Nothing but the Bit: Wi-Fi Sensing for Predicate-Only Age Verification

Gioliano de Oliveira Braga
Aeronautics Institute of Technology
Brazil
gioliano.braga.102147@ga.ita.br

Rafael Pimenta M Paixão
Aeronautics Institute of Technology
Brazil
rafael.paixao.9134@ga.ita.br

Pedro H dos Santos Rocha
University of Sao Paulo
Brazil
psrocha@usp.br

Carlos H G Ferreira
Federal University of Ouro Preto
Brazil
chgferreira@ufop.edu.br

Guevara Noubir
Northeastern University
United States
g.noubir@northeastern.edu

Lourenço A Pereira Júnior
Aeronautics Institute of Technology
Brazil
lourenco.junior@gp.ita.br

ABSTRACT

Age verification is becoming a condition of access to social media, online games, and e-commerce, as COPPA, GDPR-K, and newer child-safety laws regulate how services treat minors, from the collection of their data to restricted content and contact with adults. However, current methods run out-of-band: the user leaves the application workflow to film their face or photograph an identity document. The service receives more than it needs: the decision uses one bit, whether the user meets the legal age threshold. Verifiable credentials disclose less, but a minor can pass with an adult's credential or unlocked device. We propose, to the best of our knowledge, the first architecture for age verification from Wi-Fi sensing. The user holds a hand near the device's Wi-Fi antenna, and the system derives the age predicate from the resulting Channel State Information (CSI). It returns a signed, attested verdict through a predicate-only interface; raw CSI and intermediate representations stay inside a protected trust boundary. Sensing binds the verdict to the body present at each gated action, within the application workflow, and placing the check in the operating system (OS) gives all applications one system call behind that boundary. We evaluate the sensing step on COTS Wi-Fi 6 chipsets, which expose CSI through vendor interfaces, with 113 participants (95 children and 18 adults) in one controlled environment. Under leave-one-subject-out evaluation, an SVM separates the two cohorts with a macro F1-score of 85.38% and a child recall of 91.58%, which shows that near-field CSI carries an age-class signal for cohorts far apart in age. These results open three research questions: accuracy at legal thresholds, the physical source of the separation, and generalization across sessions, environments, and devices. Until the first is answered, the verdict includes an uncertain value that routes low-confidence cases to conventional checks. We outline a networking research agenda around these questions, including whether IEEE 802.11bf sensing reports preserve the signal.

CCS CONCEPTS

• **Networks → Wireless local area networks**; • **Security and privacy → Social aspects of security and privacy**.

KEYWORDS

Wi-Fi sensing, channel state information, age verification, privacy

ACM Reference Format:
Gioliano de Oliveira Braga, Rafael Pimenta M Paixão, Pedro H dos Santos Rocha, Carlos H G Ferreira, Guevara Noubir, and Lourenço A Pereira Júnior. 2026. Nothing but the Bit: Wi-Fi Sensing for Predicate-Only Age Verification. In *The 25th ACM Workshop on Hot Topics in Networks (HotNets '26), November 16–17, 2026, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3847290.3859963

1 INTRODUCTION

Age verification is becoming a condition of access to social media, online games, and e-commerce. For example, the game platform Roblox has required a facial age check for chat from users of all ages since January 2026, and it uses the result to limit contact between adults and children [48]. Services that can harm minors, such as gambling and adult content,



This work is licensed under a Creative Commons Attribution 4.0 International License.
HotNets '26, November 16–17, 2026, Salt Lake City, UT, USA
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-3029-0/2026/11
https://doi.org/10.1145/3847290.3859963

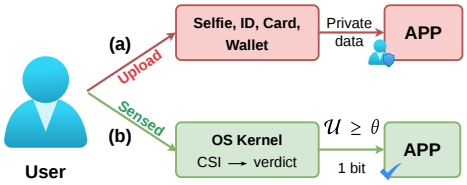


Figure 1: Disclosure in age verification: (a) current methods send the evidence to the application; (b) the proposed design sends the application the verdict alone.

go further and admit adults only (e.g., betting platforms in Brazil [42]). In both cases, one decision about the person at the device, whether that person meets an age threshold, protects a minor from contact with an adult or from a harmful service. COPPA in the United States [21] and Article 8 of the GDPR (GDPR-K) [19] regulate the collection of children's data, and newer child-safety rules govern restricted content and contact with adults [16, 17, 45]. However, current methods run out-of-band (Figure 1a). The user leaves the application workflow to film their face or photograph an identity document [13, 38, 50], typically once at enrollment. The service receives more than it needs: a face, a document, or financial data [3]. The decision itself should use one bit, whether the user meets the legal age threshold.

Verifiable credentials and platform age signals disclose less. A zero-knowledge age credential can release one bit [18], and Apple and Google return an age range to applications [2, 25]. However, both establish the age fact once, at credential issuance or account setup, and bind the check to the holder, so a minor can pass with an adult's credential or unlocked device. Age verification at the gated action requires evidence from the person who uses the device.

We argue that an age-verification primitive should be (1) *contactless* inside the application workflow, (2) *privacy-preserving*, with a yes/no answer as its only output, (3) *re-evaluable* at each gated action, (4) *physically bound* to the person at the device, and (5) *tamper-evident*, through an attested, signed verdict, because the user controls the device. When assessed against these five properties, each deployed method we survey meets a subset of them.

Wi-Fi Channel State Information (CSI) carries a measurable, person-specific imprint of the human body [9, 39, 57]. For about a decade, CSI-based systems have estimated body composition [56] and identified people [6, 14, 52, 59, 64]. Our design inverts the identification objective and treats the spectral structure that identifies a person as the quantity to suppress. Our insight is that a hand held a few centimeters from a Wi-Fi antenna dominates the static channel response, so a short capture reflects the structure of the body present. This raises a question for the networking community: *can Wi-Fi sensing support an age-verification primitive with these five properties and keep the biometric signal inside the device?*

We propose, to the best of our knowledge, the first architecture for age verification from Wi-Fi sensing (Figure 1b). The user holds a hand near the device's Wi-Fi antenna, and the system derives the age predicate from the resulting CSI. It returns a signed, attested verdict through a predicate-only interface, and raw CSI and intermediate representations stay inside a protected trust boundary. Placing the check in the operating system gives all applications one system call behind that boundary, where the system enforces attestation and limits queries to a fixed set of thresholds, which blocks recovery of the exact age through repeated queries. Applications invoke the check at each gated action, so the verdict binds to the body present at that moment.

We evaluate the sensing step on commercial off-the-shelf (COTS) Wi-Fi 6 chipsets, which expose CSI through vendor interfaces, with 113 participants (95 elementary school children and 18 adults) in one controlled environment. Under leave-one-subject-out evaluation, an SVM separates the children from the adults with a macro F1-score of 85.38% and a child recall of 91.58%, which shows that near-field CSI carries an age-class signal for cohorts far apart in age. These results open three research questions: accuracy at legal thresholds, the physical source of the separation, and generalization across sessions, environments, and devices. Until the first is answered, the verdict includes an *uncertain* value that routes low-confidence cases, such as a 12-year-old near a threshold of 13, to a conventional check.

This paper makes three contributions. First, it proposes an architecture in which the operating system is a declassification point for a sensing-derived legal predicate. Prior OS sensing services share context data with applications [12, 22]. Second, it instantiates the architecture as a CSI-backed age check and identifies its trust, policy, and protocol boundaries. Third, it reports preliminary subject-grouped evidence for two cohorts far apart in age and derives a networking research agenda for the three questions, including whether IEEE 802.11bf sensing reports preserve the signal.

2 BACKGROUND

We review age-verification methods, motivate the use of Wi-Fi CSI, and discuss related work on sensing and OS interfaces.

2.1 Age Verification Methods

We assess deployed methods against the five properties of Section 1: *contactless*, *privacy-preserving*, *re-evaluable*, *physically bound*, and *tamper-evident*.

Self-declaration through a birthdate field or checkbox has low invasiveness and low friction. Its claim is detached from

the present user, so circumvention is straightforward, and the check happens once, at enrollment [21]. *Facial age estimation* [54] is contactless and convenient and captures a biometric. Reported mean absolute errors of 5 to 6 years complicate decisions near an adult/minor boundary [44], and photos or AI-altered selfies enable presentation attacks [53]. *Identity-document upload* [31] exposes government-issued data and creates a standing breach risk [32]. Borrowed or stolen documents weaken the binding to the present user, and verification generally occurs once, at enrollment. *Credit-card checks* [21] expose financial data unrelated to age and fail when a minor can use a parent's card [41]. *Parental consent* through "email-plus" adds friction and permits self-approval by a child with a second address, a weakness identified by the FTC [20].

Verifiable digital credentials [1, 18, 26] provide low-disclosure, cryptographically protected, and repeatable proofs. Their open problem is presence binding: a credential attests to its holder, device-bound presentation may require another biometric prompt [3], and an adult may authenticate before handing over the device. FIDO-AC combines FIDO2 with a zero-knowledge attribute proof and requires a liveness check that keeps the attribute bound to its holder [61]. A sensing-based presence signal could fill this role. *Platform age signals* return an age range from a declaration or credential tied to the account at setup [2, 25], and California AB 1043 requires operating system providers to supply such a signal to developers from 2027 [7]. *On-device biometrics* such as fingerprint readers bind to the person present and attest identity. Reporting age from a fingerprint requires a backing identity record, which reintroduces the disclosure that a predicate interface removes.

Position of the proposal. A sensed predicate offers presence binding, contactless operation, and re-evaluation at each gated action. Its accuracy at legal thresholds remains to be demonstrated. It requires cooperative hand placement, depends on attestation and on chipset access to CSI, and faces presentation attacks like every biometric. Verifiable credentials are more mature and exact. We therefore position the sensed predicate as a complement to established checks.

2.2 Why Wi-Fi CSI?

Wi-Fi is deployed across personal devices, homes, workplaces, and vehicles. COTS chipsets expose CSI through vendor interfaces today, and *IEEE 802.11bf* makes WLAN sensing part of the standard [49], which opens a path to uniform access across vendors.

We build on CSI. The CSI matrix H captures the CFR that environmental absorption, refraction, and multipath reflection produce [11], and it decomposes into static and dynamic components: $H(k,t) = H_s(k) + H_d(k,t)$.

Most Wi-Fi sensing reads motion from the *dynamic* component: gait [64], respiration and heartbeat [36], gestures [37], and daily activity [52]. Our approach to age verification uses the *static* component, which carries the response of a body at rest. The user holds a hand still in the sensing zone.

The static channel mixes the response of the body with reflections from walls, furniture, and fixed clutter, where the body is one scatterer among many. Proximity increases its relative contribution. The near field is the region within a wavelength-scale distance of the antenna ($\lambda \approx 6$ cm at 5 GHz), where the far-field path-loss model stops applying [23]. Reflected strength falls sharply with path length [23, 47], so a hand a few centimeters from the antenna can dominate the measured static response. We call this regime *static near-field domination*. Prior near-field sensing uses motion to isolate a subject [29, 30].

Wi-Fi CSI offers three advantages: deployment on Wi-Fi hardware already present in many devices; contactless, motion-free operation that needs only cooperative hand placement in the sensing zone; and measurement of the body present, which raises the cost of remote reuse relative to documents, passwords, and stored images. The second supports the *contactless* property, and the third supports the *physically bound* and *re-evaluable* properties. Privacy and tamper evidence depend on the architecture that handles the signal and attests its verdict (Sections 3 and 3.1). Generalization across sessions, environments, and devices [6, 11, 57] remains open (Section 6).

2.3 Related Work

Operating systems and middleware have offered sensing as a service for more than a decade. CondOS moves the conversion of raw sensor data into context units into the OS and offers applications a higher-level interface [12]. Smartphone frameworks add privacy-aware sensor management and policy [60], and context-awareness middleware gives applications shared sensing abstractions over specific hardware [4, 22]. Recognizers [33] and Darkly [34] restrict perceptual applications to recognized objects or transformed camera input. These systems release context or derived features to applications. Our abstraction declassifies one legal predicate and releases that predicate alone. The closest OS precedent for the interface is the biometric API, which returns an authentication result and keeps the template in a TEE [5, 63]. In Wi-Fi sensing, DeepCPD separates children from adults in a car cabin from motion and breathing features of CSI [35]. The contribution is the combination: a sensed attribute, bound to the person present and exposed as a signed, predicate-only OS primitive.

3 A CSI AGE PREDICATE AS AN OS PRIMITIVE

We sketch a preliminary design from the physical channel to the application layer. For a user $\mathcal{U}$ and jurisdictional threshold θ, the design evaluates the predicate $P_\theta(\mathcal{U}) = [\text{age}(\mathcal{U}) \geq \theta]$. The system returns *adult*, *minor*, or *uncertain*, and returns *adult* only when the confidence score meets a minimum threshold ε_{th}. A deployment sets ε_{th} on a held-out, subject-grouped calibration set to bound the child-to-adult error, as deployed biometrics fix an operating threshold for a target false-accept rate [27, 58]. The threshold requires only that the score rank subjects by confidence.

Regulations define age thresholds: COPPA uses 13 years [21]; GDPR Article 8 uses 16, with national floors down to 13 [19]; and other jurisdictions set thresholds for social-media access or restricted content [16, 45]. The application therefore needs a binary answer for a jurisdiction-selected θ, commonly 13, 16, or 18. A finer age estimate adds disclosure beyond what the decision uses.

Borderline ages. Our evidence covers cohorts far apart in age, and the separation of adjacent ages, such as 12 and 13, is untested. Deployed age-estimation services handle this case with a guard band: they add a buffer age and send users estimated near the legal age to another check [62]. We adopt the same pattern. Errors are asymmetric, so the policy favors the *minor* verdict and accepts extra fallbacks in exchange for fewer minors admitted. *Uncertain* and *minor* verdicts route to a conventional method, such as a credential, a zero-knowledge proof, or a document. We propose to report the *deflection rate*, the share of users that the predicate resolves at a target child-to-adult error. Its estimation requires subjects near the thresholds (Section 6).

Figure 2 traces the information flow across five stages.

Stage 1: Physical Environment. A person $\mathcal{U}$ places a hand within centimeters of a Wi-Fi receiver, inside its near-field zone (Section 2.2). The access point emits Null Data Packets (NDPs) [49]. The body is a passive scatterer that perturbs the received amplitude and phase, so the perturbed channel $\mathcal{S}'$ contains body-derived information [9].

Stage 2: PHY Layer (IEEE 802.11). The PHY estimates the channel frequency response per antenna pair, and the output is the raw CSI C_{raw}.

Stage 3: MAC Layer (IEEE 802.11bf). The MAC runs the standardized *WLAN sensing procedure*: it negotiates parameters, exchanges NDPA/NDP sounding frames, and packages the measurements into a sensing report frame $\mathcal{F}_{\text{mac}}$, which quantizes the in-phase and quadrature components to 8 or 10 bits and may group subcarriers [49]. Identity-bearing CSI first becomes transportable here, so the MAC layer is the earliest point for confidentiality protection and representation shaping (Section 6).

Stage 4: OS Mediation and Protected Inference (trust boundary). This stage is our main contribution. The Wi-Fi driver extracts the sensing report $\mathcal{F}_{\text{mac}}$ and hands it to a protected component (a TEE or protected VM) behind the kernel interface. The component preprocesses the signal into $\tilde{C}$, extracts a feature vector $\mathcal{F}$, and infers $(age_class, confidence)$ against threshold θ. The kernel owns the driver and mediates the interface, and hardware attestation establishes its integrity (Section 3.1). Confidence below ε_{th} yields *uncertain*, which the system denies by default (fail-closed) and the application routes to a fallback check (*Borderline ages*). The representations $C_{\text{raw}}, \tilde{C}, \mathcal{F}$ stay inside the trust boundary, and the verdict alone crosses it, which implements the GDPR principle of data minimization [24]. The path from the driver to the protected component requires an authenticated channel, which remains open (Section 3.1).

Stage 5: Userspace (Application). The verdict reaches *userspace* through a single system call (`verify_age()`) that returns a signed token over a relying-party nonce, the threshold θ, the result, a timestamp, and the model hash. This call is the entire public surface of the primitive. CSI, the sensing procedure, and the model stay hidden, as in minimal-disclosure age statements [38, 63]. A cached "verified" state would let a shared or borrowed device pass a one-time gate, so the application re-invokes the call at each gated action [38].

Threat model and trusted computing base. Applications and remote services are untrusted. The kernel is attackable, because an attacker can recompile it or load modules. The trusted computing base is the hardware root of trust (TPM or TEE), the firmware it measures, and the model-distribution path, and each verdict carries evidence of that measured state (Section 3.1). The public interface exposes a fixed set of jurisdiction-approved predicates, requires authorization, and rate-limits queries to block threshold enumeration and repeated measurement.

Five attack classes remain open. First, the call attests the presence of a body above the threshold. Binding that body to the logged-in account requires a separate mechanism. A cooperating adult who places a hand for a minor therefore satisfies the check, and re-invocation at the gated action raises the cost from a single favor to sustained presence. Second, a physical proxy with similar geometry and dielectric response may reproduce an adult signature, and liveness requires evidence beyond a static signature. Every deployed biometric faces this presentation-attack problem (silicone fingerprints, deepfakes, masks), and platform certification reports a spoof acceptance rate for it [46]. We adopt that metric and treat the cost and reliability of such proxies as part of the security margin to be measured. Third, the privacy objective requires limited linkability among subjects in the same age class. Prior work recovers identity from related spectral

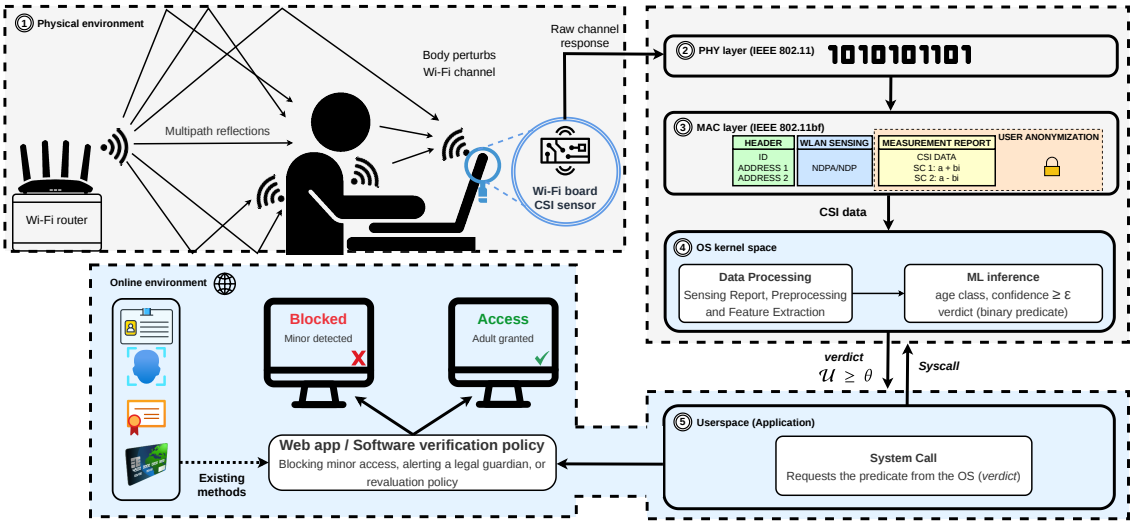


Figure 2: Information flow of the CSI-backed age check as an OS primitive.

structure [9], so a privacy claim requires a measurement of within-class re-identification. Fourth, a modified operating system could return any verdict; attestation makes the modification detectable to a relying party. Fifth, a tampered router or Wi-Fi device that injects or replays CSI could feed a forged channel, and injection has defeated CSI-based liveness detectors [28]. Candidate defenses are sensing with the device's own radio, an authenticated sounding peer, and unpredictable sounding patterns; their support in IEEE 802.11bf is an open question.

3.1 Attestation and Signed Verdicts

A verdict is as trustworthy as the platform that produced it, so we combine four mechanisms. (i) *Measured boot*: Secure Boot and a TPM measure the kernel, the sensing driver, and the model hash, and the device can prove these measurements to a relying party. (ii) *Protected inference*: inference in a TEE or protected VM places a compromised kernel outside the trusted base for the model and its inputs. (iii) *FIDO-style signed verdicts*: at registration the device creates a per-site key whose attestation binds it to the measured state, and the device signs each verdict over a fresh relying-party nonce for replay resistance, as in the signing-and-attestation use of Android fingerprint APIs [5]. Batch or anonymous attestation limits the linkability of the device across relying parties. (iv) *Zero-knowledge proofs* can hide the identity of the device inside the attestation [61]. Extending the chain below the kernel requires three steps: the sounding peer authenticates its sounding frames and attests its firmware, the NIC delivers the sensing report over an authenticated channel into the protected component, and that component alone signs the verdict. Each stage then vouches for the one before it. Attestation proves which software ran, and the spoof acceptance rate measures exposure to physical proxies, as in platform certification [46]. Attestation is the condition for a guarantee stronger than the methods of Section 2.1: it makes an altered stack detectable.

Deployment options. The signer can sit in a host TEE, as above; in the Wi-Fi chipset, which keeps CSI on the chip and signs with an attested on-chip key; or in a USB token, like a FIDO security key, that carries the radios, the model, and the key while the host relays the verdict. A remote server verifies each verdict without trusting the host OS: it checks the signature over its nonce and the attestation chain of the key to the hardware vendor, as WebAuthn does for FIDO authenticators [55]. A compromised host can drop a verdict; forging one requires the key or, for a host TEE, a breach of the authenticated channel from the NIC. Browsers can expose the call to web applications through a permission-gated API on the same model.

4 PRELIMINARY RESULTS

Developmental changes in skeletal maturation, bone mineralization, and tissue dielectric composition suggest a physical basis for an age-related near-field response, because these properties affect how the body perturbs an incident electromagnetic field. Hand-wrist radiographs estimate biological age from an age-ordered sequence of skeletal maturation [10]; hand bone mineral density rises toward an early-adulthood peak and then declines [40]; and childhood body-water composition changes with age and affects tissue permittivity and conductivity at radio frequencies [43].

4.1 Experimental Setup

We collected near-field CSI from 113 subjects (95 elementary school children and 18 teachers) in one controlled environment. The setup is bistatic: two separate COTS ESP32-C5 boards are the sensing transmitter (an access point) and the receiver, which reports CSI through the vendor interface, under IEEE 802.11ax (Wi-Fi 6) at 5 GHz with a 20 MHz channel bandwidth and 1 m between transmitter and receiver. Each participant held the right hand 2 to 5 cm from the receiver's antenna, within its near-field zone, for one ten-second capture at a 100 Hz packet rate.

The analysis uses CSI amplitude. Preprocessing isolates the quasi-static response through per-subcarrier outlier rejection, zero-phase low-pass filtering, and per-packet Z-score normalization; normalization removes AGC gain fluctuation and keeps the spectral shape across subcarriers. Each subject yields one 228-dimensional median profile. We excluded phase given its sensitivity to residual synchronization offsets.

4.2 Can CSI separate children from adults?

At an imbalance of about 5:1, plain accuracy misleads, so we report macro precision, recall (equivalently, balanced accuracy), and F1-score, plus child recall, whose complement is the safety-critical error for an age gate: a child predicted as an adult. We use two subject-grouped protocols. Leave-one-subject-out (LOSO) suits shallow models that see one profile per subject; for a window-level network it would require 113 retrainings, so we use grouped 5-fold for that network.

Table 1 reports the best architecture under each protocol. Under LOSO, the SVM reaches a macro F1-score of 85.38%; its child recall of 91.58% corresponds to an 8.42% child-to-adult error rate. Separation from a single median profile shows that the median amplitude spectrum carries cohort-discriminative information. Under grouped 5-fold, the window-level 1D-CNN reaches a macro F1-score of 82.02%, with macro precision of 78.12% and macro recall of 92.63%. It identifies every adult in this cohort and reaches a child recall of 85.26%. The two protocols preclude a direct model ranking.

Three caveats bound the claim. First, physical build varies together with age in the two cohorts, so the experiment establishes cohort separation and leaves the contributions of developmental maturity and physical build unresolved. Isolating an age-related contribution requires a cohort in which age varies independently of build (Section 6). The thresholds of 13, 16, and 18 fall where physical build overlaps across the boundary, so the region of greatest legal significance coincides with the region of weakest contrast in build. Second, the adults are 18 teachers from one school, and all captures come from one room, one device pair, and one session per subject, so we read the numbers as evidence that the signal exists for cohorts far apart in age, and the operating point remains uncalibrated. Third, the numbers hold under subject-grouped splits; a split that places windows of one subject in both training and test raises the macro F1 of the window-level model by about eight points.

Table 1: Best architecture per subject-grouped protocol, by macro F1-score.

Model	Protocol	Precision	Recall	F1-score	Child recall	Adult recall
SVM	LOSO	82.21%	90.23%	85.38%	91.58%	88.89%
1D-CNN	grouped 5-fold	78.12%	92.63%	82.02%	85.26%	100.00%

5 DISCUSSION

The architecture applies the decoupling principle [51] to age verification: the application learns whether the user meets the threshold, and the body-derived signal stays inside the trust boundary. The OS adds two guarantees to this one-bit release: attestation of the stack that computed the verdict, and query limits that block recovery of the exact age through repeated queries. The sensing report carries identity-bearing structure until it reaches the protected component, and its within-class re-identification and cross-session linkability remain to be measured (Section 6).

Our results support a triage role for the predicate under the fallback policy of Section 3: it resolves clear cases, and uncertain or minor verdicts route to a check backed by an issued birth date. The case for sensing rests on three claims, each falsifiable by one of the experiments proposed in the future directions (Section 6): the signal tracks age beyond physical build (Section 4), which a broad cohort of small adults and large adolescents tests; it persists across days, rooms, and devices; and it resists cheap, reusable proxies, such as a water-filled phantom hand. If the first claim fails, simpler cues of build, such as touch contact area, deliver the same verdict. If the third fails, sensing loses presence binding, its advantage over credentials.

The architecture extends beyond age. Only the classifier in Stage 4 is specific to age; the trust boundary, the signed verdict, and the query limits apply to any sensed predicate. Proximal or ambient sensing may support policy predicates, such as presence, occupancy, or liveness, with the minimal disclosure that anonymous credentials provide [8].

6 FUTURE DIRECTIONS

The results open three questions, and the architecture raises three more.

Accuracy at legal thresholds. The next experiment recruits subjects near 13, 16, and 18 and reports accuracy by age year under subject-grouped evaluation. It calibrates ε_{th}

to a target child-to-adult error and reports the resulting deflection rate, the share of users that the predicate resolves before the fallback of Section 3.

Physical source of the separation. Our captures measure the combined perturbation of the hand and the rest of the body, and in our cohorts physical build varies together with age (Section 4.2). A cohort of small adults and large adolescents, in which age varies independently of build, tests whether the separation persists, and captures that interleave both cohorts in the same sessions control for acquisition drift. Our evidence rests on the static component of the CFR, and most sensing work studies motion-driven dynamic signals. The contribution of each component to age inference, and their complementarity, are open.

Generalizing across sessions, environments, and devices. Each subject contributed one ten-second session, so stability across days is untested; repeated captures of the same subjects measure it. The surroundings shape CSI through multipath, scattering, attenuation, and interference, so a model may learn environmental structure together with body-derived structure. Devices add variation: subcarrier count varies with bandwidth and subcarrier spacing across Wi-Fi generations (20 to 320 MHz from Wi-Fi 4 to 7), so feature vectors from different devices may differ in dimensionality. Operation across settings therefore requires separating the body-derived signal from environmental artifacts, and architectures that ingest variable-width spectral input from any device with one trained model. Cross-domain methods (domain-invariant features, virtual sample generation, transfer and few-shot learning [6, 11]) are candidates. Drift is also a security signal: a drifting input lowers confidence and yields an *uncertain* verdict with fallback [15]. Fusion with dynamic CFR, multi-band sounding, or non-RF cues such as touch contact area may improve generalization; its effect is an open empirical question.

Limiting identity leakage and retaining the age predicate. Stage 4 keeps raw and derived representations inside the trust boundary. A further step shapes the representation at the MAC layer, where CSI first becomes transportable (Stage 3), so that it preserves the age class and limits what it reveals about identity within that class. Related spectral structure supports person re-identification [9], so the achievable trade-off is an empirical question. Evaluation should report predicate utility, within-class re-identification, and cross-session linkability. Aggregation, quantization, calibrated noise, or learned feature suppression may limit what an authorized recipient learns, and authenticated encryption protects the report from other parties in transit or storage; characterizing both and standardizing a sensing representation are candidate extensions to IEEE 802.11bf. The same discipline applies to the model-building pipeline, which calls for governed recruitment, retention limits, and on-device or federated extraction.

Presentation attacks and the sensing path. Open work includes measuring the spoof acceptance rate against physical proxies, for example gel or water-filled phantoms, and against injected CSI [28], and evaluating the defenses of Section 3 (the device's own radio, an authenticated sounding peer, unpredictable sounding) and their support in IEEE 802.11bf. Dynamic CFR (pulse, tremor) may add a liveness cue to the same capture. The goal is a measured spoof acceptance rate comparable across modalities.

Maturing alongside the standard. IEEE 802.11bf standardizes WLAN sensing, and our bistatic geometry maps onto its sensing procedure [49]. The open question is fidelity. To bound overhead, the standard quantizes measurements and reports a fraction of the subcarriers, which is the structure our check reads. Support for a sense-and-decide-locally mode, in which the report stays on the device, will determine whether the primitive can run on the standardized procedure.

ACKNOWLEDGEMENTS

This work was supported in part by Nubank, the São Paulo Research Foundation (FAPESP), grants #2020/09850-0 and #2024/21006-1, the National Council for Scientific and Technological Development (CNPq), grant 312294/2025-5, and Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, Brasil (CAPES), and the Comitê Gestor da Internet no Brasil (CGI.br).

ETHICAL CONSIDERATIONS

The IFSP Research Ethics Committee, the Brazilian equivalent of an IRB, approved the study (CAAE 00717726.5.0000.5473). Guardians gave informed consent and children gave assent; adults gave informed consent. We recorded only radio-channel captures, with no images, names, or account identifiers. Deployment would require user initiation, a visible sensing indicator, a fallback path, and retention limits.

REFERENCES

[1] Apple Inc. 2022. Apple, Google, and Microsoft commit to expanded support for FIDO standard. Apple Newsroom. https://www.apple.com/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard/

[2] Apple Inc. 2026. Declared Age Range. Apple Developer Documentation. https://developer.apple.com/documentation/declaredagerange Accessed: 2026-10-12.

[3] Apple Inc. 2026. *Get started with the Verify with Wallet API.* Apple Developer. https://developer.apple.com/wallet/get-started-with-verify-with-wallet/

[4] Rajesh Krishna Balan, Youngki Lee, Tan Kiat Wee, and Archan Misra. 2014. The challenge of continuous mobile context sensing. In *2014*

Sixth International Conference on Communication Systems and Networks (COMSNETS). 1–8. https://doi.org/10.1109/COMSNETS.2014.6734869

[5] Antonio Bianchi, Yanick Fratantonio, Aravind Machiry, Christopher Kruegel, Giovanni Vigna, Pak Chung, and Wenke Lee. 2018. Broken Fingers: On the Usage of the Fingerprint API in Android. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Internet Society, San Diego, CA, USA. https://doi.org/10.14722/ndss.2018.23079

[6] Gioliano de Oliveira Braga, Pedro Henrique Dos Santos Rocha, Giovani Hoff Da Costa, Rafael P. de Mattos Paixão, Gustavo Cavalcanti Morais, Lourenço Alves Pereira, and Guevara Noubir. 2026. HandPass: Cross-Environment Static Spectral Signature Identification via Wi-Fi CSI. In *2026 IEEE Conference on Communications and Network Security (CNS)*. 1–9. https://doi.org/10.1109/CNS69863.2026.11720911

[7] California State Legislature. 2025. Assembly Bill 1043: Age Verification Signals: Software Applications and Online Services (Digital Age Assurance Act). https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB1043 Signed October 13, 2025; operative January 1, 2027.

[8] Jan Camenisch and Anna Lysyanskaya. 2001. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In *Advances in Cryptology — EUROCRYPT 2001*, Birgit Pfitzmann (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 93–118. https://doi.org/10.1007/3-540-44987-6_7

[9] Marco Cascio, Luigi Cinque, Donato Distante, Gian Luca Foresti, and Alessio Fagioli. 2025. A Benchmark Dataset for Radio Signal Image-based Person Re-Identification. *Scientific Data* 12, 1 (Aug. 2025), 1522. https://doi.org/10.1038/s41597-025-05804-0

[10] Federica Cavallo, Angelika Mohn, Francesco Chiarelli, and Cosimo Giannini. 2021. Evaluation of Bone Age in Children: A Mini-Review. *Frontiers in Pediatrics* 9 (2021), 580314. https://doi.org/10.3389/fped.2021.580314

[11] Chen Chen, Gang Zhou, and Youfang Lin. 2023. Cross-Domain WiFi Sensing with Channel State Information: A Survey. *ACM Comput. Surv.* 55, 11, Article 231 (Feb. 2023), 37 pages. https://doi.org/10.1145/3570325

[12] David Chu, Aman Kansal, Jie Liu, and Feng Zhao. 2011. Mobile Apps: It's Time to Move Up to CondOS. In *13th Workshop on Hot Topics in Operating Systems (HotOS XIII)*. USENIX Association, Napa, CA. https://www.usenix.org/conference/hotosxiii/mobile-apps-its-time-move-condos

[13] Lorrie Faith Cranor. 2026. User (Non-)Compliance with Age Verification: Evidence from a Deceptive Web Experiment. In *2026 USENIX Conference on Privacy Engineering Practice and Respect (PEPR 26)*. USENIX Association, Santa Clara, CA, 1–15. https://www.usenix.org/conference/pepr26/presentation/cranor

[14] G F da Costa, G O Braga, P H S Rocha, R Paixão, G C Morais, G Noubir, and L A Pereira Jr. 2026. An Exploratory Cross-Layer Study of Physical Presence Attestation via Wi-Fi CSI for In-Person Payment Anomaly Detection. In *GLOBECOM 2026 - 2026 IEEE Global Communications Conference. (to appear)*.

[15] Gioliano de Oliveira Braga, Pedro Henrique dos Santos Rocha, Rafael Pimenta de Mattos Paixão, Giovani Hoff da Costa, Gustavo Cavalcanti Morais, and Lourenço Alves Pereira Júnior. 2025. SoK: Security Evaluation of Wi-Fi CSI Biometrics: Attacks, Metrics, and Open Challenges. arXiv:2511.11381 [cs.CR] https://arxiv.org/abs/2511.11381

[16] Department of Infrastructure, Transport, Regional Development, Communications and the Arts. 2024. Social media minimum age. Australian Government, Department of Infrastructure Website. https://www.infrastructure.gov.au/media-communications/internet/online-safety/social-media-minimum-age Accessed: 2026-07-10.

[17] European Commission. 2025. Guidelines on the Protection of Minors under the Digital Services Act (DSA), article 28. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors

[18] European Commission. 2026. The EU Age Verification Solution — Privacy by Design via Zero-Knowledge Proof Cryptography. https://ageverification.dev/

[19] European Parliament and Council of the European Union. 2016. Regulation (EU) 2016/679 (General Data Protection Regulation), article 8: Conditions Applicable to Child's Consent in Relation to Information Society Services. Official Journal of the European Union, L 119. https://gdpr-info.eu/art-8-gdpr/

[20] Federal Trade Commission. 2020. *Complying with COPPA: Frequently Asked Questions*. Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

[21] Federal Trade Commission. 2025. Children's Online Privacy Protection Rule; Final Rule Amendments. Federal Register, Vol. 90, No. 76. , 16918–16983 pages. https://www.federalregister.gov/documents/2025/04/22/2025-07612/childrens-online-privacy-protection-rule 16 CFR Part 312.

[22] Borja Gamecho, Luis Gardeazabal, and Julio Abascal. 2013. Combination and abstraction of sensors for mobile context-awareness. In *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication* (Zurich, Switzerland) *(UbiComp '13 Adjunct)*. 1417–1422. https://doi.org/10.1145/2494091.2496037

[23] Andrea Goldsmith. 2005. *Wireless Communications*. Cambridge University Press, New York, NY, USA.

[24] Abigail Goldsteen, Gilad Ezov, Ron Shmelkin, Micha Moffie, and Ariel Farkash. 2022. Data minimization for GDPR compliance in machine learning models. *AI and Ethics* 2, 3 (Aug. 2022), 477–491. https://doi.org/10.1007/s43681-021-00095-8

[25] Google LLC. 2026. Play Age Signals API (beta): Overview. Android Developers, Google Play. https://developer.android.com/google/play/age-signals/overview Last updated 2026-07-20 UTC. Accessed: 2026-10-12.

[26] Google LLC. 2026. Update your account to meet age requirements. Google Account Help. https://support.google.com/accounts/answer/1333913?hl=en Accessed: Out. 22, 2026.

[27] Patrick Grother, Mei Ngan, and Kayee Hanaoka. 2019. *Face Recognition Vendor Test (FRVT) Part 2: Identification*. NIST Interagency Report NIST IR 8271. National Institute of Standards and Technology. https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

[28] Qiuye He and Song Fang. 2023. Phantom-CSI Attacks against Wireless Liveness Detection. In *Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses* (Hong Kong, China) *(RAID '23)*. 440–454. https://doi.org/10.1145/3607199.3607245

[29] Jingyang Hu, Hongbo Jiang, Tianyue Zheng, Jingzhi Hu, Hongbo Wang, Hangcheng Cao, Zhe Chen, and Jun Luo. 2024. M2-Fi: Multi-person Respiration Monitoring via Handheld WiFi Devices. In *IEEE INFOCOM 2024 - IEEE Conference on Computer Communications*. IEEE, Vancouver, BC, Canada, 1221–1230. https://doi.org/10.1109/INFOCOM52122.2024.10621199

[30] Jingzhi Hu, Tianyue Zheng, Zhe Chen, Hongbo Wang, and Jun Luo. 2023. MUSE-Fi: Contactless MUti-person SEnsing Exploiting Near-field Wi-Fi Channel Variation. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking* (Madrid, Spain) *(ACM MobiCom '23)*. Article 75, 15 pages. https://doi.org/10.1145/3570361.3613290

[31] IDScan.net. 2025. What is OCR in ID scanning and document verification? IDScan.net Blog. https://idscan.net/blog/what-is-ocr-in-id-and-document-scanning/ Accessed: 2026-10-22.

[32] Internet Society. 2025. *Age Restrictions and Online Safety: An Internet Society Public Policy Brief.* Public Policy Brief. Internet Society. https://www.internetsociety.org/wp-content/uploads/2025/12/Age-Restrictrions-and-Online-Safety-Policy-Brief-EN.pdf

[33] Suman Jana, David Molnar, Alexander Moshchuk, Alan Dunn, Benjamin Livshits, Helen J. Wang, and Eyal Ofek. 2013. Enabling Fine-Grained Permissions for Augmented Reality Applications with Recognizers. In *22nd USENIX Security Symposium (USENIX Security 13)*. USENIX Association, Washington, D.C., USA. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/jana

[34] Suman Jana, Arvind Narayanan, and Vitaly Shmatikov. 2013. A Scanner Darkly: Protecting User Privacy from Perceptual Applications. In *2013 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 349–363. https://doi.org/10.1109/SP.2013.31

[35] Sakila S. Jayaweera, Beibei Wang, Wei-Hsiang Wang, and K. J. Ray Liu. 2025. DeepCPD: Deep Learning Based In-Car Child Presence Detection Using WiFi. arXiv:2505.08931 https://arxiv.org/abs/2505.08931

[36] Bofan Li, Zhankai Ye, Weikuan Yu, Yongning Tang, and Xin Liu. 2026. 2FiA: Towards WiFi Sensing-Based Authentication with Unique Biometrics . In *2026 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA, 2929–2945. https://doi.org/10.1109/SP63933.2026.00087

[37] Xin Li, Hongbo Wang, Zhe Chen, Zhiping Jiang, and Jun Luo. 2024. UWB-Fi: Pushing Wi-Fi towards Ultra-wideband for Fine-Granularity Sensing. In *Proceedings of the 22nd Annual International Conference on Mobile Systems, Applications and Services (MobiSys '24)*. ACM, Tokyo, Japan, 1–14. https://doi.org/10.1145/3643832.3661889

[38] Shuang Liu and Sarah Scheffler. 2026. Adequately Tailoring Age Verification Regulations. In *Proceedings of the Symposium on Computer Science and Law* (Berkeley, CA, USA) *(CSLAW '26)*. 239–248. https://doi.org/10.1145/3788646.3789526

[39] Yongsen Ma, Gang Zhou, and Shuangquan Wang. 2019. WiFi Sensing with Channel State Information: A Survey. *ACM Comput. Surv.* 52, 3, Article 46 (June 2019), 36 pages. https://doi.org/10.1145/3310194

[40] I. Malkin, G. Bigman, R. Matias, L. Kalichman, M. J. Seibel, E. Kobyliansky, and G. Livshits. 2006. Age-related Changes of Bone Strength Phenotypes: Observational Follow-up Study of Hand Bone Mineral Density. *Archives of Osteoporosis* 1, 1–2 (2006), 59–68. https://doi.org/10.1007/s11657-006-0009-y

[41] Miller & Zois, LLC. 2025. Children and Online Use of Parents' Credit Cards. Maryland Child Safety Law Blog. https://childsafety.marylandinjurylawyer.net/online-child-safety/children-and-online-use-of-parents-credit-cards/ Accessed: 2026-10-22.

[42] Ministério da Fazenda, Secretaria de Prêmios e Apostas. 2024. Portaria SPA/MF nº 722, de 2 de maio de 2024. https://www.in.gov.br/en/web/dou/-/portaria-spa/mf-n-722-de-2-de--maio-de-2024-557715851 Annex I, item 10: registration limited to bettors over 18; facial recognition before account registration.

[43] Beadaa Mohammed, Jin Jin, Amin M. Abbosh, Konstanty S. Bialkowski, Mohamed Manoufali, and Stuart Crozier. 2017. Evaluation of Children's Exposure to Electromagnetic Fields of Mobile Phones Using Age-Specific Head Models With Age-Dependent Dielectric Properties. *IEEE Access* 5 (2017), 27345–27353. https://doi.org/10.1109/ACCESS.2017.2767074

[44] Jakub Paplhám and Vojtěch Franc. 2024. A Call to Reflect on Evaluation Practices for Age Estimation: Comparative Analysis of the State-of-the-Art and a Unified Benchmark. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, Seattle, WA, USA, 1196–1205. https://doi.org/10.1109/CVPR52733.2024.00120

[45] Presidência da República do Brasil. 2025. Lei nº 15.211, de 17 de setembro de 2025: Estatuto Digital da Criança e do Adolescente. Diário Oficial da União, Edição extra, 17 set. 2025. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm Vigência: 17 de março de 2026.

[46] Android Open Source Project. 2026. Measuring Biometric Unlock Security. https://source.android.com/security/biometric/measure. Accessed: Oct. 14, 2026.

[47] Theodore S. Rappaport. 2002. *Wireless Communications: Principles and Practice* (2nd ed.). Prentice Hall, Upper Saddle River, NJ, USA.

[48] Roblox Corporation. 2026. Roblox Requires Users Worldwide to Age Check to Access Chat. Roblox Newsroom. https://about.roblox.com/newsroom/2026/01/roblox-age-checks-required-to-chat

[49] Tanguy Ropitault, Claudio R. C. M. da Silva, Steve Blandino, Anirudha Sahoo, Nada Golmie, Kangjin Yoon, Carlos Aldana, and Chunyu Hu. 2024. IEEE 802.11bf WLAN Sensing Procedure: Enabling the Widespread Adoption of WiFi Sensing. *IEEE Communications Standards Magazine* 8, 1 (2024), 58–64. https://doi.org/10.1109/MCOMSTD.0004.2200062

[50] Sarah Scheffler. 2024. Age Verification Systems Will Be a Personal Identifiable Information Nightmare. *Commun. ACM* 67, 7 (July 2024), 31–33. https://doi.org/10.1145/3660519

[51] Paul Schmitt, Jana Iyengar, Christopher Wood, and Barath Raghavan. 2022. The decoupling principle: a practical privacy framework. In *Proceedings of the 21st ACM Workshop on Hot Topics in Networks* (Austin, Texas) *(HotNets '22)*. 213–220. https://doi.org/10.1145/3563766.3564112

[52] Cong Shi, Jian Liu, Hongbo Liu, and Yingying Chen. 2021. WiFi-Enabled User Authentication through Deep Learning in Daily Activities. *ACM Trans. Internet Things* 2, 2, Article 13 (May 2021), 25 pages. https://doi.org/10.1145/3448738

[53] Jasmins Soraia. 2026. Children are drawing moustaches on their faces to fool online age checks – and it's working. Euronews Next. https://www.euronews.com/next/2026/05/04/children-are-drawing-moustaches-on-their-faces-to-fool-online-age-checks-and-its-working

[54] Jalaludin Ar Raniry Wiliam Tchin, Alvin Winata, Simeon Yuda Prasetyo, and Eko Setyo Purwanto. 2025. Facial Age Estimation with Deep Convolutional Neural Network Architecture. In *2025 International Conference on Advancement in Data Science, E-learning and Information System (ICADEIS)*. IEEE, Bandung, Indonesia, 1–6. https://doi.org/10.1109/ICADEIS65852.2025.10933445

[55] W3C. 2021. Web Authentication: An API for Accessing Public Key Credentials, Level 2. W3C Recommendation. https://www.w3.org/TR/webauthn-2/

[56] Fei Wang, Jinsong Han, Shiyuan Zhang, Xu He, and Dong Huang. 2019. CSI-Net: Unified Human Body Characterization and Pose Recognition. arXiv:1810.03064 [cs.LG] https://arxiv.org/abs/1810.03064

[57] Fei Wang, Tingting Zhang, Wei Xi, Han Ding, Ge Wang, Di Zhang, Yuanhao Cui, Fan Liu, Jinsong Han, Jie Xu, and Tony Xiao Han. 2026. A Survey on Wi-Fi Sensing Generalizability: Taxonomy, Techniques, Datasets, and Future Research Prospects. *IEEE Communications Surveys & Tutorials* 28 (2026), 5227–5266. https://doi.org/10.1109/COMST.2026.3670854

[58] Craig Watson, Gregory Fiumara, Elham Tabassi, Su Lan Cheng, Patricia Flanagan, and Wayne Salamon. 2014. *Fingerprint Vendor Technology Evaluation.* NIST Interagency Report NIST IR 8034. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8034

[59] Tong Xin, Bin Guo, Zhu Wang, Mingyang Li, and Zhiwen Yu. 2016. FreeSense:Indoor Human Identification with WiFi Signals. arXiv:1608.03430 [cs.HC] https://arxiv.org/abs/1608.03430

[60] Zhi Xu and Sencun Zhu. 2015. SemaDroid: A Privacy-Aware Sensor Management Framework for Smartphones. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy* (San Antonio, Texas, USA) *(CODASPY '15)*. 61–72. https://doi.org/10.1145/

2699026.2699114

[61] Wei-Zhu Yeoh, Michal Kepkowski, Gunnar Heide, Dali Kaafar, and Lucjan Hanzlik. 2023. Fast IDentity Online with Anonymous Credentials (FIDO-AC). In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 3029–3046. https://www.usenix.org/conference/usenixsecurity23/presentation/yeoh

[62] Yoti Ltd. 2024. *Yoti Facial Age Estimation White Paper*. Technical Report. Yoti Ltd. https://www.yoti.com/blog/yoti-age-estimation-white-paper/ Accessed: Oct. 14, 2026.

[63] Xin Zhang, Min Zhang, Zhe Liu, Bin Zhao, Zhengyu Yang, and Min Yang. 2025. An Empirical Study on Fingerprint API Misuse with Lifecycle Analysis in Real-world Android Apps. In *Proceedings of the 2025 Network and Distributed System Security Symposium (NDSS)*. Internet Society, San Diego, CA, USA. https://doi.org/10.14722/ndss.2025.230699

[64] Yi Zhang, Yue Zheng, Guidong Zhang, Kun Qian, Chen Qian, and Zheng Yang. 2021. GaitSense: Towards Ubiquitous Gait-Based Human Identification with Wi-Fi. *ACM Trans. Sen. Netw.* 18, 1, Article 1 (Oct. 2021), 24 pages. https://doi.org/10.1145/3466638