collapses when age determination itself requires the collection that COPPA regulates.

III. THE STRUCTURAL IMPOSSIBILITY

A. Formal Statement

The impossibility can be stated precisely. Under the amended COPPA Rule, collecting biometric identifiers from a child under 13 requires verifiable parental consent obtained before the collection occurs. To determine whether a subject is a child under 13 in an ambient sensing environment, the device must process biometric data from that subject (at minimum, facial geometry sufficient to estimate age, or voice characteristics sufficient to estimate age from vocal features). Processing biometric data from that subject is, under the amended Rule, collection of personal information. If the subject is a child, the collection required verifiable parental consent that was not and could not have been obtained, because the child’s status as a child was unknown until the collection occurred.

More formally: Let C represent the act of collecting biometric data from a subject. Let D represent the act of determining whether that subject is a child. Let P represent obtaining verifiable parental consent. COPPA requires: if D yields “child,” then P must precede C . But D requires C . Therefore P must precede C , which must precede D , which determines whether P was required. The temporal ordering $P \rightarrow C \rightarrow D$ is required, but D depends on C , and the requirement for P depends on D . This is a circular dependency that cannot be resolved by reordering operations. Critically, D is not a separate step from C ; it is a subset of C . Any automated analysis of facial geometry sufficient to estimate age necessarily processes the biometric identifiers that the amended Rule defines as personal information. There is no age determination operation that does not constitute biometric collection. D and C are the same act, which means P must precede the very operation whose result determines whether P was required.

B. Why Engineering Cannot Resolve the Paradox

Several technical approaches might appear to offer solutions. None withstand scrutiny.

On-device processing. Some manufacturers argue that processing biometric data locally, without transmitting it

to cloud servers, mitigates privacy concerns. But COPPA regulates collection, not transmission. The amended Rule defines collection broadly. When a device captures facial geometry and processes it through recognition algorithms, collection has occurred regardless of where the processing takes place. Edge AI does not circumvent COPPA; it merely changes the location of the violation.

Immediate deletion. A device could theoretically scan a face, determine it is not a recognized contact, and immediately delete the captured data. But the scan itself is collection of biometric data. Deletion after collection does not retroactively un-collect the data. The COPPA obligation attaches at the moment of collection, not at the moment of retention. The FTC's enforcement action against Amazon over Alexa voice recordings confirmed that collection and retention are separate regulatory events, both independently regulated. Moreover, during the 2024-2025 rulemaking process, multiple commenters and one FTC-approved COPPA Safe Harbor program specifically requested an exception for the temporary use of biometric data for purposes such as age verification, followed by prompt deletion (FTC, 2025, 16927-28). The Commission explicitly declined, stating that it had decided not to add any additional exceptions to COPPA Rule requirements related to biometric data at this time, other than the narrow exception for audio files containing a child's voice collected solely to respond to a specific request. This is not a gap in the regulatory record; the FTC was asked precisely the question that the ephemeral processing defense raises, and answered it in the negative. The volatile memory argument was considered and rejected before the amended Rule was finalized. It bears emphasis that the statutory text regulates collection, not storage. Processing biometric data in volatile memory, in a temporary buffer, or in an ephemeral computational pipeline is still processing. The facial geometry is still extracted. The algorithmic comparison is still performed. The biometric template is still generated, however briefly it persists. The COPPA Rule does not condition its consent requirement on the durability of the medium in which collection occurs. A device that captures a child's facial geometry, processes it through a recognition algorithm in RAM, and discards the result in 200 milliseconds has still collected that child's biometric data within the meaning of the statute. The collection event is the computational act, not the storage decision that follows it.

Age estimation before recognition. A device could attempt to estimate a subject's age before performing full biometric recognition, using coarser visual features that might not constitute biometric templates. However, any automated analysis of facial features sufficient to estimate age with reasonable accuracy involves processing facial geometry, which the amended Rule covers. The FTC's biometric policy statement explicitly warns that biometric systems may infer age, gender, and other traits from facial and voice data, placing such inference within the regulatory ambit. Moreover, age estimation from facial features is unreliable for the 10-to-12 age range most critical for COPPA compliance, where many children are physically indistinguishable from young adolescents above the statutory threshold. More fundamentally, the argument that age estimation from a raw camera frame is not recognition of an individual and therefore does not trigger the biometric identifier definition fails on close reading of the amended Rule. The Rule's definition covers biometric identifiers such as the listed examples, making the enumeration illustrative, not exhaustive. Any age estimation algorithm that analyzes facial geometry, including bone structure proportions, facial feature spacing, and cranial dimensions, is processing the same underlying biometric data from which a faceprint could be generated. The input to the algorithm is facial geometry regardless of whether the output is labeled age estimate or face template. The FTC's 2023 biometric policy statement explicitly warns that biometric systems may infer age, gender, and other traits from facial and voice data, placing such inferences within the regulatory ambit. The label a manufacturer applies to the output of facial geometry processing does not change the nature of the input data collected.

Opt-out mechanisms. Proposals for bystander opt-out, such as wearing devices that signal do not scan or registering in a do not process database, shift the burden of compliance from the operator to the data subject. More fundamentally, COPPA requires affirmative parental consent before collection, not bystander opt-out after collection. A child's parent cannot opt out of a scan that has already occurred. Even a preregistered opt-out database would require the device to first identify the person (biometric collection) to check them against the database, recreating the same circular dependency.

Geofencing. Disabling biometric features near schools, playgrounds, or other child-dense areas would reduce but not eliminate the problem. Children exist in every public space: grocery stores, parks, sidewalks, airports, sporting events. A device that disables biometric sensing wherever children might be present would need to disable biometric sensing essentially everywhere, defeating its purpose.

De minimis or incidental collection. A final defense would argue that COPPA was designed for intentional, targeted collection of children's data, and that fleeting ambient capture of a child's face by a passing smart glasses wearer is analogous to a security camera capturing a child walking past a store. This analogy fails because traditional security cameras were not running facial recognition algorithms, were not generating biometric templates, and were not using artificial intelligence to identify, track, or classify individuals. The amended Rule added biometric identifiers precisely because the technology evolved beyond passive recording into active biometric processing. The distinguishing feature is not the camera; it is the algorithmic analysis performed on the captured image. When a device processes facial geometry through recognition, classification, or identification algorithms, it is performing the collection the Rule regulates, regardless of how briefly the data persists. Moreover, during the rulemaking process, commenters specifically requested exceptions for temporary or incidental biometric processing, and the Commission declined to adopt any such exception (FTC, 2025, 16927-28). The *de minimis* argument was raised, considered, and rejected before the amended Rule was finalized.

C. The Impossibility Is Structural, Not Practical

It is important to distinguish between practical difficulty and structural impossibility. Many regulatory compliance challenges are practically difficult but theoretically achievable. A company might struggle to implement effective age verification, but the task is not logically impossible; better technology or more investment could improve results.

The ambient biometric COPPA problem is categorically different. It is not that compliance is expensive, or technically challenging, or that current technology is insufficient. It is that the logical structure of the regulatory requirement (consent before collection) is incompatible with the logical structure of the technology (collection before determination). No future technology can resolve a logical contradiction. The paradox is as fundamental as the halting problem in computer science: it is not an engineering limitation but a structural property of the problem space.

IV. PRODUCT TAXONOMY: TEN CATEGORIES OF STRUCTURAL NONCOMPLIANCE

The following taxonomy demonstrates that the structural impossibility is not confined to a single product or company but pervades an entire class of consumer technology. Each category shares the same fundamental architecture: the device processes biometric identifiers from people in its sensing environment who have not consented to that processing, and some of those people are or may be children under 13.

A. Smart Glasses and AR Wearables with Facial Recognition

Meta's Ray-Ban smart glasses represent the most prominent example. Meta is reportedly developing an internal feature called Name Tag that would use facial recognition via Meta's AI assistant to identify people the wearer encounters. The feature would initially focus on people known through Meta platforms or with public Instagram accounts, but the underlying architecture requires scanning every face in the camera's field of view to determine whether any face matches a known contact. Internal documents acknowledge obvious civil liberties and privacy risks, and reporting indicates Meta considered timing the launch during a period when privacy advocates would be distracted by broader political battles.

In a 2024 demonstration, researchers paired off the shelf Ray-Ban Meta glasses with the PimEyes facial recognition service to identify strangers on public transit, retrieving names, addresses, and other personal details, without any bystander consent mechanism. This demonstrated that the technical capability for ambient facial identification from smart glasses already exists using commercially available components.

Meta is not alone. Samsung has announced Galaxy Glasses for 2026. Google has confirmed plans for AI powered smart glasses launching in 2026, leveraging its Gemini platform. Apple is reported to be developing smart glasses to compete with Meta's offerings. Xreal's Project Aura and Brilliant Labs' open source alternatives are also in development or shipping. Each of these platforms, to the extent it incorporates person detection, facial recognition, or visual AI features that process faces in the wearer's environment, faces the same structural COPPA impossibility.

B. AI Wearable Pins, Clips, and Pendant Recorders

A rapidly growing category of AI wearables continuously records ambient audio and, in some cases, video from the wearer's environment. Plaud's NotePin S, demonstrated and available for purchase at CES 2026, clips to clothing and records conversations within approximately a 10 foot radius, sending recordings to cloud services for AI transcription and summarization. The device is marketed for general purpose note taking, not enterprise or controlled environment use.

Under the amended COPPA Rule, voiceprints are biometric identifiers. Any device that records ambient audio and processes it through speech recognition, speaker identification, or AI transcription systems that distinguish between speakers is potentially creating voiceprint data from bystanders. When those bystanders include children, the same structural impossibility applies: the device cannot determine that a voice belongs to a child without first capturing and processing that voice, which is the collection event requiring prior parental consent.

Other devices in this category include Humane's AI Pin, SwitchBot's AI MindClip (described as a second brain that records all conversations and sends them to the cloud), Memories.ai's Project LUCI (a multimodal pin with a 109-degree camera), and numerous other CES 2026 entrants marketing always-on AI recording as a consumer lifestyle product.

C. Smart Home Cameras and Displays with Facial Recognition

Amazon's Visual ID feature on Echo Show devices uses facial recognition to personalize content when recognized users walk into view. The feature is always watching for enrolled faces once enabled. Visual ID profiles can be created for children tied to Amazon Kids accounts, making this explicitly a mixed age, multi user use case.

The structural problem is acute here because the domestic environment is where children under 13 are most consistently present. When Visual ID operates in a household with children, the camera must continuously capture and process facial geometry from everyone in view, including children and their visiting friends, to determine whether a recognized user is present. Google's Nest cameras with familiar-faces detection and numerous third-party camera vendors with person identification share the same architecture.

The FTC has already demonstrated willingness to enforce COPPA against smart home devices. The 2023 enforcement action against Amazon over Alexa established that retaining children's voice recordings and using them to train algorithms violated COPPA. But that action focused on retention and secondary use, not on the threshold question of whether ambient capture itself constitutes collection requiring prior consent. The structural impossibility identified here is upstream of the Alexa enforcement; it concerns whether the initial capture can lawfully occur at all.

D. Cashierless Retail and In-Store Tracking Systems

Amazon's Just Walk Out technology uses dense camera networks and computer vision to track every shopper's movements, identifying faces, hand gestures, and other biometric features to associate specific people with the items they take from shelves. In ongoing litigation under Illinois' Biometric Information Privacy Act, a court denied Amazon's motion to dismiss, rejecting the argument that the system does not collect biometric information.

Children accompany parents to stores. The Just Walk Out system cannot exclude children from its tracking; doing so would require first identifying them as children, which requires the biometric processing that triggers the COPPA obligation. The same logic applies to facial recognition systems used for loss prevention, customer identification, and biometric payment terminals deployed by retailers including Walmart, Amazon, and numerous grocery and convenience store chains.

E. Voice Assistants and Ambient Audio Devices

Voice assistants deployed in homes, including Amazon Alexa, Google Assistant, and Apple Siri on HomePod devices, continuously listen for wake words and process ambient audio to detect those triggers. When a child speaks near such a device, the device captures and processes that child's voice data. Under the amended Rule's inclusion of voiceprints as biometric identifiers, this processing may constitute collection of children's personal information.

The FTC's Alexa enforcement action confirmed regulatory attention to children's voice data in this context, but focused on post collection retention and use rather than on the structural impossibility of obtaining consent before the ambient capture occurs. The trajectory of voice assistant technology toward more continuous listening, contextual understanding, and speaker identification intensifies the structural problem as these devices process increasingly biometric grade voice data from everyone in the home, including children.

F. Mixed-Reality and AR Headsets with Passthrough Cameras

Modern mixed reality headsets such as Meta's Quest line and Apple's Vision Pro use outward facing cameras to capture the physical environment for passthrough video, spatial mapping, and person detection. Person occlusion (rendering virtual objects behind real people), social presence features, and hand tracking all require the device to detect, track, and in some cases identify people in the user's environment.

Privacy scholarship on MR devices has extensively catalogued the types of data captured about bystanders, including facial images, body posture, gaze direction, and environmental context, and proposed technical mitigations such as bystander face blurring (Corbett et al., 2024). However, this work has focused on privacy as a general data protection and ethical design problem. None of the identified literature connects bystander capture in MR to COPPA's biometric identifier definition or to the structural impossibility of age based consent branching when age determination itself requires biometric processing.

G. Social and Companion Robots

Social robots designed for home use increasingly incorporate facial recognition for personalization, greeting users by name, and adjusting behavior based on who is present. At CES 2026, companion robots were demonstrated that use facial recognition to greet users, memorize personal preferences, and express emotions in response to recognized individuals.

These devices are frequently marketed for family environments where children are the primary or co-primary users. A social robot that recognizes family members by face must process facial biometric data from every person it

encounters, including children and their friends who visit the home. The same structural paradox applies: the robot cannot determine whether a new face belongs to a child without the biometric scan that constitutes regulated collection.

H. Vehicle Occupant Monitoring Systems

An increasing number of vehicles incorporate interior cameras for driver monitoring, drowsiness detection, and occupant identification. Some systems use facial recognition to adjust seat positions, mirror angles, and infotainment preferences based on who is driving or sitting in the vehicle. When children are passengers, these systems capture and process their facial geometry alongside adult occupants.

The automotive context introduces additional complexity because the vehicle environment is semi private and regularly includes children. A family vehicle's occupant monitoring system processes children's biometric data on every trip. The manufacturer cannot obtain verifiable parental consent before the camera activates, because activation is tied to vehicle operation, not to a consent workflow.

I. Connected Toys and Child-Directed Devices with Biometric Features

Connected toys and educational devices that incorporate voice recognition, face detection, or other biometric capabilities present a particularly acute version of the problem because they are explicitly directed at children. A smart toy that recognizes a child by face or voice is, by definition, collecting that child's biometric data. While COPPA compliance for child-directed products has always required parental consent, the expansion of personal information to include biometric identifiers means that any face or voice processing by such devices now triggers the consent requirement, including for incidental processing of other children who may be playing alongside the device's registered user.

J. Airport, Transit, and Public Venue Biometric Systems

Private companies operate biometric identification systems at airports (CLEAR), stadiums (facial recognition entry), transit hubs, and other public venues. These systems capture biometric data from individuals seeking expedited entry or identification, but the camera infrastructure necessarily captures facial data from everyone in the vicinity, including children in queues, passing through terminals, or attending events.

The structural impossibility here is compounded by the high throughput, public nature of these environments. A CLEAR kiosk at an airport cannot pre-screen its camera's field of view for children before capturing the facial geometry of the adult using the kiosk, because the camera's capture area includes the surrounding space where children may be standing, walking, or waiting.

The risks of deploying biometric surveillance infrastructure in environments where children are present were concretely demonstrated in December 2025, when security researchers discovered that Flock Safety had left at least 60 of its AI powered Condor PTZ cameras exposed to the open internet with no authentication, no encryption, and no access controls (Koebler, 2025). These cameras, deployed across the United States in parking lots, bike paths, intersections, and playgrounds, were capable of automatically panning, tilting, and zooming to track individuals using artificial intelligence. Researchers observed the cameras streaming live footage of unattended children on a playground swing set, footage that anyone with an internet connection could watch, download, or archive. The exposure included 30 days of stored video and full administrative access to camera controls. This is the ambient biometric surveillance problem made literal: a company deployed AI powered tracking cameras into public spaces where children are guaranteed to be present, and the children's biometric data was not merely collected without parental consent but broadcast to the open internet without any safeguards whatsoever.

V. SUMMARY OF AFFECTED PRODUCT CATEGORIES

Table 1 summarizes the ten product categories, representative products, the specific biometric data implicated, and the status of COPPA specific analysis in existing literature.

Table 1: *

Table 1. Ten product categories affected by the ambient biometric COPPA impossibility. *Prior COPPA Analysis* refers to published legal scholarship or regulatory guidance addressing the structural impossibility in that product category specifically. In no case has the cross product pattern been identified.

Category	Products	Biometric Data	Status	Prior COPPA
Smart glasses / AR wearables	Meta Ray-Ban (Name Tag), Samsung Galaxy Glasses, Google, Apple	Facial geometry, faceprints	Shipping / 2026	None identified
AI pins, clips, pendants	Plaud NotePin S, Humane AI Pin, SwitchBot MindClip, Project LUCI	Voiceprints, ambient voice; some facial	Shipping	None identified
Smart home cameras / displays	Amazon Echo Show (Visual ID), Google Nest, third-party NVRs	Facial templates for recognition	Shipping	Alexa (retention only)
Cashierless retail	Amazon Just Walk Out, biometric payment terminals	Facial geometry, hand geometry, gait	Deployed; BIPA litigation	BIPA only; no COPPA
Voice assistants	Amazon Alexa, Google Assistant, Apple Siri / HomePod	Voiceprints from ambient listening	Deployed	Alexa (retention / reuse)
MR / AR headsets	Meta Quest 3/4, Apple Vision Pro	Facial images via passthrough; person detection	Shipping	None identified
Social / companion robots	CES 2026 companion robots, home robots	Facial recognition for personalization	Shipping / announced	None identified
Vehicle occupant monitoring	Various OEM driver / occupant monitoring systems	Facial geometry for driver ID	In new vehicles	None identified
Connected toys	Voice-enabled toys, face-recognizing devices	Voiceprints, facial data	Shipping	General COPPA (not biometric)
Public venue biometrics	CLEAR, stadium entry, transit kiosks	Facial geometry for identification	Deployed	None identified

VI. THE LITERATURE GAP

A comprehensive review of legal scholarship, law firm client alerts, FTC guidance, and academic research reveals substantial attention to individual components of this problem but no published analysis that connects them into the cross product structural impossibility described in this paper.

A. Law Firm COPPA Analyses

Detailed 2025 client alerts on the amended COPPA Rule from firms including Davis Wright Tremaine (Libin & Dharia, 2025), Mayer Brown (Shen et al., 2025), Finnegan (Dupree & Saeedi, 2025), and others emphasize the expansion of

biometric identifiers, the narrowing from the proposed derived data language, and the codification of facial-recognition-based ID verification for parents. They note that mixed-audience operators can collect limited data for age verification prior to applying full COPPA protections, but implicitly assume a direct, user initiated digital interaction. None address continuous sensing of bystanders in physical space. None identify the structural impossibility of age determination requiring the biometric collection that COPPA regulates.

B. FTC Enforcement and Guidance

The FTC’s 2023 biometric policy statement warns that biometric systems can be used to infer age, gender, and other traits, and stresses potential harms from misuse and bias. The Alexa COPPA enforcement action penalizes retention and secondary use of children’s voice recordings. However, neither document analyzes systems that must process biometrics from unknown passersby and branch logic based on inferred age. The enforcement model still assumes a user service relationship, not an ambient sensing relationship.

C. Wearable AI Scholarship

A 2024 law review article in the Boston University Law Review proposes mandatory privacy frictions for wearable AI devices as a form of bystander notice and de facto consent (Takhshid, 2024). A separate practitioner analysis of AI spy wearables warns that child privacy regimes make always on devices a recipe for regulatory scrutiny and points to stricter consent standards for children. Both identify real problems but frame them in terms of notice and consent mechanics, not in terms of an unsatisfiable COPPA condition that cannot be implemented even in principle.

D. MR/AR Privacy Research

Work on mixed reality bystander privacy, including proposals for bystander facing privacy enhancing technologies and catalogues of data types captured from non users by AR devices (Corbett et al., 2024; Perez et al., 2018), clearly recognizes that these devices photograph and analyze people who have no relationship to the device owner. Yet these papers discuss privacy under general data protection principles and contextual integrity frameworks, not under COPPA’s biometric definition. They do not explore the age estimation requires biometrics paradox.

E. The Gap

The existing literature thus exhibits a consistent pattern. Individual researchers and practitioners have identified that: (a) ambient biometric sensing devices capture data from bystanders; (b) children require heightened privacy protections; (c) the amended COPPA Rule now covers biometric identifiers; and (d) age estimation from biometric features is unreliable and raises its own regulatory questions. But no published source connects these four observations into the structural conclusion that ambient biometric sensing as a product class faces a COPPA compliance impossibility that cannot be engineered around.

This gap exists because the relevant expertise is siloed. COPPA compliance lawyers advise on web and app flows, not hardware. AR privacy researchers focus on data protection frameworks, not U.S. children’s privacy statutes. Wearable AI commentators flag regulatory risk without performing the formal compliance analysis. Compliance strategies have typically been articulated on a product by product basis, not across the product class. The structural impossibility lives at the intersection of these silos, visible only from a vantage point that takes in the full landscape.

VII. IMPLICATIONS

A. The April 22, 2026, Cliff

The compliance deadline for the amended COPPA Rule is April 22, 2026, approximately two months from the date of this paper. Every product identified in Section IV that collects biometric data from bystanders in environments where children may be present will, on that date, face a regulatory obligation it cannot satisfy. Companies that have not grappled with this impossibility may find themselves in violation on day one.

B. Market Impact

The smart glasses market alone is projected to grow from approximately \$2.5 billion in 2025 to over \$14 billion by 2033, at a compound annual growth rate of 24.2% (Grand View Research, 2026). Global smart glasses shipments grew 110% year over year in the first half of 2025, with the AI glasses segment specifically growing by over 250% year over year (Counterpoint Research, 2025). Meta has sold over 7 million pairs of Ray-Ban smart glasses. The broader ambient computing ecosystem, encompassing smart home, retail, automotive, and entertainment applications, represents hundreds of billions of dollars in current and planned investment. All of this investment rests on the assumption that ambient biometric sensing is legally viable. This paper challenges that assumption.

C. Strategic Timing by Manufacturers

Reporting on Meta's Name Tag feature reveals that the company's internal strategy document from May 2025 proposed launching facial recognition features during what it called a dynamic political environment, meaning a period when privacy advocates would be consumed by broader political battles and less able to mount effective opposition (Hill, Huang, & Isaac, 2026). This suggests that at least some manufacturers are aware of the legal vulnerability and are pursuing a strategy of timing, distraction, and fait accompli rather than compliance.

D. Regulatory Response Options

The FTC could respond to the structural impossibility in several ways. It could issue guidance clarifying that ambient biometric sensing in mixed age environments triggers COPPA obligations that effectively prohibit the practice without a viable consent mechanism. Alternatively, it could create a limited exception for incidental capture with immediate deletion and no retention, though this would require rulemaking and would not resolve the fundamental problem that collection occurs before age can be determined. A third possibility is enforcement inaction, allowing the impossibility to persist as a theoretical violation while declining to bring actions, but this approach would undermine the regulatory framework the FTC just spent two years strengthening.

Manufacturers may also raise First Amendment challenges, arguing that requiring consent before a wearable device processes images in public spaces constitutes an unconstitutional prior restraint on the wearer's right to record. However, COPPA regulates commercial collection of children's personal information by operators of online services, not individual photography by private citizens. The First Amendment distinction between commercial and individual speech is well established, and commercial data collection receives substantially lower constitutional protection than individual expression. The device manufacturer, not the individual wearer, is the operator subject to COPPA, and its commercial collection of biometric data through a product it designed, marketed, and deployed is regulable commercial conduct.

The constitutional argument also fails on a more fundamental level. There is a categorical difference between a human being looking at a crowd and a commercial server indexing that crowd. When a person glances across a park,

no biometric template is generated, no facial geometry is extracted, no data is transmitted to a corporate database, and no algorithmic classification occurs. The human gaze is ephemeral, unrecorded, and incapable of being queried, sold, or aggregated. When a smart glasses wearer's device processes the same scene, a commercial system extracts facial geometry from every visible person, generates biometric templates, transmits data to cloud infrastructure, and potentially retains or cross references that data against databases of millions of faces. The device does not augment human sight; it replaces a fleeting human perception with a permanent commercial record. COPPA regulates the latter, not the former, and the First Amendment does not convert commercial biometric surveillance into protected observation merely because the camera sits on a human face rather than on a building.

A related defense manufacturers may raise is the hardware-software split: the argument that the device manufacturer merely provides the hardware platform while the AI application performing biometric processing is a separate operator. Meta, for example, might argue that its Ray-Ban smart glasses are inert camera hardware and that the facial recognition feature is a software service provided by a distinct division or partner, thereby fragmenting the compliance obligation. This argument fails for several reasons. First, COPPA's definition of operator includes any person who operates a website or online service, and the FTC has consistently interpreted operational control broadly. A manufacturer that designs the camera array, integrates the AI processing pipeline, controls the cloud infrastructure, and markets the combined product as a unified experience cannot credibly claim it merely provided the lens. Second, the FTC has already rejected analogous corporate structuring defenses. In the Epic Games enforcement, Epic could not escape liability by arguing that Fortnite's social features were technically provided by separate services; the FTC assessed the integrated user experience. Third, even if the hardware software split were accepted, it would not resolve the structural impossibility; it would merely redistribute it. The software operator would still face the same circular dependency: needing to collect biometric data to determine whether the subject is a child before having consent to collect that data. Fragmenting the corporate entity does not fragment the logical paradox.

Individual FTC commissioners have informally signaled interest in permitting age verification processes without requiring prior parental consent, which would effectively carve out an exception for the ephemeral biometric processing this paper identifies as the structural impossibility. However, any such carve out would require formal rulemaking under the Administrative Procedure Act. The FTC cannot amend a final rule through informal guidance, enforcement discretion, or commissioner speeches. Until the Rule is formally amended through notice and comment rulemaking, the structural impossibility stands as a matter of positive law. Moreover, the fact that commissioners are signaling interest in such a carve out constitutes an implicit regulatory admission that the structural impossibility exists; there would be no need to create an exception for age verification if age verification were already permissible under the current Rule.

It bears noting that the judicial landscape for agency rulemaking has shifted significantly. The Supreme Court's 2024 decision in *Loper Bright Enterprises v. Raimondo* overturned *Chevron* deference (Loper Bright, 2024), meaning courts will no longer defer to the FTC's interpretation of ambiguous statutory terms like collection. A manufacturer subject to enforcement could argue before a court that ephemeral processing in RAM does not constitute collection within the ordinary meaning of the statute. Courts interpreting COPPA's text independently, rather than deferring to FTC rulemaking, might reach different conclusions about the scope of the consent requirement as applied to ambient sensing. This judicial uncertainty does not resolve the structural impossibility under the Rule as written, but it introduces an additional dimension of legal risk for both manufacturers and the Commission.

Similarly, COPPA's Safe Harbor provision, which allows FTC-approved industry self-regulatory programs to provide alternative compliance frameworks, does not offer an escape. Safe Harbor programs must provide protections at least as protective as those required by the Rule itself (16 C.F.R. § 312.11). A Safe Harbor program that approved biometric collection from children before obtaining parental consent would be less protective than the Rule, not equivalently protective, and would be subject to FTC revocation. The Safe Harbor mechanism cannot authorize what

the Rule prohibits.

E. Broader Implications for Ambient Computing

The structural impossibility identified here extends beyond COPPA. The European Union's General Data Protection Regulation imposes heightened protections for children's data. The UK's Age Appropriate Design Code requires age assurance before processing children's data. Australia, Brazil, and other jurisdictions are adopting similar frameworks. Each faces a version of the same paradox when applied to ambient biometric sensing: the system cannot determine whether heightened protections apply without first performing the processing that triggers those protections.

The ambient computing vision, in which AI powered devices seamlessly recognize, understand, and assist people in physical environments, is on a collision course with children's privacy law worldwide. This is not a bug in the law. It is a signal that the technology imposes costs and risks that the legal system has determined require affirmative consent. The fact that affirmative consent is structurally unobtainable for ambient sensing does not invalidate the law; it invalidates the product category.

Moreover, the legal landscape is already moving beyond COPPA's actual knowledge standard. Florida's statute treats willful disregard of a user's age as equivalent to actual knowledge. Connecticut combines actual and constructive knowledge standards, lowering the threshold for operator liability. The proposed COPPA 2.0 legislation would impose a constructive knowledge standard on large platforms, meaning operators would be liable for collecting children's data if they reasonably should have known children were present, not merely if they actually knew. These developments signal a trajectory in which the actual knowledge defense, already strained by FTC enforcement practice, is being legislatively eliminated. Manufacturers of ambient biometric devices who rely on the actual knowledge standard as their primary legal shield are building on ground that is actively eroding beneath them.

F. The Actual Knowledge Paradox

The structural impossibility creates an additional legal trap for manufacturers of general audience devices. Under COPPA, operators of general audience products (as distinct from child-directed products) are subject to the Rule only when they have actual knowledge that they are collecting personal information from a child under 13. Manufacturers of smart glasses, AI wearable recorders, and similar devices will predictably argue that their products are general audience, intended for adults, and therefore outside COPPA's scope absent actual knowledge of child users.

But the biometric scan itself defeats this defense. The moment a device's age estimation algorithm processes a bystander's face and determines that the subject appears to be, for example, eleven years old, the operator possesses actual knowledge that the system is processing a child's biometric data. The scan that was intended to enable compliance is the event that triggers the legal obligation retroactively. The operator cannot claim ignorance of the child's presence, because the operator's own system just identified the child as a child.

This creates a perverse incentive structure. A manufacturer that builds age estimation into its device, attempting to comply with COPPA by identifying children before processing their data further, simultaneously generates the actual knowledge that subjects it to COPPA liability for the collection it has already performed. A manufacturer that declines to build age estimation, remaining deliberately ignorant of whether bystanders are children, may have a stronger defense against COPPA enforcement under the actual knowledge standard, but at the cost of processing children's biometric data with no safeguards whatsoever. The regulatory structure thus creates a perverse incentive: the less a manufacturer knows about its users, the stronger its legal position, even as children receive less protection. This is the actual knowledge paradox, and it compounds the structural impossibility by making even the most responsible engineering approach legally self defeating for general audience ambient sensing devices.

The FTC's enforcement record confirms that engineered ignorance of children's presence is not a viable defense. In its \$275 million settlement with Epic Games, the largest COPPA penalty ever obtained, the FTC found that Epic had actual knowledge children were playing Fortnite through internal surveys, toy licensing deals, and player support communications, even as Epic's privacy policy disclaimed being child-directed (FTC & DOJ, 2022). In the \$170 million settlement with Google and YouTube, the FTC established that YouTube marketed itself to advertisers as a top destination for children aged 6 to 11 while simultaneously telling one advertising company that it did not have users younger than 13 on its platform (FTC & NY AG, 2019). In both cases, the companies possessed evidence that children used their services and chose to structure their operations to avoid triggering COPPA obligations. The FTC treated this not as absence of actual knowledge but as its willful avoidance. For manufacturers of ambient biometric devices, the parallel is direct: deploying facial recognition or voice processing into public and domestic environments where children are statistically guaranteed to be present, while declining to implement age detection, is the same strategic ignorance the FTC has already penalized at a combined \$445 million in these two cases alone.

Manufacturers may attempt to distinguish their products from Epic and YouTube by arguing they lack equivalent internal evidence that children use their devices. They market to adults, sell through adult retail channels, and do not license children's intellectual property. But for ambient biometric devices, the deployment environment is itself the evidence. A device designed to scan faces in public parks, grocery stores, living rooms, and sidewalks will encounter children. This is not a matter of internal surveys or marketing decisions; it is a matter of demographic reality. The U.S. Census Bureau reports approximately 48 million children under 13 in the United States. They exist in every public and domestic environment where ambient sensing devices operate. A manufacturer deploying facial recognition into these environments while claiming no knowledge that children are present is asserting ignorance of a census fact. The FTC's totality of circumstances analysis, as applied in Epic, considers the actual deployment context, not merely the manufacturer's marketing materials or stated target demographic.

VIII. CONCLUSION

The amended COPPA Rule's inclusion of biometric identifiers in the definition of children's personal information creates a structural compliance impossibility for ambient biometric sensing devices. This impossibility is not product specific; it is category wide. It affects smart glasses, AI wearable recorders, smart home cameras, cashierless retail systems, voice assistants, mixed reality headsets, social robots, vehicle monitoring systems, connected toys, and public venue biometric infrastructure. It cannot be resolved through engineering, edge processing, immediate deletion, opt-out mechanisms, or geofencing.

No prior published analysis has identified this impossibility as a cross product structural problem. Existing scholarship treats bystander biometric collection as a product specific compliance challenge, a practical consent difficulty, or a general privacy concern, not as a logical paradox inherent to the product class. This paper fills that gap.

With the April 22, 2026, compliance deadline approaching, the stakes are immediate. Companies investing billions in ambient biometric products face a choice: acknowledge the impossibility and redesign their products, lobby for regulatory exemptions that would weaken children's privacy protections, or proceed in knowing violation of the law. The first option is the only one consistent with the regulatory framework. The second reveals priorities. The third, as internal Meta documents suggest some manufacturers may be contemplating, relies on the assumption that enforcement will not be immediate.

The device must break the law to find out whether it is breaking the law. That is not a compliance challenge. It is a compliance impossibility. And it applies not to one product, but to an entire technological era that is about to discover it was never legal in the first place.

ACKNOWLEDGMENTS

The author discloses the use of speech-to-text software (Wispr Flow) and Anthropic’s Claude as assistive technology for a diagnosed neurodevelopmental condition.

Correspondence concerning this article should be addressed to Travis Gilly, Real Safety AI Foundation, Illinois, United States. Email: t.gilly@ai-literacy-labs.org.

REFERENCES

- 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-secret-weapon/>
- Corbett, M., David-John, B., Shang, J., Hu, Y. C., & Ji, B. (2024). Securing bystander privacy in mixed reality while protecting the user experience. *IEEE Security & Privacy*, 22(1), 33–42. <https://doi.org/10.1109/MSEC.2023.3331649>
- 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>
- 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>
- 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>
- European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Arts. 4(14), 8, 9.
- 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>
- 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>
- 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-protection.html>
- 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-look-at-your-kids-meta-s-name-tag-and-amended-coppa>
- 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-sensing-mode-with-facial-recognition>
- 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-that-s-always-listening>
- 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-amended>
- International Data Corporation (IDC). (2026, March 25). *XR market expands 44.4% in 2025 as smart glasses take center stage*. <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-8703>
- 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-significant-amendments-to-coppa>
- 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-recognition>
- 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-privacy-laws-across-the-u-s/>
- Harary, M. (2024, November 27). Amazon’s “Just Walk Out” tech faces BIPA lawsuit. Darrow AI. <https://www.darrow.ai/resources/amazon-bipa-lawsuit>
- 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/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-childrens-information/>

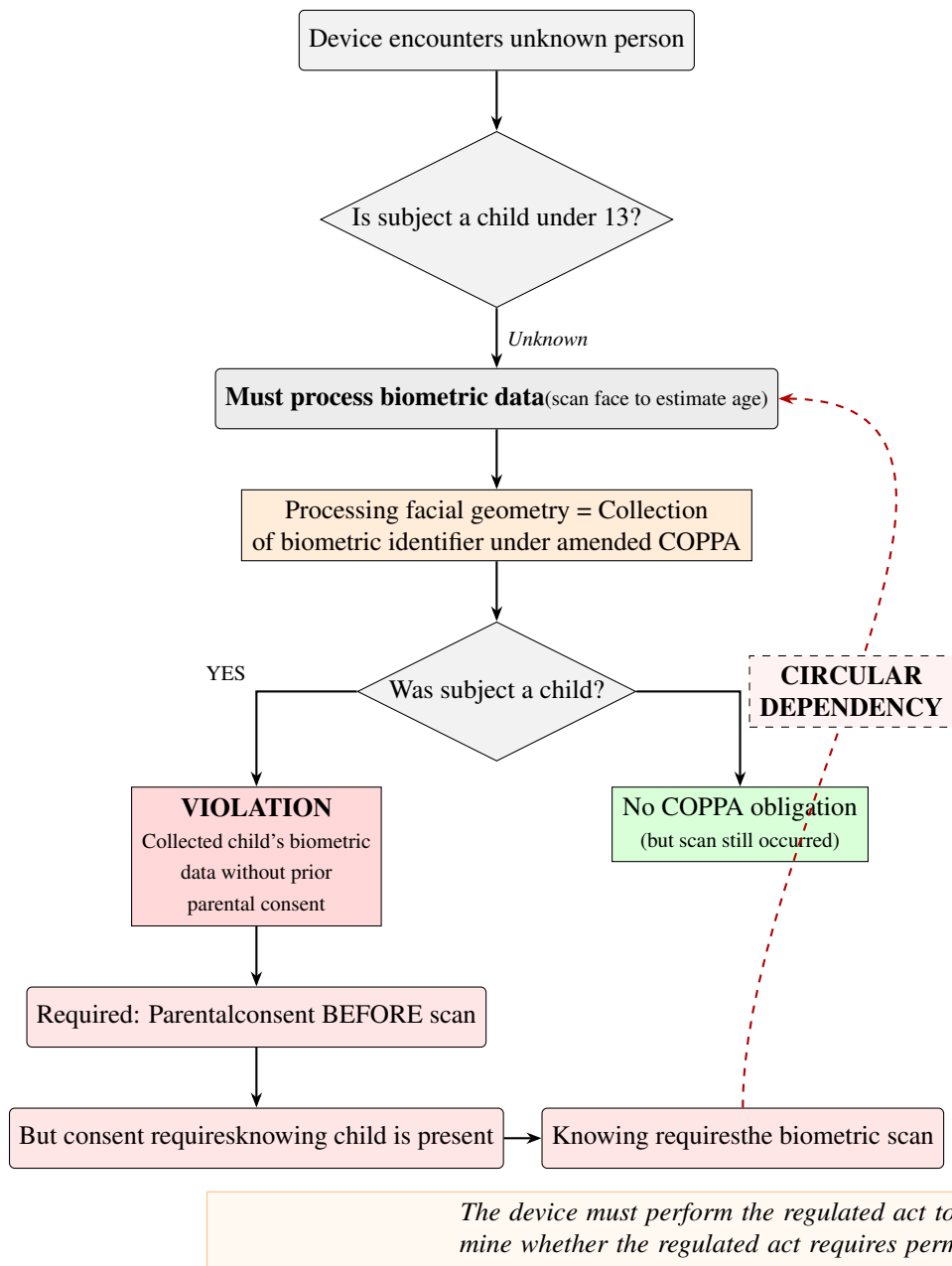


Figure 1: *

Figure 1. The COPPA Compliance Impossibility: Circular Dependency. The device must perform the regulated act (biometric collection) to determine whether the regulated act requires permission (parental consent). This creates an unresolvable circular dependency.